Description of document:	Department of Homeland Security (DHS) After Action Reports for Three (3) Top Officials (TOPOFF) Exercises, 2003-2006 and TOPOFF) 4 Exercise Evaluator Handbook, 2007
Requested date:	15-January-2017
Released date:	24-May-2017
Posted date:	12-June-2017
Reports included:	Top Officials (TOPOFF) Exercise Series: TOPOFF 2 (T2) After Action Summary Report, 2003 (PDF page 4) Top Officials (TOPOFF) 3 (T3) Full Scale After-Action Report, 2005 (PDF page 441) Top Officials (TOPOFF) 4 (T4) Command Post Exercise After-Action Report, 2006 (PDF page 839) Top Officials (TOPOFF) 4 (T4) Exercise Evaluator Handbook, 2007 (PDF page 1019)
Source of document:	FEMA Information Management Division FOIA Request 500 C Street, S.W., Mailstop 3172 Washington, D.C. 20472 Email: fema-foia@dhs.gov Online FOIA Request Form

U.S. Department of Homeland Security
500 C Street, S.W. Mail Stop 3172
Washington, DC 20472-3172

FEMA

May 24, 2017

SENT VIA E-MAIL

Re: **FOIA Request Number 2017-FEFO-00972**

This is the final response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), dated January 15, 2017, and received in this office on January 17, 2017. You are seeking a digital/electronic copy of the After Action Report for TOPOFF 2, the After Action Report for TOPOFF 3, the After Action Report for TOPOFF 4 and the TOPOFF 4 Evaluator Handbook.

A search of FEMA's National Preparedness Directorate (NPD) for documents responsive to your request produced a total of 1,045 pages. Of those pages, I have determined that 1,028 pages of the records are releasable in their entirety, and 17 pages are partially releasable pursuant to Title 5 U.S.C. § 552(b)(6), FOIA Exemption 6.

FOIA Exemption 6 exempts from disclosure of personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right to privacy. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

You have the right to appeal if you disagree with FEMA's response. The procedure for administrative appeals is outlined in the DHS regulations at 6 C.F.R. § 5.8. In the event you wish to submit an appeal, we encourage you to both state the reason(s) you believe FEMA's initial determination on your FOIA request was erroneous in your correspondence, and include a copy of this letter with your appeal. Should you wish to do so, you must send your appeal within

90 days from the date of this letter to fema-foia@fema.dhs.gov, or alternatively, via mail at the following address:

FEMA
Office of the Chief Administrative Officer
Information Management Division (FOIA Appeals)
500 C Street, SW, Seventh Floor, Mail Stop 3172
Washington, D.C. 20472-3172

As part of the 2007 amendments, the Office of Government Information Services (OGIS) was created to offer mediation services to resolve disputes between FOIA requesters and Federal agencies. You may contact OGIS in any of the following ways:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road- OGIS
College Park, MD 20740-6001
E-mail: ogis@nara.gov
Web: https://ogis.archives.gov
Telephone: 202-741-5770/Toll-free: 1-877-684-6448
Facsimile: 202-741-5769

Provisions of the FOIA allow us to recover part of the cost of complying with your request. In this instance, because the cost is below the $25 minimum, there is no charge.

If you need any further assistance or would like to discuss any aspect of your request, please contact us and refer to FOIA case number **2017-FEFO-00972**. You may send an e-mail to fema-foia@fema.gov, call (202) 646-3323, or you may contact our FOIA Public Liaison in the same manner.

Sincerely,

ERIC A NEUSCHAEFER

Digitally signed by ERIC A NEUSCHAEFER
DN: c=US, o=U.S. Government, ou=Department of Homeland Security, ou=FEMA, ou=People, cn=ERIC A NEUSCHAEFER, 0.9.2342.19200300.100.1.1=0647718256.FEMA
Date: 2017.05.23 11:16:58 -04'00'

Eric Neuschaefer
Chief, Disclosure Branch
Information Management Division
Mission Support

Enclosure: Responsive Records, (1,045 pages)

TOP OFFICIALS (TOPOFF) EXERCISE SERIES

TOPOFF 2 (T2)
After Action Report

September 30, 2003

Homeland Security

FOR OFFICIAL USE ONLY

This page intentionally left blank

ADMINISTRATIVE HANDLING INSTRUCTIONS

1. The title of this document is *Top Officials (TOPOFF) Exercise Series: TOPOFF 2 (T2) After Action Summary Report.*

2. Information contained in this document is intended for the exclusive use of T2 Exercise Series participants. Material may not be reproduced, copied, or furnished to non-exercise personnel without written approval from the Exercise Directors.

3. This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate Canadian, U.S. Department of Homeland Security (DHS), U.S. Department of State (DOS), the State of Illinois, the State of Washington, and local/city security directives. This document is marked For Official Use Only ~~(FOUO),~~ and information contained herein has not been given a security classification pursuant to the criteria of an Executive Order, but this document is to be withheld from the public because disclosure would cause a foreseeable harm to an interest protected by one or more ~~FOUO~~ exemptions.

4. Reproduction of this document, in whole or in part, without prior approval of DHS is prohibited.

5. DHS, Office for Domestic Preparedness (ODP), and DOS, the Office of the Coordinator for Counterterrorism, cosponsored the T2 Exercise Series. Mr. Theodore Macklin (b)(6) (b)(6) and Mr. Corey Gruber (202-514-0284) are the ODP Points of Contact (POC) and (b)(6) (b)(6), the Office of the Coordinator for Counterterrorism, is the POC for international play.

6. This report is intended for the use of Federal, State, and local (FSL) officials responsible for homeland security. It is intended to improve the FSL plans to prevent and respond to weapons of mass destruction by understanding the lessons learned from T2.

This page intentionally left blank

Top Officials (TOPOFF) Exercise Series:

TOPOFF 2 (T2) After Action Summary Report

Prepared for
U.S. Department of Homeland Security
Office for Domestic Preparedness
by AMTI and the CNA Corporation
Under Schedule Number GS-10F-0324M,
Order Number 2003F028

This page intentionally left blank

SUMMARY REPORT

I. Introduction

Top Officials (TOPOFF) 2 (T2) was a Congressionally-mandated, national combating terrorism exercise. The exercise was designed to improve the nation's domestic incident management capability by exercising the plans, policies, procedures, systems, and facilities of Federal, State, and local (FSL) response organizations against a series of integrated and geographically dispersed terrorist threats and acts.

T2 was cosponsored by the U.S. Department of Homeland Security (DHS) and the U.S. Department of State. The T2 After Action Report (AAR) provides the findings from the analysis of the Full-Scale Exercise (FSE), and also integrates the findings from the pre-FSE seminars and the Large-Scale Game (LSG).

The domestic objectives of the T2 exercise were to improve the nation's capacity to manage complex/extreme events; create broader operating frameworks of expert domestic incident management and other systems; validate FSL authorities, strategies, plans, policies, procedures, protocols, and synchronized capabilities; and build a sustainable, systematic exercise process for advancing domestic preparedness. There was also an international aspect of T2 that exercised a segment of the Canadian response to weapons of mass destruction (WMD) attacks upon the United States. This cross-border play focused on bilateral goals in the areas of communication, preparedness, and response to WMD terrorism incidents.

T2 was the largest and most comprehensive terrorism response exercise ever conducted within the United States. The T2 exercise scenario depicted a fictitious, foreign terrorist organization that detonated a simulated radiological dispersal device (RDD) in Seattle, Washington, and released the Pneumonic Plague (*Yersinia pestis*) in several Chicago area locations. There was also significant pre-exercise intelligence play, a cyber attack, and credible terrorism threats against other locations.

II. Background

A. T2 Authorization

Public Law 106-553 authorized T2, and Senate Report 106-404 outlined the concept. T2 supported the National Security Council's Policy Coordinating Committee on Counter-terrorism and National Preparedness Exercise Sub-group requirement for a large-scale, counterterrorism exercise commencing in 2002 and finishing in 2003. While T2 planning began under earlier Presidential Directives, the Homeland Security Presidential Directive (HSPD)-5 articulates the new federal incident management policy that ultimately guided the exercise. Participating FSL authorities were asked to submit exercise objectives to T2 planners at the start of the T2 design cycle to ensure that the exercise design would support participant objectives while also addressing national priorities.

B. Exercise Design and Concept

The first TOPOFF Exercise (TOPOFF2000) was a single, no-notice, FSE co-chaired by the Department of Justice and the Federal Emergency Management Agency (FEMA) in May 2000. Unlike TOPOFF2000, T2 was designed as an "open" exercise in which participants were introduced to the exercise scenario prior to the FSE through a cycle of exercise activity of increasing complexity that included:

- A series of seminars that explored emergency public information, RDD response, bioterrorism, and national direction and control issues;
- An LSG that explored intermediate and long-term recovery issues;
- An Advanced Distance Learning Exercise, conducted in conjunction with the *National Direction and Control Seminar*, that employed distance education technology to disseminate information and provide interactive training opportunities; and
- The *Top Officials Seminar* that brought together top government officials from 25 FSL agencies and departments, and the Canadian Government, in a round-table discussion to explore intergovernmental domestic incident management in response to WMD terrorist attacks upon the United States.

These activities culminated in an FSE which was played out from May 12 to May 16, 2003.

The purpose of the open exercise design was to enhance the learning and preparedness value of the exercise through a "building-block" approach, and to enable participants to develop and strengthen relationships in the national response community. Participants at all levels stated that this approach has been of enormous value to their domestic preparedness strategies.

III. Findings of the Exercise Analysis

A. Special Topics

The FSE exercised numerous critical aspects of the national response to radiological and bioterrorism attacks. This response cut across several predetermined areas of analysis, as decided by T2 participants in earlier exercise activities (see below). Specific special interest items included the following:

- Alerts and Alerting: The Elevation of the Homeland Security Advisory System Threat Level to Red;
- Declarations and Proclamations of Disaster and Emergency;
- Department of Homeland Security Play in T2: The Role of the Principal Federal Official;
- Data Collection and Coordination: Radiological Dispersal Device Plume Modeling and Deposition Assessment in Washington;
- Play Involving the Strategic National Stockpile;
- Hospital Play in the Illinois Venue: Resources, Communications, and Information Sharing during a Public Health Emergency;
- Decision-Making Under Conditions of Uncertainty: The Plague Outbreak in the Illinois Venue; and
- Balancing the Safety of First Responders and the Rescue of Victims.

B. Core Areas of Analysis

Rather than evaluating participant ability and performance or specific agency-by-agency objectives, the exercise evaluation methodology focused on the objective analysis of decision and coordination processes that support the nation's top officials and the broader system of FSL agencies. The exercise events were analyzed as they unfolded in light of six major areas of analysis, identified through a survey of TOPOFF 2000 findings, and other exercise or real-world lessons learned:

- Emergency Decision-Making and Public Policy;
- Emergency Public Information;
- Communications, Coordination, and Connectivity;
- Jurisdiction;
- Resource Allocation; and
- Anticipating the Enemy.

IV. Artificialities

Artificialities are inherent in every exercise and result from the simulated nature of exercises. False conclusions can arise if the natures and effects of artificialities are not accounted for during the analysis process. Some artificialities were essential in exercise design including the simulated RDD explosion, prescheduled top official play, limited public involvement, and notional road closures. Some artificialities were specific to the T2 design process, such as the known scenario and the lack of 24-hour play by some entities. Other T2 artificialities, while not preplanned, were nonetheless anticipated in the exercise, as it encouraged free play. The evaluation team researched, documented, and factored all such artificialities into the analysis of the FSE.

V. Special Topics

A. Alerts and Alerting: The Elevation of the Homeland Secnrity Advisory System Threat Level to Red

The FSE exercised the use of the Homeland Security Advisory System (HSAS); the decision to elevate the HSAS Threat Level to Red; and the actions associated with Threat Level "Severe," or Red. It also allowed examination of the implications of raising specific regions or localities to Red. The FSE highlighted that further refinement of this advisory system is needed.

Significant findings from the FSE include the following:

- Following the local threat level elevations of Seattle and King County early in the FSE, there was uncertainty as to the status of the HSAS Threat Condition of other jurisdictions. This situation was caused in part by a) a lack of awareness of local threat advisory systems; b) inconsistent or nonexistent formal notification protocols of threat elevations; and c) a lack of language clarity—elevations of the HSAS are referred to as elevations of the "National Threat Level," even if applied to regions or localities;
- The FSL response to elevations of the HSAS needs to he further developed and synchronized. Participants in the T2 After Action Conference (AAC) suggested the development of a tiered, operational response linked to the HSAS levels and based upon the nature of the threat. This system would he defined by a coalition of FSL agencies and would offer a comprehensive operational response framework that jurisdictions at all levels could use to help define their response plans at each HSAS Threat Condition. DHS is leading an interagency effort to review these recommendations and make appropriate refinements to the HSAS; State, local, and private sector constituents are active partners in this process; and
- Agencies are concerned about the lack of specific intelligence accompanying threat level elevations and the cost of maintaining a raised threat level. DHS is currently examining ways to improve information flow to and from State and local governments and the private sector regarding changes in alert level. Also, the DHS-led HSAS Working Group is currently addressing the economic and operational impacts of a raised threat condition.

B. Declarations and Proclamations of Disaster and Emergency

During the FSE, several declarations and proclamations of emergencies and disasters were issued. Local and State jurisdictions in both exercise venues invoked their authorities to declare emergencies and requested Federal assistance under the Stafford Act. These requests ultimately led to a Presidential Declaration of Major Disaster in Washington and a Presidential Declaration of Emergency in Illinois. The bioterrorism attack in Illinois was especially challenging as its impact involved multiple counties, the city of Chicago, and the state of Illinois. In addition, the Secretary of the Department of Health and Human Services (HHS) declared a Public Health Emergency in the state of Illinois under the authorities of the Public Health Service Act. This occurred before the Presidential Declaration of Emergency, enabling the activation of several response assets.

Significant findings from the FSE include the following:

- Officials in Illinois requested a Major Disaster Declaration to obtain maximum Federal assistance for the growing bioterrorism disaster, out of concern for the perceived five million dollar limit and other limits to Federal assistance in declarations of emergency. Some were unaware that the President can approve an expenditure of funds in excess of that limit under the conditions where, as stated in the Stafford Act, "continued emergency assistance is immediately required; there is a continuing and immediate risk to lives, property, public health, or safety; and necessary assistance will not otherwise be provided on a timely basis." In addition, the nature of the declaration in Illinois led to concerns about whether some individual assistance programs, which are specifically authorized for a disaster but not for an emergency, would be authorized;
- It is worth noting that during the FSE, the President did not declare the large-scale bioterrorism attack a Major Disaster under the Stafford Act. It is not clear from the FSE whether the difference in declaring an emergency or a major disaster would result in substantive operational issues given the exception clauses under declarations of emergency as previously described;
- There was some uncertainty regarding the relationships between State and local declarations of emergency. In Illinois there was some uncertainty as to whether county-level declarations needed to be enacted in light of a State declaration of emergency or whether a state declaration made these moot. Officials determined that in legal terms, county-level declarations needed to be enacted, even when preceded by a State declaration of emergency, to access funds that the State declaration made available; and
- The relationships between the authorities and resources brought to bear under the Public Health Act and the Stafford Act should continue to be exercised. Additional clarity regarding the authorities and resources brought to bear under both Acts is required.

C. Department of Homeland Security Play in T2: The Role of the Principal Federal Official

The FSE was the first major opportunity for the newly created DHS to exercise and experiment with its domestic incident management organization, functions, and assets. For example, the DHS Principal Federal Official (PFO) concept was first implemented during the FSE, which provided the opportunity to examine the role of the PFO during an emergency response. During the FSE, the PFOs in both venues facilitated integrated communications and coordinated action planning. In addition, they both encouraged active communications with state and local authorities.

Significant findings from the FSE include the following:

- The PFO was well-received and successfully integrated into the unified command structure in both venues. In Seattle, the PFO quickly instituted a unified command to manage the overall Federal response and coordinate integrated communications and action planning. The PFO in Seattle also helped to prioritize and adjudicate between the often-competing needs of the crisis and consequence management sides of the response phase. In Illinois, the PFO worked within the framework of a unified command to ensure that integrated communications were achieved and that action plans were coordinated;

- The PFO relationships with Federal officials differed in part due to the different problems that each encountered with the two different attacks. In Seattle, although an RDD was involved, the event unfolded in more of a traditional first-responder fashion with a relatively well-delineated disaster site. In Illinois, events unfolded more gradually, as would be expected in a disease outbreak. As a result, the PFOs in each venue had different relationships with the FEMA Regional Director (RD), the FEMA Federal Coordinating Officer (FCO), and the FBI Special-Agent-In-Charge (SAC). The roles and responsibilities of the PFO relative to FEMA and FBI officials have been clarified through issuance of the Initial National Response Plan (INRP); and
- Both PFOs required additional technical support beyond their deployed administrative and security details. The FSE highlighted the need for the PFO to have a dedicated staff with the flexibility and expertise to support all emergencies, natural and terrorist-related. DHS has recently developed operational procedures for providing additional resources to the PFO to facilitate domestic incident management activities. Further delineation of the roles and responsibilities of the PFO, as well as PFO support requirements, will be included in the final version of the National Response Plan (NRP).

D. Data Collection and Coordination: Radiological Dispersal Device Plume Modeling and Deposition Assessment in Washington

During the FSE, there were multiple FSL agencies that had responsibilities for collecting data. The data was then sent to one or more locations to be compiled and analyzed. Once the analyses were complete, information was provided to top officials to assist in their decision-making. However, there were critical data collection and coordination challenges that impacted the response to the RDD attack in Seattle, to include the provision of timely, consistent, and valid information to top officials.

Significant findings from the FSE include the following:

- The coordination of onsite and offsite data collection by multiple agencies at FSL levels of government needs to be improved. The FSE highlighted the many radiological data collection assets that exist at all levels of government. FSL agencies and departments, therefore, need to be educated about the importance of coordinating the data collection process, and to work with the Federal Radiological Monitoring and Assessment Center (FRMAC) to ensure that coordination takes place during radiological emergencies. The development of the NRP will more clearly delineate the data collection and coordination processes in the future;
- The development and distribution of multiple radiological plume analysis products—including plume model prediction overlays and empirical deposition/footprint maps—to decision-makers needs to be better coordinated. Different FSL agencies and jurisdictions used one or more plume models to generate predictions. Each jurisdiction also developed its own data products based upon separate and sometimes conflicting empirical data. As a result, Seattle, King County, and Washington State top officials had different or conflicting information upon which to base their decisions. In addition, several Federal agency and department headquarters developed their own plume predictions to make internal assessments concerning assets that might be required. Conflicting predictions were, therefore, presented to department and agency top officials;

- There is a need for additional education among both responders and decision-makers as to the timing and value of the different types of information following a radiological incident. The value and limitations of plume models and other analysis products are not widely understood. Importantly, it appears as though few decision-makers were informed of the limited usefulness and lifecycle of plume models. Plume models provide a prediction of where the material in the explosion will travel. They can be useful in assisting decision-makers in making preliminary decisions regarding likely areas of contamination. Once actual data from the incident is collected and evaluated, the value of plume models diminishes. Once responders learn what really is out there and where it is, predictions alone become less important. However, predictions updated with initial measurement data can he useful in estimating protective actions in areas that have not yet been surveyed, or in areas that have been contaminated below the measurement threshold of available instruments; and
- The Homeland Security Council is leading an interagency effort to remedy the plume modeling process deficiencies noted during the exercise.

E. Play Involving the Strategic National Stockpile

The activation, requests for, deployment and distribution of the Strategic National Stockpile (SNS) were extensively played during the FSE. The exercise tested the ability of all levels of government to make decisions, allocate resources, coordinate and communicate, and inform the public regarding this critical SNS resource. The state of Illinois tested its ability to break down and secure the antibiotic stocks, and local jurisdictions tested their abilities to distribute supplies of antihiotics to their first responders and citizens. Overall, the request, receipt, hreakdown, distribution, and dispensing of the SNS during the FSE were completed successfully. Some components of the SNS were not tested during the exercise. Some aspects of the requesting process exercised in T2 presented specific challenges.

Significant findings from the FSE include the following:

- Determining a prophylaxis distribution policy for first responders and citizenry across local jurisdictions was challenging. This was due, in part, to the enormous logistical challenges of distrihuting medications to a large metropolitan area, as well as the very real limitation of the amount of medication that was immediately available. Determining a prophylaxis distrihution policy was also challenging due to the need to factor in anticipated public reaction if the general citizenry were not given access to the medication;
- Contradictory information complicated decision-making with respect to the allocation of the SNS. Decision-makers experienced difficulty determining the amounts in local stockpiles; how much the State had and how its amount would be allocated; and how much would be coming from the SNS, when it would arrive, and how much each jurisdiction would receive;
- Inconsistent information was given by different jurisdictions as to who should seek prophylaxis and when, the locations of the suspected plague release sites, and whether one should stay home or seek medical attention; and

- The Homeland Security Council is leading an interagency working group to resolve the mass prophylaxis issues that arose during the exercise.

F. Hospital Play in the Illinois Venue: Resources, Communications, and Information Sharing during a Public Health Emergency

During the FSE, 64 hospitals in the Illinois venue participated in the exercise, making it one of the largest mass casualty exercises ever undertaken. This aspect of T2 presented an unprecedented opportunity to examine the coordinated efforts of the medical and public health communities to react to and control the spread of a disease outbreak, specifically an outbreak initiated by a bioterrorism attack. Because of the large number of participating hospitals, challenges regarding communication and the management of resource requirements were significant.

Significant findings from the FSE include the following:

- During the FSE, the lack of a robust and efficient local emergency communications infrastructure was apparent. Communications heavily relied upon telephones and faxes for data transmission. The unanticipated large call volume was the greatest problem. The phone system in at least one location was overwhelmed, requiring tbree amateur radio operators to maintain communications connectivity. Facsimile communications were also subject to transmission and receipt problems due to call volumes. "Blast fax transmissions" took up to two hours to complete. In addition, information was often copied manually to a form. The form was then faxed (in some cases degrading its readability) to a collection point, where it was then manually tabulated on another form, and then entered into an information system for transmission. This process significantly increases potential errors; and
- Resource demands challenged hospitals throughout the FSE. These included short supplies of isolation and negative pressure rooms, as well as staff and bed shortages. Hospitals employed a number of solutions to these problems including activating staff phone trees to recall medical personnel; using extra conference rooms, lobbies, and Clinical Decision Units (closed units) as isolation wards; and using same-day surgery, radiology, and endoscopy labs, as well as an offsite tent, as negative pressure (i.e., disease containment) rooms.

G. Decision-Making Under Conditions of Uncertainty: The Plague Outbreak in the Illinois Venue

During a disease outbreak, whether naturally occurring or initiated by an act of terrorism, decision-makers must make effective response decisions. Officials rely upon scientists, medical doctors, and the public health system to provide them with the best scientific information. It is this information that decision-makers must use to formulate answers within the context of the logistical, political, social, public health, and economic aspects of a response. This is especially difficult following terrorist attacks due to the enormous media and time pressures that decision-makers will operate under. During the FSE, public health officials initially were uncertain as to the extent and possible duration of the plague epidemic. This produced an environment where officials had to make decisions without the benefit of positive-proof information.

Significant findings from the FSE include the following:

- Coordination processes between agencies and across jurisdictions regarding epidemiological model predictions and patient data need to be improved. In fact, information about some modeling efforts was not provided to all operations centers during the FSE;
- There needs to be an enhanced understanding of the implications of long-term patient load during a bioterrorism incident. Two issues of concern are: (1) a lack of confidence in the patient data, and no clear way to model the long-term effects in the face of poor patient data; and (2) a lack of long-term exercise play—the FSE concluded before the extensive scale of the outbreak was apparent;
- During the early stages of an outbreak, decision-makers are likely to see reports about only the early presenters, not the full number of exposed persons. It is absolutely critical to determine rapidly the scale of the outbreak. This is especially true in cases of potential bioterrorism where traditional epidemiological curves could be multiplied by multiple, continuing, or widespread initial exposures; and
- The Homeland Security Council is leading an interagency effort to resolve mass care and medical surge capacity issues that arose during the exercise.

H. Balancing the Safety of First Responders and the Rescue of Victims

During incidents when victim survival is dependent upon the timeliness of medical treatment, first responders typically initiate victim rescue and removal as rapidly as possible, while incident commanders manage responder safety with an ongoing risk-benefit analysis. However, when faced with an emergency that potentially involves WMD, first responders face a greater potential of becoming casualties themselves. Given the uncertainty surrounding the simulated RDD explosion during the FSE, even when many of the responders artificially had the knowledge that it was a radiological incident, the incident commander had to take precautions to ensure that the responders were safe. However, a number of public health officials and data collectors at the incident site, many of whom were subject matter experts, expressed concern about the time it took to triage, treat, and transport victims.

Significant findings from the FSE include the following:

- Rescue operations at the RDD incident site highlighted the need for more frequent, informational communication between incident command and hospital control. Incident commanders may need to be more proactive in providing information. While hospital control was aware that radiation had been detected at the incident site, there is no indication in the data analyzed that incident command or the medical group at the incident site communicated with hospital control to explain the need to conduct a more detailed risk-benefit analysis before rescue operations could commence. In addition, hospital control was unaware of the periodic halts to rescue operations that occurred during the initial hours of the exercise response due to both the suspected and simulated presence of secondary explosive devices; and
- The public health and medical communities, the media, and the general public should be educated on the unique considerations that must be factored into rescue operations following a terrorist WMD attack. Considerations non-responder communities should be aware of are the need to balance responder safety and rescue efforts and the specific

practices rescuers employ when responding to critical situations, such as the potential for secondary explosive devices in or around an incident scene. The public health and medical communities should be made aware of the need for incident command to conduct a detailed risk-benefit analysis prior to the start of rescue operations. Finally, a consistent message to the public from incident command, public health, and medical communities is critical.

VI. Six Core Areas of Analysis

A. Emergency Public Policy aud Decision-Making

Emergency Public Policy and Decision-Making encompasses the unique challenges, difficulties, and nuances faced by top officials in the initial aftermath of a terrorist WMD attack. During the FSE, top officials were faced with two critical decisions that have not yet occurred in the real world: (1) elevations of the threat status to Red by City, County, and Federal authorities; and (2) a request for and issuance of Presidential Declarations for RDD and bioterrorism attacks.

Significant findings from the FSE include the following:

- Making decisions under conditions of uncertainty, when information is rapidly changing or unknown, remains a significant challenge. Decision-makers experienced challenges obtaining reliable, validated, and timely information. In the case of bioterrorism, the parameters are difficult to define, and the full extent of the effects from such an attack may be unknown. During a physical disaster, such as the case of an RDD blast, the parameters can often be roughly determined, but life-saving and public safety decisions may be required before perfect information is available;
- Greater understanding is needed of the mid- to long-term impacts of multiple terrorist attacks. The FSE did not play out long enough for participants to face the long-term economic, health, social, or political implications of the scenario. To more thoroughly examine long-term issues, the private sector should be encouraged to participate more extensively in future TOPOFF exercises and events; and
- The international aspect of T2 and the active participation of the Canadian Government represented a significant new element of the TOPOFF Exercise design. The cross-border play expanded the scope of decisions faced by domestic top officials during the FSE and enhanced the realism of the exercise.

B. Emergency Public Information

Emergency Public Information encompasses the unique public information challenges and implications faced by top officials and their support staff in the midst of a terrorist WMD attack. Emergency public information was a dominant issue of TOPOFF 2000 and remained one throughout the T2 seminars, LSG, and FSE. T2 provided a unique opportunity for jurisdictions at all levels to exercise, experiment with, and improve upon critical public information strategies. This exercise was an opportunity for participants to showcase the value of concepts, such as regional Joint Information Centers (JICs), that may be expanded for more comprehensive coordination at both broader FSL levels and in environments where people cannot be physically co-located.

Participants commented that future TOPOFF Exercises should continue to allow participants to experiment in the emergency public information arena, which should include an aggressive news-gathering element and a realistic mock-public response to further challenge exercise participants.

Significant findings from the FSE include the following:

- Speaking with one voice proved to be one of the greatest emergency public information challenges during the FSE. JICs were implemented in both venues and helped to unify messages, but not all information was coordinated through the JICs. In both venues, however, the DHS PFO emphasized and worked for a consistent Federal message that was also consistent with the State and local messages;
- Official messages to the public regarding protective action guidelines were often incomprehensive or conflictive;
- Rumors abounded during the FSE. Determining which statements were true proved to be a significant challenge for T2 participants. Improving official channels of communication would help to counter and confirm rumors. Ensuring accurate information depends upon having structured, well-defined, and robust information flow strategies, where information is accepted from predefined validated sources. Such strategies exist in numerous policies such as the INRP, but implementation of them remains a challenge. Although the exercise did not play out long enough in either venue to establish how the long-term role of the PFO might affect information flow, during a disaster, the PFO role has the potential to strengthen and streamline the movement of key information between the State and local governments and Federal agencies;
- Even though the need for pre-coordinated information packages was mentioned throughout the seminars and during the LSG, many agencies lacked a full set of pre-coordinated, off-the-shelf packages prior to the FSE; and
- DHS has led an interagency effort to successfully remedy the incident communications deficiencies noted during TOPOFF 2000. Results include an interagency-approved incident communications strategy, hotline, subject matter expert reach-back, and improved FSL incident communications processes and protocols.

C. Communications, Coordination, and Connectivity

Communications, Coordination, and Connectivity encompasses the challenges that result from information exchange across all levels of government, the information flow that supports decision-makers, and the electronic means by which information is shared. Communications, coordination, and connectivity issues probably present the greatest challenges when responding to a mass casualty incident, especially one involving WMD. During the FSE, several challenges emerged in these three dimensions of information exchange. A lack of coordination was the primary communication challenge observed during the FSE.

Significant findings from the FSE include the following:

- There were numerous instances when participants experienced difficulties obtaining or validating information. In the absence of a commonly understood process for official notifications, agencies had difficulty confirming the status of the HSAS Threat Level for

several hours. Also, agencies spent substantial time confronting rumors regarding, among other misinformation, transportation closures, patient numbers in both venues, and casualty figures at the RDD scene. Some agencies attributed these problems to too many official reporting channels, where various agencies exercised not only their own independent procedures but also redundantly requested updates from agencies;

- Inconsistent language was another communication challenge during the FSE. In Washington State, confusion arose as many participants interchangeably used the term *casualties* to mean *fatalities* or *injured people*, or both. Similarly, the nonspecific references to plague in internal agency communications resulted in at least one instance when a public health person gave advice that applied to Bubonic Plague rather than Pneumonic Plague;
- Officials also remarked on the critical importance of having technical data translated into non-technical language to support decision-making and risk communications;
- Data collection and coordination issues challenged both the Washington and Illinois venues. In Washington, the primary coordination challenges involved the collection and reporting of radiological ground data and the apparent lack of a unified command structure during the early stages of the response at the RDD site. In Illinois, the greatest coordination challenges involved the collection of information and the data flow requirements among the 64 hospitals, the five POD hospitals (the five lead hospitals for coordinating disaster medical response in a specific region upon activation of the emergency medical disaster plan by Illinois Operations Headquarters and Notifications Office (IOHNO)), and three separate but interrelated statewide organizations: Illinois Department of Public Health (IDPH), IOHNO, and the Illinois State Emergency Operations Center (EOC);
- The FSE provided opportunities for participation from some organizations not typically included in a response, and also encouraged some organizations to participate in new ways. For example, the American Red Cross participated in the Federal Joint Operations Center (JOC) and Bank of America co-located an EOC with the Federal Reserve. Further, participants reported that the T2 building-block process was extremely valuable in helping them to develop new or stronger relationships with their colleagues at all levels; and
- Connectivity challenges impacted the ability of technical experts, agencies, and jurisdictions to communicate effectively. Hospitals and the medical system lack robust Internet-based communications systems in many cases and overwhelmingly rely on phones and faxes for transmitting and tracking critical patient and resource information which is extremely inefficient. In Illinois, organizations reported their fax machines were unreliable due to mechanical breakdowns and an inadequate number of staff to monitor them. Also some machines were reported to be in locked rooms. Likewise, the lack of verified phone numbers caused communication delays while emergency personnel spent critical time looking for the correct numbers to report emergency data. In Washington, the Department of Health Radiation Monitoring and Assessment Center (RMAC) and FRMAC experienced significant connectivity challenges that impacted their ability to distribute data and data products, respectively, to decision-makers, subject matter experts, and responders.

D. Jurisdiction

Jurisdiction encompasses the issues, conflicts, or gaps in authorities and the assumptions that may arise when policies and agreements are put into practice under the uniquely challenging conditions of a terrorist WMD attack. The FSE demonstrated that jurisdictional policies and the extent to which they are understood by various entities drive and influence every element of response. Participants at all levels of government continue to state that exercises such as TOPOFF remain one of the most effective means to explore the operational implications of these jurisdictional policies and refine authorities that may appear clear on paper but which lack clarity when implemented under the complex conditions of a disaster.

Significant findings from the FSE include the following:

- Throughout the T2 cycle, the primary jurisdictional question evolved from "who is in charge" to "who is in charge of what." During the FSE, there was some confusion with the multiple, and sometimes overlapping, authorities that were driving the disaster response. For example, in Illinois there were many discussions concerning the jurisdiction over the decontamination process and the facilities where the biological agent was released (the United Center, O'Hare International Airport, and Union Station). Similar questions arose in the Washington venue regarding the management of the long-term impacts of the radiological contamination;
- The FSE provided an opportunity to explore jurisdictional issues involving DHS. For example, there was uncertainty between the Transportation Security Administration and the Federal Aviation Administration regarding the authority to close and reopen airspace and issue temporary flight restrictions. Issues also arose regarding the activation, requests for, deployment, and distribution of the SNS, where both HHS and DHS are involved in these processes. Furthermore, questions arose regarding the relationship between HHS and DHS during a Public Health Emergency, and how expertise and health and medical assets—which are now split between DHS and HHS—are used and managed. The FSE helped to highlight areas where the role of the PFO as it relates to FEMA officials needs additional clarification. Lastly, the Environmental Protection Agency noted the need to clarify its authorities relative to DHS, specifically noting development and maintenance of health and safety plans; and
- The authority to release information can be especially problematic when a disaster crosses jurisdictional boundaries, as was the case during the FSE with both the RDD and bioterrorism attacks. Organizations at State and local levels repeatedly expressed concerns about Federal organizations releasing information that the State and local organizations believed they should have released instead.

E. Resource Allocation

Resource Allocation encompasses the challenges that require decision-makers to weigh conflicting needs and determine how best to allocate limited resources. Conflicting resource needs can challenge decision-makers within a single agency, or can force decision-makers from different agencies and departments to work together under stressful and time-constrained conditions to decide how best to manage critical resources that are in short supply. Often the solution requires individuals and organizations to use unconventional methods.

While the scenario did not fully stress the Washington venue resources and the FSE ended before the number of plague patients overwhelmed the Chicago area medical and public health capabilities, a number of resource allocation issues and "best practices" emerged.

Significant findings from the FSE include the following:

- State and local participants were often not aware of which Federal resources were available and how to access them. State and local emergency managers and responders would benefit from an "Emergency Response Knowledge Base," or Procedural Flow, that described all Federal assets, helped State and local officials identify those assets that would best meet their needs in an emergency, and explained how to request the response assets;
- A "one stop shop" for tracking the status of Federal assets that have been activated or deployed during an emergency does not exist. FEMA currently tracks and reports the usage of Federal assets in a disaster through its Mission Assignments and Situation Reports, but distribution of these reports is fairly inefficient. A Web-based, searchable knowledge base of all available Federal resources and their status (potentially expanded to include State and local resources) may be helpful in this regard, particularly when resources are stressed;
- Having a contingency plan for the receipt and distribution of the SNS contributed to a fairly smooth-running process in Illinois. In contrast, shipment and distribution of the National Pharmaceutical Stockpile (the previous name for the SNS) did not transition as smoothly in the TOPOFF 2000 exercise. In part, this reflects the tremendous investments in planning and preparedness that have occurred in State and local public health departments since the fall of 2001;
- Participants utilized unconventional strategies to meet resource demands. They did this by relying on unconventional sources of support and by intervening with executive orders that exempt individuals from repercussions that were often legal and which would otherwise prevent them from providing services; and
- Decision-makers anticipated future demand. In Washington, several assets were placed on standby in case they were needed at another incident site. Illinois emergency managers and public health officials developed a plan to deal with the limited supply of medication and anticipated potential hospital surge requirements that the growing epidemic would require. In Washington, D.C., the DHS Emergency Preparedness and Response Directorate worked on a plan to distribute the SNS to other states that requested it, recognizing the inevitable spread of Pneumonic Plague cases outside Illinois.

F. Anticipating the Enemy

Anticipating the Enemy encompasses the unique considerations that influence decision-making when there is a potential enemy threat. The existence of an enemy makes the response to a terrorist attack qualitatively different from the response to any natural or conventional disaster. For example, the desire to keep the terrorists from gathering information regarding response plans works against the desire to keep the public informed.

Significant findings from the FSE include the following:

- There were a number of responder and top official activities that demonstrated a keen awareness of potential follow-on attacks. In Washington, the National Guard Civil Support Team was released from the incident site in part so that they would be available to redeploy in the event of another terrorist attack. In the Chicago area, authorities increased surveillance and decreased parking and deliveries at likely terrorist targets after the RDD explosion in Seattle. At the interagency venue, HHS, DHS, the Centers for Disease Control and Prevention, and others gave considerable thought to the need to reserve the SNS and other resources, specifically mentioning that Chicago might not be the only city to have been attacked with Pneumonic Plague;
- Many agencies stated that they either were not playing against an enemy or that it was the responsibility of others (e.g., the Federal Bureau of Investigation (FBI) and the JOC) to consider the enemy. However, when participating in a response, agencies should be aware that their responders are at risk. The loss of responders in additional attacks could seriously impair an agency's response capability, not to mention how such a loss would impact the morale of other responders and the public at large; and
- While an active opposing force, known as a Red Team, was limited in scope during the FSE, even its limited presence was beneficial to employing a more robust Red Team in future exercises.

VII. Exercise Design and Conduct Lessons Learned

The T2 AAC attendees and exercise participants identified several lessons learned relating to exercise design and conduct. Considerations for developing the following areas may benefit the success of succeeding TOPOFF Exercises: 1) planning and participation, 2) exercise artificiality, 3) scenario scripting, 4) the role the Virtual News Network (VNN), 5) a functional Web-based control capability, and 6) exercise security.

Other considerations worth investigating are the intelligence development and management processes, the guidelines for producing and publishing exercise documents, the standards for determining official exercise time, and methods for empowering the venue design and coordination teams.

VIII. Conclusions

T2 was an innovative, useful, and successful exercise built upon the accomplishments of TOPOFF 2000 and was the first national combating terrorism exercise conducted since DHS was established. As a result, T2 provided a tremendous learning experience for both the new DHS and the Federal agencies now working with DHS during a response to domestic incidents. In addition, the experience in Washington and Illinois provided important lessons regarding FSL integration. These lessons are valuable to other states and localities as they work to train, exercise, and improve their own response capabilities.

T2 involved the play of new agencies and entities within DHS (e.g., the Transportation Security Agency, the PFO, and the Crisis Action Team).

- The PFO concept was tested in both exercise venues. While this position has the potential to assist greatly with the coordination of Federal activities across the spectrum

of the response, T2 results also indicated that the roles and responsibilities of the PFO need to be clarified with respect to those of the FBI SAC, the FEMA RD, and the FCO. In addition, the PFO requires an emergency support team with the flexibility and expertise to provide support across the full range of homeland security operations.

T2 represented the first time (real or notional) in which the HSAS Threat Level was raised to Red.

- Valuable experience was gained as the Secretary of DHS, in concert with the Homeland Security Council, first raised selected areas of the country and then the whole country to Threat Level Red. In addition, local jurisdictions raised their own threat levels to Red.

T2 involved an extraordinary sequence of two Presidential Declarations wrapped around a Public Health Emergency declaration by the Secretary of HHS.

- The Presidential declarations were for a major disaster in the Washington venue and an emergency in the Illinois venue. These two declarations illustrated some of the subtleties of the Stafford Act that may not have been fully appreciated before the exercise; for instance, a bioterrorism attack does not clearly fit the existing definition of *disaster* as defined by the Act. The Secretary of HHS, acting on authorities through the Public Health Service Act and in consultation with the region, declared a Public Health Emergency. This permitted HHS to authorize the use of Federal assets (with costs covered by HHS).

Planning and development of the NRP and National Incident Management System should take advantage of the TOPOFF Exercise Series.

- Communication and coordination issues drove the course and outcome of critical public policy decisions, from raising the threat level to the various disaster/emergency declarations, and from the determination of exclusion zones to the reopening of transportation systems. To the extent that there were problems in these areas, communication issues were likely the primary cause; and
- T2 showed that how people believe communications and coordination should work as based upon policy is often not how they work in reality. What may appear to be clearly defined processes—such as requesting the SNS—in practice become much more difficult.

With the active participation of 64 hospitals in the Chicago area responding to the notional bioterrorism attack, T2 represented one of the largest hospital mass casualty exercises ever conducted.

- T2 represented a significant experiment in communications and coordination for the public health and medical communities. In particular, the massive amounts of communication required to track resource status (beds, specialized spaces, and medical equipment), and the cumbersome procedures and insufficient electronic means to do so in many cases, taxed hospital staff;
- T2 did not allow full exploration of the impacts of mass casualties on the medical system. Much less than half of the infected population was visible to the medical system at the conclusion of the exercise; and

- While there were a number of attempts to estimate the potential scope of the outbreak, the focus of most activities appeared to be on the cases that were presented to the health care system. It should be noted that HHS was working actively during the FSE to identify the resources that would be required to deal with the infected population.

T2 Illinois play also involved an extensive SNS request and distribution component.

- Although the actual distribution process appeared to go quite well, there was some confusion over the procedures and processes for requesting and receiving the SNS. The SNS Operations Center coordinated the stockpile deployment through the FEMA Emergency Preparedness and Response Director. Additionally, senior-level consultation occurred between DHS and HHS via Video Teleconference and direct communication; and
- The jurisdictions in the Chicago area were forced to confront important decisions about how the stockpile (and local assets) would be divided and who would be among the first population groups to receive prophylaxis. The discussions and decision-making involved, as well as the challenges in coordinating public information, are worthy of study by other metropolitan areas for the lessons they provide.

DHS should consider the integration of existing response policies and plans into the NRP.

- States are familiar with and have built their response plans to coincide with Federal assets and plans using similar agency and department structures and language;
- Federal agencies are satisfied with the language, authorities, and relationships outlined in existing plans such as the Federal Radiological Emergency Response Plan and the Federal Response Plan; and
- As the NRP undergoes development, the integration of response plans and policies merit consideration—particularly where existing plans are considered effective for emergency response.

T2 involved more intense and sustained top officials play than occurred during TOPOFF 2000.

- Of particular note was the involvement of DHS (which had been in existence for only a little more than ten weeks prior to the exercise), the DHS Secretary, and other senior civilians;
- HHS operated the Secretary's Command Center for 24 hours per day throughout the exercise with extensive play at the Assistant Secretary- and Operating Division Director-levels. The Secretary was actively involved, and since one venue involved substantial public health and medical play, the active participation of HHS was critical to the success of the exercise; and
- In both Washington and Illinois, the offices of the mayors, county executives, and governors were well-represented throughout the exercise by either the elected officials themselves or high-level policy-makers in respective administrations. In particular, the Mayor of Seattle participated substantially in the FSE, providing local top leadership that greatly contributed to the realism of play and to a greater appreciation of the local challenges and perspectives in a national WMD incident.

T2 represents a foundational experience to guide the future development of the TOPOFF Exercise Series.

- Because of the extensive data collection process and the effort to make T2 findings both well-documented and traceable through a detailed reconstruction of the exercise events, T2 represents a baseline upon which subsequent TOPOFF exercises can build and to which they can be rigorously compared;
- T2 demonstrated the value of the international, private sector, and nonprofit perspectives and roles in response to WMD terrorism. Future exercises will, no doubt, expand upon these elements by broadening the participation of all these sectors;
- Red Team activities during T2 provided ground rules for the involvement of a simulated active enemy threat in future exercises. This play should also be expanded in future exercises, as it represents one of the fundamentally different challenges responders face in a terrorist WMD disaster relative to any natural or conventional disaster; and
- The success of the VNN and widespread participant feedback regarding the desire for additional challenges in the area of public information suggest that future exercises should include a more aggressive mock-media element with a more aggressive news-gathering function that includes mock-press conferences.

This page intentionally left blank

PARTICIPATING AGENCIES LIST

United States Federal Departments and Agencies
American Red Cross (ARC)
Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)
Centers for Disease Control and Prevention (CDC)
Defense Threat Reduction Agency (DTRA)
Department of Agriculture (USDA)
Department of Defense (DoD)
Department of Energy (DOE)
Department of Health and Human Services (HHS)
Department of Homeland Security (DHS)
Department of Housing and Urban Development (HUD)
Department of Justice (DOJ)
Department of Labor (DOL)
Department of Navy (DON)
Department of the Interior (DOI)
Department of State (DOS)
Department of Transportation (DOT)
Department of Veterans Affairs (VA)
Environmental Protection Agency (EPA)
Federal Bureau of Investigation (FBI) – Critical Incident Response Group (CIRG)
FBI – WMD Countermeasures Unit
Federal Aviation Administration (FAA)
Federal Emergency Management Agency (FEMA)
General Services Administration (GSA)
Institute for Security Technology Studies (ISTS)
Joint Forces Command (JFCOM)
National Aeronautics and Space Administration (NASA)
National Imagery and Mapping Agency (NIMA)
National Reconnaissance Office (NRO)
National Security Council (NSC)
National Weather Service (NWS) (Department of Commerce)
Nuclear Regulatory Commission (NRC)
Occupational Safety and Health Administration (OSHA)

United States Federal Agencies and Organizations (Continued)
Postal Inspection Service (U.S. Postal Service [USPS])
Small Business Administration (SBA)
Social Security Administration (SSA)
Technical Support Working Group (TSWG)
Transportation Security Administration (TSA)
U.S. Coast Guard (USCG)
U.S. Customs Service (USCS)
U.S. Geological Survey (USGS)
U.S. Secret Service (USSS)
Canadian Agencies
Agriculture and Agri-Food Canada (AAFC)
British Columbia Ministry of Health EOC (BCMOH)
British Columbia Provincial Emergency Program (BCPEP)
Canadian Coast Guard (CCG)
Canada Customs and Revenue Agency (CCRA)
Canadian Food Inspection Agency (CFIA)
Canadian Nuclear Safety Commission (CNSC)
Canadian Security Intelligence Service (CSIS)
Citizenship and Immigration Canada (CIC)
Department of Justice (DOJ)
Department of Defense (DoD)
Department of Foreign Affairs and International Trade (DFAIT)
Environment Canada (EC)
Health Canada (HC)
Industry Canada (IC)
Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)
Privy Council Office (PCO)
Public Works and Government Services Canada (PWGSC)
Royal Canadian Mounted Police (RCMP)
Solicitor General (SGC)
Transport Canada (TC)

State and Local Agencies
American Red Cross of Greater Chicago (ARCGC)
Chicago Department of the Environment (CDOE)
Chicago Department of Public Health (CDPH)
Chicago Fire Department (CFD)
Chicago Office of Emergency Management and Communications (OEMC)
City of Bellevue
Cook County Sheriff's Office (CCSO)
Cook County Sheriff's Office Emergency Management Agency (CCSO EMA)
Cook County Department of Public Health (CCDPH)
DuPage County Office of Emergency Management (DCOEM)
DuPage County Health Department (DCHD)
Illinois Department of Public Health (IDPH)
Illinois Emergency Management Agency (IEMA)
Illinois Hospital Association (IHA)
Illinois Office of the State Fire Marshal
Illinois State Fire Chiefs Association
Illinois State Police (ISP)
Illinois Commerce Commission (ICC)
Illinois Department of Transportation (IDOT)
Illinois Department of Human Services (IDHS)
Kane County Office of Emergency Management (KCOEM)
Kane County Health Department (KCHD)
King County Fire Chiefs Association (KCFCA)
King County Government (KCG)
King County Office of Emergency Management (KCOEM)
King County Police Chiefs Association (KCPCA)
Public Health – Seattle and King County
Lake County Emergency Management Agency (LCEMA)
Lake County Health Department (LCHD)
Lake County Fire Department Specialized Response Team
Metropolitan Chicago Healthcare Council (MCHC)
Office of the Governor of the State of Illinois
Office of the Governor of the State of Washington
Office of the Mayor of the City of Chicago

State and Local Agencies (Continued)
Office of the Mayor of the City of Seattle
Port of Seattle
Seattle Fire Department (SFD)
Seattle Emergency Management (SEM)
Seattle Police Department (SPD)
Washington State Department of Agriculture (WSDA)
Washington State Department of Ecology (WSDE)
Washington State Department of Health (WSDH)
Washington State Department of Information Services (WSDIS)
Washington State Department of Transportation (WSDOT)
Washington State Emergency Management Department (WSEMD)
Washington State Ferries (WSF)
Washington State Patrol (WSP)

This page intentionally left blank

Top Officials (TOPOFF) Exercise Series:

TOPOFF 2 (T2) After Action Report

Prepared for
U.S. Department of Homeland Security
Office for Domestic Preparedness
by AMTI and the CNA Corporation
Under Schedule Number GS-10F-0324M,
Order Number 2003F028

This page intentionally left blank

TABLE OF CONTENTS

ADMINISTRATIVE HANDLING INSTRUCTIONS

1. The title of this document is *Top Officials (TOPOFF) Exercise Series: TOPOFF 2 (T2) After Action Report.*

2. This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate Canadian, U.S. Department of Homeland Security (DHS), U.S. Department of State (DOS), the State of Illinois, the State of Washington, and local/city security directives. This document is marked For Official Use Only ~~(FOUO),~~ and information contained herein has not been given a security classification pursuant to the criteria of an Executive Order, but this document is to be withheld from the public because disclosure would cause a foreseeable harm to an interest protected by one or more FOUO exemptions.

3. Reproduction of this document, in whole or in part, without prior approval of DHS is prohibited.

4. DHS, Office for Domestic Preparedness (ODP), and DOS, the Office of the Coordinator for Counterterrorism, cosponsored the T2 Exercise Series. Mr. Theodore Macklin (b)(6) (b)(6) and Mr. Corey Gruber (202-514-0284) are the ODP Points of Contact (POCs) and (b)(6) (b)(6) the Office of the Coordinator for Counterterrorism, is the POC for international play.

5. This report is intended for the use of Federal, State, and local (FSL) officials responsible for homeland security. It is intended to improve the FSL plans to prevent and respond to weapons of mass destruction by understanding the lessons learned from T2.

This page intentionally left blank

I. INTRODUCTION

Top Officials (TOPOFF) 2 (T2) was a congressionally-directed, national combating terrorism exercise. It was designed to improve the nation's domestic incident management capability by exercising the plans, policies, procedures, systems, and facilities of Federal, State, and local (FSL) response organizations against a series of integrated, geographically dispersed terrorism threats and acts. The T2 exercise was co-sponsored by the U.S. Department of Homeland Security (DHS), Office for Domestic Preparedness (ODP), and the U.S. Department of State (DOS), Office of the Coordinator for Counterterrorism.

A. T2 Goals

T2 was driven by four overarching national goals:

- To improve the nation's capacity to manage complex/extreme events;
- To create broader operating frameworks of expert domestic incident management and other systems;
- To validate FSL authorities, strategies, plans, policies, procedures, protocols, and synchronized capabilities; and
- To build a sustainable, systematic exercise process for advancing domestic preparedness.

As one of the first major projects within DHS, T2 brought together extensive inter-governmental and international participation. The U.S./Canadian aspect of T2 was designed to increase coordination and communication in response to a weapons of mass destruction (WMD) incident.[1] This cross-border play focused on several bi-lateral goals:

- To improve U.S. and Canadian top officials' understanding of the international implications of a multi-faceted WMD terrorist incident;
- To improve top officials' capability to respond in partnership to the crisis and consequence management aspects of a WMD terrorism incident;
- To build a sustainable U.S./Canadian joint exercise program in support of bi-lateral preparedness and response strategies for WMD terrorism incidents;
- To assess and strengthen partnerships between all organizations, including non-traditional partners, involved in responding to a WMD terrorism incident to improve overall crisis and consequence management capabilities;
- To exercise and assess Federal, State/Provincial, and local crisis and consequence management plans, directives, and processes for addressing cross-border WMD terrorism incidents; and

[1] Analysis of international aspects of T2 and U.S./Canadian play during the Full-Scale Exercise is provided in *Annex B* of this report.

- To conduct a joint exercise in accordance with the U.S./Canadian Smart Border Declaration and U.S./Canadian Chemical, Biological, Radiological, and Nuclear (CBRN) Guidelines.

B. T2 Open Exercise Design and Concept

The first TOPOFF exercise (TOPOFF 2000) was a single, no-notice, Full-Scale Exercise (FSE) co-chaired by the Department of Justice (DOJ) and the FEMA in May 2000. Unlike TOPOFF 2000, T2 was designed as an "open" exercise in which participants were introduced to the exercise scenario prior to the FSE through a cycle of exercise activity of increasing complexity that included:

- A series of seminars exploring acute response issues;
- The Large-Scale Game (LSG) that explored mid- and long-term recovery issues;
- An Advanced Distance Learning Exercise (ADLE) which used satellite networks to support first responder training nationwide;
- A Top Officials Seminar designed to explore top official response to terrorism incidents involving WMD; and
- An FSE that allowed top officials to join all players in response to a simulated terrorist attack with a radiological dispersal device (RDD) in Seattle, Washington and a simulated, deliberate release of Pneumonic Plague (*Yersinia pestis*) at several locations in the Chicago, Illinois, metropolitan area.

The purpose of the open exercise design was to enhance the learning and preparedness value of the exercise through a "building-block" approach, and to enable participants to develop and strengthen relationships in the national response community. Participants at all levels have stated that this was of enormous value to them.

C. Significant Aspects of T2

The T2 exercise was much more than a large-scale, WMD training exercise for civilian agencies; as the name *TOPOFF* denotes, a major component of the exercise was the involvement of top officials. The top officials playing in T2 included elected officials, such as governors and mayors, as well as non-elected officials who are at the apex of homeland security decision-making: cabinet members and other agency heads at the Federal level; police, fire, emergency management, and public health chiefs, among others, at the local level; and the directors of statewide agencies, including state police and the National Guard. The top officials were involved not only for their own learning but also to make possible realistic multi-government-level play. At the T2 After Action Conference (AAC), DHS Secretary Tom Ridge stated that the Homeland Security Council, which met repeatedly during the FSE, "dramatically increased its awareness of the nature and complexity of top-level issues related to terrorist attacks."

> *The TOPOFF process…provides the nation an architecture upon which terrorism preparedness responsibilities can be played out, tested, and evaluated.*
> ~DHS Secretary Tom Ridge

The following developments made the T2 FSE a significant national event:

- It was the first national exercise conducted since the establishment of DHS;
- It was the largest peacetime terrorism exercise ever sponsored by DHS or DOS;
- It involved the play of DHS and the new agencies and entities within DHS, such as the Transportation Security Agency, the Principle Federal Official (PFO), and the Crisis Action Team (CAT), as well those outside of DHS, such as the Department of Health and Human Services (HHS) Secretary's Emergency Response Team (SERT);
- It represented the first time—both real and within an exercise—that the Homeland Security Advisory System (HSAS) Threat Condition was raised to Red;
- It represented one of the largest mass casualty exercises to incorporate hospital play[2]; and
- It involved intense and sustained top official play.
- It introduced the concept of a live opposing force (OPFOR) in a national exercise which established ground rules for the involvement of a simulated active enemy threat in future exercises.
- It expanded the use of sophisticated news reporting simulation through the use of the Virtual News Network (VNN).

As a result, T2 provided an unmatched opportunity to examine domestic incident management policies, procedures, and systems, as well as an opportunity to review critical communication and coordination issues as they have evolved since TOPOFF 2000, the terrorist attacks of 9/11, and the anthrax attacks during the fall of 2001. Therefore, the results and findings of this exercise will allow agencies and organizations at all levels of government to identify problems and develop solutions. At the AAC, DHS Secretary Tom Ridge underscored the success of the T2 model as "a proven framework for bringing together all elements of DHS" and designated the TOPOFF Exercise Series as the lead exercise within DHS.

D. Overview of the AAR

This After Action Report (AAR) provides the results of the FSE analysis, and integrates the findings from pre-FSE seminars and the LSG.[3] The *Background* section provides a history of the exercise scenario and a brief description of findings from TOPOFF 2000, other exercises, and real-world events that have influenced both the design and evaluation of T2. It also outlines the exercise evaluation methodology, focusing in particular on how the events of the FSE were reconstructed and analyzed. The *Reconstruction* section summarizes exercise events in the Washington and Illinois venues as well as interagency play in Washington, D.C.[4] The next section details exercise *Artificialities*. The *Special Topics* section examines a set of events or issues (such as the elevation of the HSAS to Red) that have special significance to the response community and which fall outside of or have substantial overlap between the six, pre-determined areas of analysis. The *Analysis of the Six Core Areas* discusses the overarching issue areas identified from a review of TOPOFF 2000 and other exercise findings, FSL agency objectives for T2 submitted prior to the FSE, and real-world events such as 9/11. Included in this section is

[2] Sixty-four hospitals actively responded to the notional bioterrorism attack in the Illinois venue and 16 hospitals responded to the radiological event in the Washington venue.
[3] The findings from the seminars, the large scale game, and the ADLE were published previously.
[4] A searchable, detailed reconstruction of events from the WA, IL, and Interagency venues is provided in Annex A.

a summary of how the findings from the seminars and the LSG relate to the conclusions drawn from the analysis of the data collected during the FSE. The next section provides *A Comparison of T2 to TOPOFF 2000*. Lessons learned from the design and conduct of the exercise are described *Exercise Design and Conduct Lessons Learned*. In the final section of this report are the *Conclusions* drawn from the *Special Topics* and *Analysis of the Six Core Areas*.

During the FSE, DHS and DOS invited representatives from the Stanford University Center for International Security and Cooperation Institute for International Studies to observe activities in Washington, D.C.; and the Washington State and Illinois venues. Their report is included as an appendix to *Annex B*.

Two other exercises were conducted simultaneously to the T2 FSE: the TOPOFF 2 CyberEx and The National Capital Region Functional Exercise (NCRFE). The CyberEx was a functional exercise intended to examine, in an operational context, the integration of inter- and intra-governmental actions related to a large-scale cyber-attack synchronized with a terrorist WMD attack against a major urban area of the United States. The NCRFE was designed to coincide with the FSE to assist the National Capital Region jurisdictions in assessing their preparedness and coordination in response to a general attack on the nation and changes to the HSAS Threat Condition. The AAR for the CyberEx can be found in *Annex C*, and the NCRFE AAR in *Annex D*.

This AAR, along with its annexes, is designed to support the accomplishments of the exercise series goals and objectives and to provide an accurate and comprehensive portrait of the exercise conditions. The data contained within the main body of this report encompasses the direct observations of nearly 800 FSE data collectors, and the evaluation team's analysis of that information, as well as input from official FSL participants.

II. BACKGROUND

Understanding the concept driving Top Officials (TOPOFF) 2 (T2) requires a description of the Public Laws Authorizing the TOPOFF Exercise Series; Federal, State, and local (FSL) agency objectives for T2; TOPOFF 2000; related real-world events (such as the attacks of 9/11, the follow-on anthrax attacks, and other terrorist incidents); the T2 building block events; and the exercise scenario. It is also imperative to understand the evaluation methodology used to achieve the findings from the data collected during the Full-Scale Exercise (FSE).

A. Public Law Authorizing the Top Officials Exercise Series

Public Law 106-553 authorized T2, and Senate Report 106-404 outlined the concept:

> *The Committee believes that **the nation will benefit from regular exercises**. In order to ensure that the collective national preparedness, as tested for the first time by TOPOFF, is continuously improved and departments and agencies know their roles and responsibilities, (...) **national-level exercise series shall be instituted**.*
>
> *This series of exercises, capitalizing on the lessons of TOPOFF, **should include a regularly scheduled sequence of increasingly challenging exercise building-blocks**. (...) It will feature the participation of key top officials at the Federal, State, and local levels. (...) This series of exercise components will also improve "crisis resistance" through opportunities to measure plans, policies and procedures required to (to provide an) effective response to a WMD terrorist incident. (...)*
>
> *T2 (...) **will support the national strategy to combat terrorism**, and include events that assess the Nation's crisis and consequence management capacity. It will include the involvement of Federal, State, and local top officials. The lead agency for T2 will be the Department of Homeland Security, and the exercise will be designed, developed and executed by Department of Homeland Security (DHS), Office for Domestic Preparedness (ODP)*[5].

T2 supported the National Security Council's Policy Coordinating Committee on Counter-terrorism and National Preparedness Exercise Sub-group requirement for a large-scale, counterterrorism exercise commencing in 2002 and finishing in 2003.

Homeland Security Presidential Directive (HSPD)-5 articulates the federal incident management policy that guided the T2 exercise. HSPD-5, in part, states:

> *To prevent, prepare for, respond, to, and recover from terrorist attacks, major disasters, and other emergencies, the United States Government shall establish a single, comprehensive approach to domestic incident management. In these efforts, with regard to domestic incidents, the United States Government treats*

[5] The T2 effort was initiated under the auspices of the Office of Domestic Preparedness (ODP) formerly part of the Department of Justice. ODP was later transferred to DHS when it was established.

crisis management and consequence management as a single, integrated function, rather than two separate functions. The Secretary of Homeland Security is the Principle Federal Official for domestic incident management.

B. Overview of Federal, State, and local Agency Objectives for T2

Participating FSL agencies were asked to submit objectives to T2 planners at the start of the exercise design cycle to ensure the exercise design would support participant objectives while also addressing national priorities. Agency objectives covered such areas as unified command, mutual aid, law enforcement investigation, mortuary services and fatality management, public information/education, surveillance, and epidemiology, among numerous others.[6] Figure 1 demonstrates that the FSE design, as documented and executed through the Master Scenario Events List (MSEL), largely addressed FSL agency objectives. These objectives were linked to MSEL items (defined by participating agencies and described in the T2 Exercise Plan (EXPLAN)). Those objectives for which the associated MSEL item took place during the FSE are noted in the figure as being "addressed at least once," during FSE play. Those for which the associated MSEL item did not take place are noted as "possibly not addressed" during FSE play.[7]

[6] A detailed list of these objectives is provided as an appendix to the T2 Exercise Plan (EXPLAN).

[7] The word "possibly" is used because just because the associated MSEL item did not occur does not necessarily mean the objective was not addressed. Each agency has determined whether its objectives were accomplished and has documented this in their respective AARs.

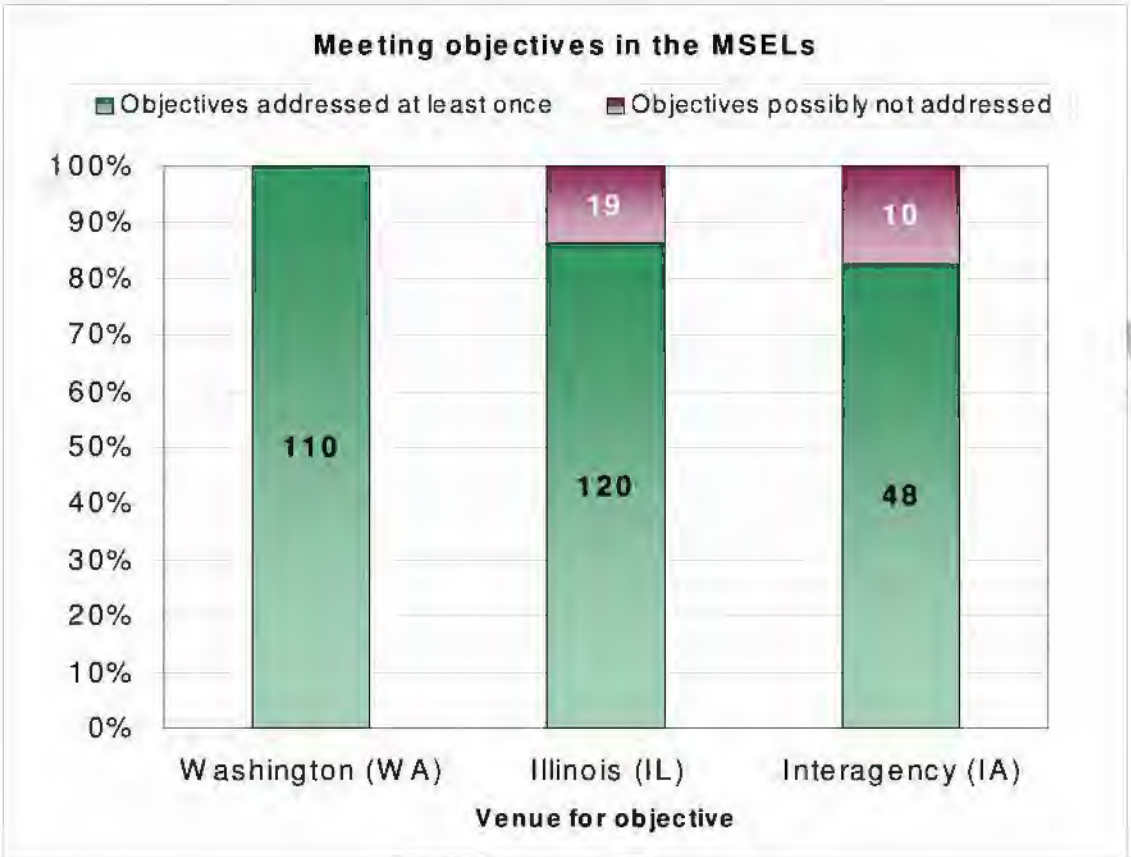


Figure 1. FSE Addressed FSL Objectives

C. TOPOFF 2000

Like T2, TOPOFF 2000 involved simulated terrorist attacks against two metropolitan regions: a chemical attack in Portsmouth, New Hampshire, and an intentional release of pneumonic plague in Denver, Colorado. Executed during May 2000, the TOPOFF 2000 FSE pre-dated the terrorist attacks of 9/11.

There were eight principle observations drawn from TOPOFF 2000:[8]

- Multiple direction and control nodes, numerous liaisons, and an increasing number of response teams complicated coordination, communications, and unity of effort;
- Threat information and a common "threat picture" were not shared or coordinated in a timely manner;
- Collaboration and methodologies in coordinating and sharing WMD hazard information and analysis need to be strengthened;
- Educating, exercising, and equipping crisis and consequence managers and responders remained a national priority need;

[8] *TOPOFF 2000 Exercise Observation Report*, page EX-17.

- The response to a large-scale bioterrorism incident was significantly different from response to other WMD;
- The fragility of the public health infrastructure, reluctance to invest heavily in preparing for a low probability event, and shortfalls in current bioterrorism preparedness increased the reliance on leadership, effective response, and information management at the federal level;
- The respective and compassionate management of contaminated human remains, including legal requirements, evidentiary controls, and evidence collection, and their ultimate disposition required concerted analysis and planning; and
- The importance of joint public affairs in a WMD incident could not be overstated. The interagency public affairs community needed to continue to demonstrate an increasing capacity for joint public affairs following a WMD incident.

The success of TOPOFF 2000 was instrumental in obtaining continued funding for conduct of suhsequent TOPOFF exercises. While the intent was to conduct a no-notice exercise, Congress realized the value of a building-block approach to preparedness and instructed TOPOFF planners to develop a series of exercise activities of increasing complexity. Many elements developed in TOPOFF 2000, such as the Virtual News Network (VNN), were retained and expanded for T2. TOPOFF 2000 participants initiated numerous corrective actions based upon the lessons of the exercise, and these were evident in the management of the events surrounding 9/11 and the anthrax attacks, as well as during the T2 FSE.

D. Related Real-World Events

1. 9/11

The events of 9/11 affected T2 planning, which was in the preliminary stages when the attacks occurred. In the aftermath of 9/11, the President created the Office of Homeland Security, and the Administration and Congress subsequently established DHS. Though planning for T2 was well underway by the time DHS was established, the participation of the new department became imperative, as many of the exercises' objectives centered around determining how existing procedures would he changed by a DHS-managed, federal response to incidents involving WMD.

2. Anthrax

The attacks of 9/11 were followed by mail-based anthrax attacks. These attacks served to underscore and reinforce some of the TOPOFF 2000 observations listed above in the *Background* as well as the need to exercise the nation's bioterrorism response.

3. Other real-world events

In June 2002, Attorney General John Ashcroft announced that Jose Padilla, also known as Ahdullah al Muhaji, had heen arrested in May, at Chicago's O'Hare International Airport, on suspicion of both association with the terrorist organization Al Qaeda and plotting with Al Qaeda to detonate a radiological dispersal device (RDD) somewhere within the United States.

In early 2003, the Department of Health and Human Services (HHS) began a nationwide program to administer smallpox vaccinations to healthcare workers.

E. The T2 Building-Block Events

It is important to understand that the T2 design involved a conscious decision to provide participants full access to the exercise scenario. This choice was made so that the scenario could he used in the T2 building-hlock events preceding the FSE and also to emphasize the learning process of T2.[9]

The building-block events began with the first T2 seminar, *Public Communications during a WMD Incident*, which was conducted in McLean, Virginia, from July 17 to 18, 2002. The seminar focused on both the issues that affect a government's abilities to communicate effectively with the public either directly or through the media, and also on the decisions that must be made to ensure that appropriate messages are delivered in a coordinated and timely way.

The second seminar, *National Seminar on Bioterrorism*, was held in Northbrook, Illinois, from September 17 to 18, 2002. This seminar brought together homeland security functional area leaders from FSL departments and agencies, as well as the Canadian government, to discuss issues involved in response to an unprecedented contagious bioterrorism attack.

A third seminar, *National Seminar on Radiological Dispersal Device Terrorism,* was held in Seattle, Washington, from October 16 to 17, 2002. The seminar was designed to both identify critical issues facing FSL, private sector, and international officials and also resolve key issues faced in such an attack prior to the FSE. The seminar explored how FSL and international responders prepare for the unique problems created by an RDD scenario and the best approaches to resolve these issues. The participants were from U.S. Federal departments, Canadian agencies, and State and local emergency response agencies from Illinois and Washington.

The *National Direction and Control Seminar* was conducted in conjunction with the *Advanced Distance Learning Exercise* (ADLE), which employed distance education technology to disseminate information and provide interactive training opportunities. Overall, the seminar provided an interactive forum for discussing the nation's capacity to direct and control crisis and consequence management of complex terrorist events. ADLE viewers were given the opportunity to pose questions to seminar panel members through the DHS, Office for Domestic Preparedness' Extranet Secure Portal (ESP) website.

The T2 Large-Scale Game (LSG) was developed to improve the nation's ahility to manage the long-term consequences of a terrorism attack. It focused on the mid- to long-term issues that challenge FSL and international top officials and responders in the unprecedented event of a dual radiological and contagious bioterrorism attack. Participants included senior officials from U.S. FSL departments and agencies, as well as representatives from the Canadian Government.

The lessons learned from these seminars can be found in the after action reports posted on ODP's Extranet Secure Portal (ESP).

The *Top Officials Seminar* brought together Cabinet-level officials from 25 agencies and departments in a round-table discussion that served as preparation for the T2 FSE through an

[9] While the scenario was widely known, the Master Scenario Event List (MSEL) which actually drove exercise play, was closely held and not provided to participants.

exploration of inter-governmental domestic incident management in response to WMD terrorist attacks on the United States.

The T2 FSE was played out from May 12 to May 16, 2003. The information contained within this document reconstructs and analyzes the FSE and provides recommendations for refining future operations of integrated domestic incident management.

F. Exercise Scenario

The T2 exercise scenario depicted the fictitious, foreign terrorist organization GLODO[10] detonating an RDD in Seattle and releasing the Pneumonic Plague in several Chicago metropolitan area locations. There were also significant pre-exercise intelligence play, a cyber-attack, and credible threats against other locations. Key events in the exercise scenario are briefly described Table 1.

The Homeland Security Advisory System (HSAS) national threat level was notionally raised from Yellow to Orange before the FSE on D-6 in response to credible intelligence reporting suspected threat activities.

The scenario was designed to demonstrate the tiered approach to a WMD response:

(1) Local first responder capabilities,

(2) State emergency management capabilities,

(3) State National Guard capabilities,

(4) Lead Federal Agency response, and

(5) Title 10 military support.

In the RDD scenario, the explosion took place in the Seattle, Washington, and the city was the first to respond. Seattle then called in state resources, followed by federal resources where necessary. It was not designed to require usage of Title X resources, but nonetheless demonstrated the value of the tiered response.

On D-2 in the Chicago metropolitan area, the plague agent was notionally released at three separate locations: 1) O'Hare International Airport, 2) Union Station, and 3) the United Center. Multiple people were infected at each site. Some of the plague victims watching a Chicago Blackhawks versus Vancouver Canucks hockey game at the United Center subsequently traveled to Canada.

On D-Day, the start of the FSE (STARTEX), the RDD was detonated in Seattle, killing a small number of individuals, injuring a larger number, and scattering radioactive materials around the bomb site and over a broad area as the material was transported by the wind.

On D+1, the number of admissions to Chicago metropolitan area hospitals made it clear that a major disease outbreak had begun both in the United States and in Canada (most notably in Vancouver, home of the Vancouver Canucks hockey team). By the end of D+1 a clinical diagnosis of Pneumonic Plague was made.

On D+2, with positive laboratory identification of the plague, counties in the Chicago metropolitan area mobilized their own pharmaceutical stockpile resources for distribution to the

[10] The acronym for the fictional *Group for the Liberation of Orangeland and the Destruction of Others.*

local first responder community personnel. Subsequently, the Strategic National Stockpile (SNS) was mobilized, arriving in Chicago at the reception site at O'Hare International Airport.

On D+3, the SNS was deployed from O'Hare International Airport to five distribution sites within the Chicago metropolitan area.

Table 1. Overview of Scenario

EXERCISE DAY	WASHINGTON VENUE	ILLINOIS VENUE
D-6	• Increase in hostile cyber-activity • Threat condition elevated from yellow to orange	
D-5	• Cyber-attacks by GLODO sympathizers	
D-4		
D-3	• Credible threat against Columbia Generating station	
D-2		• Covert release of biological agent in the Chicago metropolitan area
D-1		
D-Day	• Truck bomb explosion in Seattle • Radioactive material confirmed • Terrorist Radiological Dispersion Device event declared	• Initial patient presentation
D+1	• Safehouse takedown[11]	• Recognition of patient increase • Clinical diagnosis of plague • SNS request • National Disaster Medical System activated • Epidemiological investigation underway
D+2	• Marine takedown11 • Command Post Exercise	• Lab confirmation • Establish Joint Information Center (JIC)/Joint Operations Center (JOC) and Regional Operations Center (ROC) • SNS breakdown • Illinois WMD Team Takedown11 • Overwhelming #s patients
D+3	• Tabletop Exercise (Consequence Management)	• SNS distribution begins • Midway Airport event11 • Takedown in Chicago11 • Overwhelming #s patients
D+4	• Hotwash	• Hotwash

[11] These events were walled from the evaluation team, and therefore are not discussed in much detail in this AAR.

G. Evaluation Methodology

This section provides an overview of the T2 FSE evaluation methodology.[12] The process by which the exercise was reconstructed and analyzed is given special attention. The T2 evaluation goals were to 1) help agencies understand domestic incident management and WMD-related issues and develop solutions, and 2) support the establishment of a model for continuous learning.

These goals are consistent with the T2 national goals and those of the T2 domestic venues. As such, the evaluation methodology focused on decision and coordination processes that support the nation's top officials and the broader system of FSL agencies. Rather than evaluating participant ability and performance or specific agency-by-agency objectives, the evaluation methodology employed a detail-oriented data collection effort to reconstruct T2 exercise events followed by an analysis focusing on six pre-selected areas of analysis:

1. **Emergency Public Policy and Decision-making** encompasses the unique challenges, difficulties, and nuances faced by top officials in the initial aftermath of a terrorist WMD attack. These differ from those of natural disasters or accidents and from normal day-to-day operations.
2. **Emergency Public Information** encompasses the unique public information challenges and implications faced by top officials and their support staff in the midst of a terrorist attack involving WMD, which may differ from that of normal day-to-day operations.
3. **Communications, Coordination, and Connectivity** encompasses the challenges of exchanging information across all levels of government, information flows supporting decision-makers, and the electronic means by which information is exchanged.
4. **Jurisdiction** encompasses the issues, conflicts, or gaps in authorities and the assumptions that may arise when policies and agreements are put into practice under the uniquely challenging conditions of a terrorist attack involving WMD.
5. **Resource Allocation** encompasses the issues involving the allocation of scarce resources, as well as the management of resources committed during the response to a terrorist attack involving WMD..
6. **Anticipating the Enemy** encompasses the unique considerations that influence decision-making when there is knowledge of a potentially active enemy threat.

The After Action Report (AAR) also includes the analysis of several special topics. These topics represent events that attracted particular interest during the FSE and crossed multiple areas of analysis.

Evaluation of the FSE consisted of a three-step process:

Step 1: ***Observation and data collection*** during the exercise.

Step 2: ***Reconstruction*** of events and activities.

Step 3: ***Analysis*** of what happened in the exercise and why, in terms of the special topics and the six core areas.

[12] A detailed presentation of the methodology can be found in the Exercise T2 Evaluation Plan (EVALPLAN).

This methodology was intentionally structured not to evaluate player performance. Instead, the purpose was to deliver knowledge to players so that they, and non-participating agencies nationwide, can improve or create FSL policies and procedures based upon the lessons of T2.

1. Observation and data collection

T2 involved an aggressive data collection strategy.[13] Hundreds of data collectors and controllers in the field collected data. Other data were obtained by collecting the paperwork (e.g., duty logs) kept by some players in the course of executing their duties, by having a central point to which T2-related e-mails were to be sent, and by asking controllers—especially those in the control cells—to turn in their notes. In addition, the T2 evaluation team collected feedback from players at all levels of government through the use of player feedback forms. A key element in all this data-collection was time: each observation was annotated with a time at which players recorded it to have occurred. An unprecedented volume of data was collected during the course of the FSE, and was thus a tremendously successful aspect of T2.

2. Reconstruction

T2 analysts collected and organized the data submitted by players, data collectors, and controllers to use in the reconstruction and analysis of FSE play. Figure 2 illustrates the reconstruction process. Analysts reviewed data from play sources (data collected through the course of T2 play) and control sources (data collected through T2 controllers) for each venue and highlighted data points that could support analysis of what happened and why during the exercise. Play data included logs kept by players during the course of the FSE, player feedback forms, e-mails, and data collector logs. Control data, which documented the occurrence of MSEL items and ad hoc injects during play, included field controller logs, as well as data collected in the Master and Venue Control Cells during the course of the FSE.

The evaluation team received data from numerous FSL agencies and non-government organizations. These include: The Center for Disease Control and Prevention, Department of Energy, Environmental Protection Agency, Federal Bureau of Investigation, Federal Emergency Management Agency, Federal Radiological and Assessment Center, Food & Drug Administration, Department of Heath and Human Services, Department of Homeland Security, Department of Housing and Urban Development, National Oceanographic and Atmospheric Administration, Nuclear Regulatory Commission, Occupational Safety and Health Administration, Department of Transportation, U.S. Coast Guard, U.S. Marshals Service, Department of Veterans Affairs, State of Illinois Emergency Operations Center (EOC), Illinois Department of Public Health, Illinois Operations Headquarters and Notifications Office, Illinois Joint Operations Center, Chicago Metropolitan Area EOCs and Public Health Departments, participating Chicago Metropolitan Area hospitals, State of Washington EOC, Washington State Department of Health, Washington Joint Information Center, Washington Joint Operation Center, Seattle and King County EOCs, Public Health Seattle/King County, Seattle Police and Fire Departments, participating Seattle and King County hospitals, and the American Red Cross.

Where applicable, analysts tagged the data collected at the FSE, and from venue Hotwashes, the After Action Conference (AAC), agency AARs, and post-FSE interviews with exercise

[13] Also described in detail in the T2 Evaluation Plan (EVALPLAN).

participants, for instances of potentially good practices[14] or challenges in the *Six Core Areas of Analysis* and the *Special Topics*. The data were then entered into two distinctive databases for each venue: one containing the electronic record of play data tagged for the six core areas, the special topics, and artificialities; one containing the electronic record of control data (see #2 in Figure 2). The play database totaled more than 20,000 lines of data for the Washington, Illinois, and Interagency venues. The control database equaled the length of the MSEL and ad hoc injects, but also documented varying controller inputs on the times events took place.

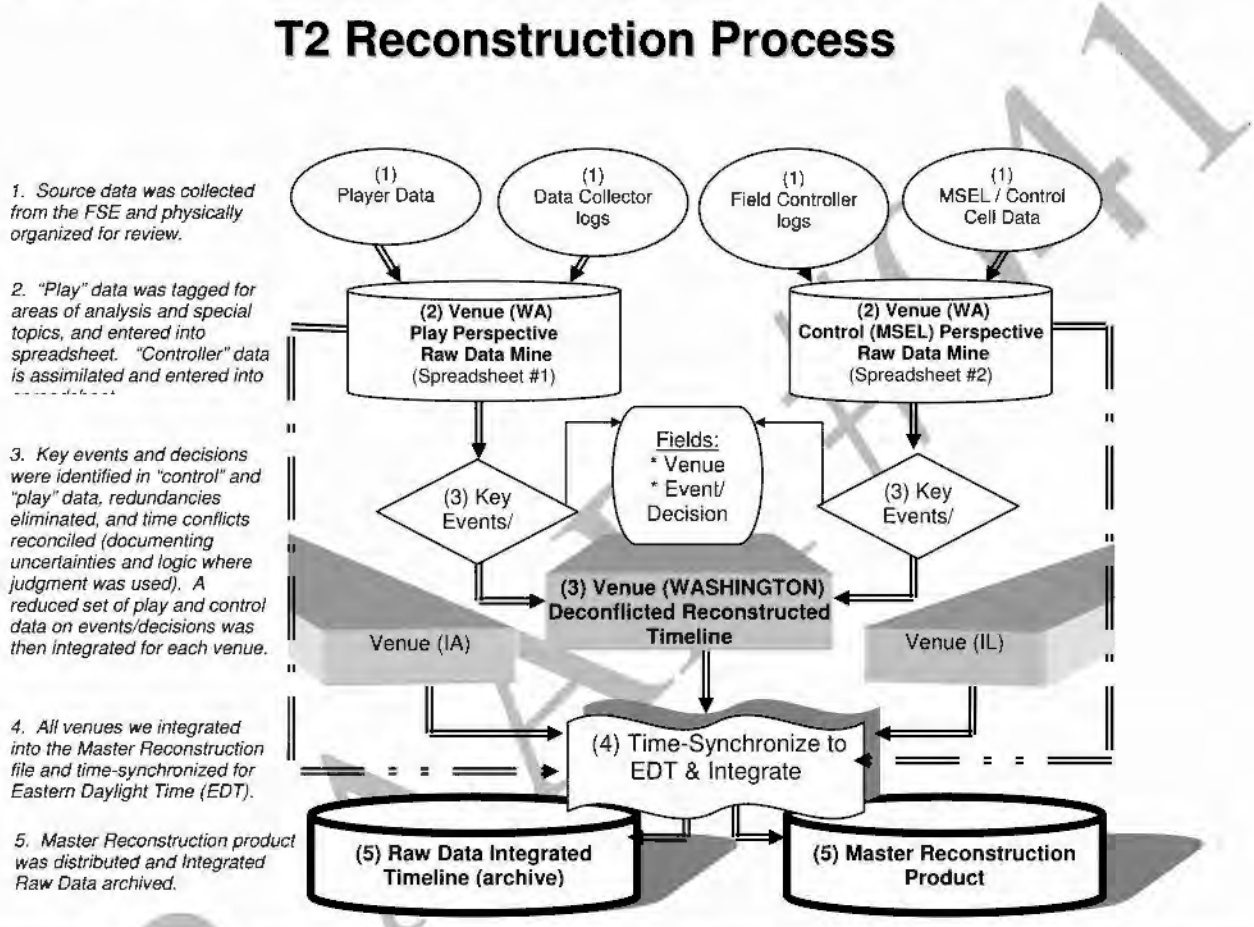


Figure 2. T2 Reconstruction Process

The analysts then reviewed the databases for each venue and identified decisions and significant events that occurred during the exercise from both the play and control data sets (see #3 in figure 2). The purpose was to filter out the innumerable events and decisions that participants faced on a daily basis, and to identify only those events that triggered top official decisions or actions.

For each data point identified as a significant event or decision, analysts researched the data to create a thorough event or decision description. For example, from one data point that read, "Susan approved the release," analysts were able to deduce from other data points recorded during relative time frames that Susan was from the Washington State Emergency Operations Center and approved a press release announcing the re-opening of local highways. Using this

[14] "Good" indicates that the intent ultimately is to objectively validate it as a "best" or "exemplary" practice.

process, analysts created a comprehensive list of significant events and decisions that participants experienced during the two scenarios that were played out in the Washington and Illinois venues during the FSE. This comprehensive listing of significant events and decisions was then transferred to a new worksheet, which became the foundation for the reconstructed timeline for each specific venue.

As part of this research, analysts reviewed the various times that were noted in all the data gathered from players, controllers, and data collectors for each given event or decision and then reconciled differences. In some cases, participant records indicating when events or decisions occurred varied by hours. The analysts used their judgment to determine the most reasonable time to assign to an event when data was not available. For example, if eighty percent of people recorded an event occurring at 0900 CDT then the analysts went with the time reflected by that eighty percent and only noted the outlying times. Likewise, if accounts of when an event occurred were equally distributed with no indication of an authoritative time, the analyst determined the average of the times. Despite widely varying accounts of when an event occurred, in some cases—such as the time of the RDD explosion in Seattle—the actual time is known because it was controlled; therefore, the actual time is entered and its basis documented. The specific times for events or decisions are less important in the overall reconstruction effort than the overall sequence and flow of events. The purpose of the reconstruction is to provide an objective context for the analysis and to provide a resource to FSL agencies that describes the types of events or decisions agencies could expect to face in real-world responses to the types of terrorist WMD attacks depicted in T2.

Once the event/decision descriptions were complete and the times were reconciled for each venue, the reconstructed timelines for each venue were combined into one master reconstruction file and sorted by date and time to produce a fact-based, integrated, reconciled, objective, meaningful timeline of events for the FSE. This timeline is the basis for the analysis presented in the AAR, and is the timeline provided as *Annex A*.

3. Analysis

The analysis process is depicted in Figure 3. Analysts consulted the play and control databases, as well as inputs from participants obtained through the player feedback forms, the Hotwashes, the AAC, and Lessons Learned reports submitted by agencies during the analysis process. The AAC was designed to allow participants and planners to provide additional input to the analysis process. For each special topic (described in more detail below), analysts consulted the collected data to create a more detailed reconstruction of events and decisions occurring within that topic's frame of reference. Analysts identified and analyzed the artificialities that impacted play in these topic areas, weaving the varied, distributed, and complex pieces of each dynamic response into a single unified story. In many cases analysts followed up with participants through phone calls and emails to clarify the data collected during events, decisions, and artificialities. To lay a foundation for development of objective qualitative and quantitative measures in the future as well as lessons-learned and best practices, the analysts identified instances of good practices or challenges in the six core areas in each special topic, reviewed additional instances that were not tied to special topics, and identified findings across the exercise

T2 Analysis Process

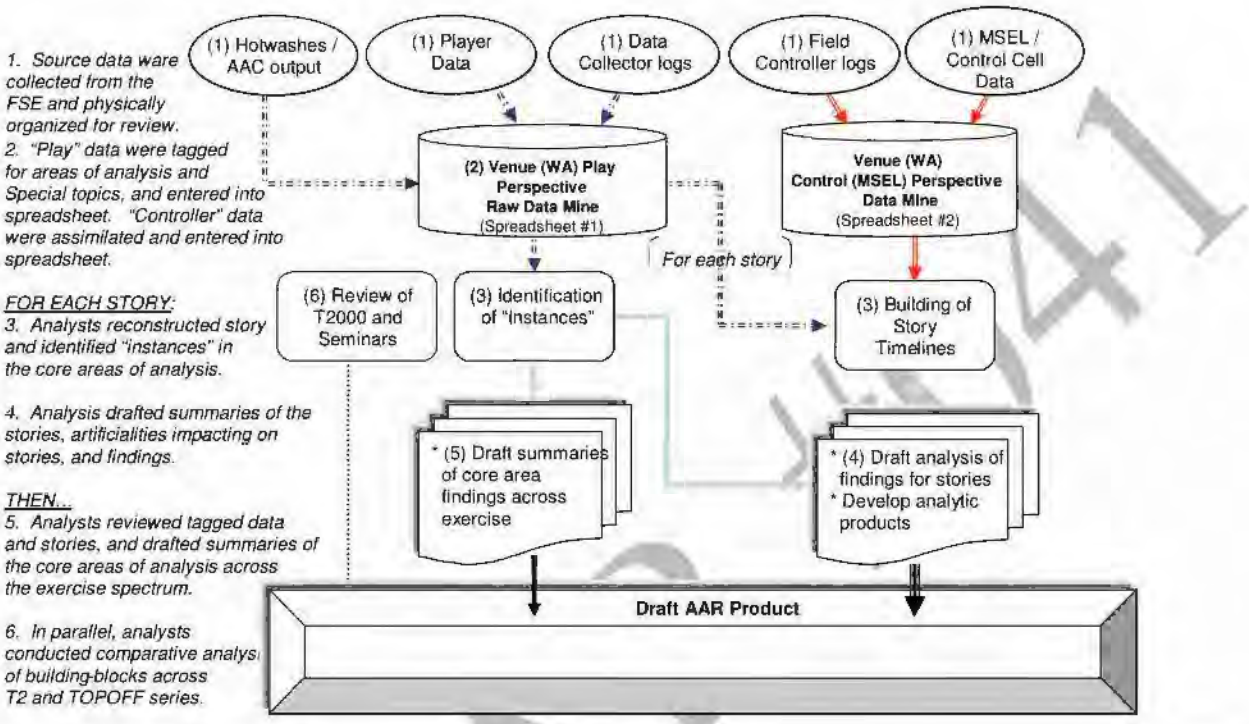


Figure 3. T2 Analysis Process

III. RECONSTRUCTION OF THE FSE

The purpose of the reconstruction was to establish an objective, fact-based timeline of the events that unfolded during the Full-Scale Exercise (FSE) as the foundation and context for analysis. The complete Top Officials (TOPOFF) 2 (T2) reconstruction product is the result of reviewing approximately 400 data collector and controller logs; thousands of player feedback forms and participant logs; many CD-ROMs; more than 2,500 emails; and hundreds of Master Scenario Events List (MSEL) items. These data sources were compiled into a spreadsheet amounting approximately 20,000 lines of data. The spreadsheet was then sorted by time, taking account each venue's specific time zone, and decisions and events were identified and filtered for redundancy.

This reconstruction, and therefore the rest of this report, does not include certain T2 activities that were partially or totally fenced off from both the analysts' view and from other events in the exercise. These include various force-on-force takedown drills; a cyber-attack exercise (CyberEx), the After Action Report (AAR) from which is published in *Annex C*; and some branch or sequel activities taking place wholly inside Canada and the National Capital Region. Furthermore, this report does not include significant data on international or Canadian play, which were collected and analyzed by the Department of State (DOS) evaluation team, the results of which are published in *Annex B*.

The activities described in this reconstruction took place in three different time zones.[15] To report all in terms of their Eastern Daylight Time (EDT) equivalents would force readers with a Washington or Illinois perspective to adjust their venue's institutional memory or records with EDT; it might also distort the connotations borne by certain times (e.g., those participating in the very early hours, and those that come at the end or beginning of the workday, or at a shift change). Yet the goal is to create a unified timeline of events. Accordingly, events are presented in the order in which they happened, but narrated in terms of the local times applicable in each venue.

Events that transcended particular time zones, such as Virtual News Network (VNN) broadcasts that were seen everywhere simultaneously, are given EDT times.

It is important to distinguish between events that were physically executed in the exercise and those that were done notionally. The physical activities involved:

- Participating top officials, and those top officials who were represented by somebody else;
- Participating agencies' personnel, numbering in the thousands;
- The more than one hundred "injured" persons in Seattle, represented by role players, and augmented by a few mannequins;

[15] Seattle is in the Pacific time zone; Chicago in the Central time zone, and the Washington, DC-based Interagency venue is in the Eastern time zone.

- The hundreds of role players acting the parts of the Chicago Metropolitan area patients, augmented by paper patients; and
- VNN broadcasts.

While these parties' actions were affected to some degree by exercise artificialities, they were real in the exercise sense that somebody physically participated and performed an action or actions, thereby encountering some semblance of realistic time delays, possibility of errors, and the issues that real operations entail.

All else—the closures of highways, airports, and ferry systems; orders to the population to shelter-in-place, elevations of the Homeland Security Advisory System (HSAS) Threat Condition; the spread of Pneumonic Plague outside the Chicago metropolitan area; etc.—was done in a purely notional sense. Also, all requests for emergency powers, changes of alert status, and so on were granted only on an exercise basis.

What follows is a reconstruction summary in a tabular format to lend context to the analysis. The table format affords the reader with the ability to view the events of one venue against the context of the others. Specific times are indicated based upon the data. They are provided not for the purpose of pinning events or decisions down to the exact minute, since the vast volume of data and multiple observer/participant accounts do not allow for such precision, but rather to illustrate the overall sequence of key events and decisions. Acronyms are not spelled out in the table for abbreviated readability, but all may be found in the Acronym Guide provided as a glossary to this AAR.

A complete, searchable reconstruction product is provided in *Annex A* to this AAR. It enables agencies or other interested readers to understand exactly what happened in T2, and more importantly—what types of activities and decisions one could expect to encounter in a radiological dispersal device (RDD) or bioterrorism attack from various perspectives and all government levels.

Table 2. T2 Summary Reconstruction

D-Day, Monday, May 12

TIME	WASHINGTON	ILLINOIS	INTERAGENCY AND FOREIGN
1200-1300 PDT 1400-1500 CDT 1500-1600 EDT	Bomb blast in Seattle. Seattle EOC activates to Level III. Washington EOC activates and notifies FEMA Region X ROC. Seattle HAZMAT, responding to blast, detects radiation. FBI JOC stands-up and investigation imitated.	Illinois EOC activates Chicago EOC activates	HHS receives message traffic from DHS, reporting the presence of Pu 229, Ce 137, and other radioactive materials in the bomb.[16] HHS reacts by officially activating the Region X REOC and sending the SERT there. SNS Operation Center activated.
1300-1400 PDT 1500-1600 CDT 1600-1700 EDT	Air, rail, highway, and ferry closures in Seattle area. Seattle and King County announce Red Alert status. Discussions of plume modeling and shelter-in-place begin. Washington requests DOE RAP assistance	Chicago increases security at likely terror targets.	DEST deployed (actually, redirected) to Seattle.
	Rumors of National, National Capital Region, and Chicago transitions to HSAS level Red abound.		
1400-1600 PDT 1600-1800 CDT 1700-1900 EDT	Seattle implements shelter-in-place, declares State of Emergency. Governor declares State of Emergency, activates National Guard. FRMAC requested. Second bomb identified on-site. FBI HMRU arrives on-site	Lake County EOC activates. Hospitals alter command relationships. Governor increases security at nuclear power plants. DuPage County EOC begins 24-hour staffing.	DOE sends Prussian Blue to Seattle. Deputies meet 1700; Principles meet 1730.
1600-1700 PDT 1800-1900 CDT 1900-2000 EDT	Stafford Act 401 request by Governor of Washington for Declaration of Major Disaster. Shelter-in-place declared	RDD info faxed to hospitals by Chicago Department of Public Health. Public transit stepped up. Four SARS-like patients coughing up blood arrive at Edward Hospital in DuPage County.	
1700-2100 PDT 1900-2300 CDT	Port to Marsec 3 per USCG. DEST and PFO arrive. AMS conducts survey. FRMAC arrives		
2000-2400 EDT	DHS Secretary declares HSAS Red for Seattle, Los Angeles, San Francisco, Houston, Chicago, New York, and Washington, D.C.		

[16] Knowledge of Pu 229 as part of the RDD this early in the exercise is an artificiality. It was not definitively identified by radiological experts in Washington State until late on May 12, 2003.

Morning of D+1, Tuesday, May 13

TIME	WASHINGTON	ILLINOIS	INTERAGENCY AND FOREIGN
2100-2400 PDT 2300-0200 CDT 0000-0300 EDT	Formulation of plans to evacuate workers and businesses west of I-5 from shelter-in-place and re-open highways. Rubble pile declared clear. Transition RDD site from rescue site to crime scene.	First Pneumonic Plague case suspected.	
0000-0300 PDT 0200-0500 CDT 0300-0600 EDT		More apparent cases of pneumonic plague. CDC EIS team on-scene.	British Columbia CDC confirms Pneumonic Plague.
0300-0500 PDT 0500-0700 CDT 0600-0800 EDT	Debate over I-5 re-opening. Evacuation of workers and businesses west of I-5 begins. Ferries resume service except to Seattle.	SERT to increase disease surveillance.	HHS orders SERT to increase surveillance.
0500-0700 PDT 0700-0900 CDT 0800-1000 EDT	Recovery and Restoration Task Force appointed. Presidential Declaration of Major Disaster approved.	Public Health Emergency Phase I activated. Phase I automatically includes Activation of POD hospitals.	
		HHS/SCC holds conference call with Region V (Chicago) to discuss biological event.	
0700-0800 PDT 0900-1000 CDT 1000-1100 EDT	State disagrees with Mayor on re-opening I-5.	Illinois Dept. of public health conference call on clinical picture of disease. Hospitals start to see connection to United Center, O'Hare International Airport, Union Station, and Canada. VNN reports flu-like illnesses in Vancouver.	DOS stands up liaison with Canada. Border security heightened - decontamination concern. Canadians intercepting Seattle flights for possible decontamination.
	False rumors of National transition to Red Alert status abound.		
0800-0900 PDT 1000-1100 CDT 1100-1200 EDT	FDA to announce embargo on foodstuffs. Americium 241, plutonium 238, and cesium 137 confirmed in RDD. Problems with plume, road re-opening, and evacuation of those sheltering-in-place.	Chicago Public Health proposes to identify travel history of all Pneumonic Plague patients. JIC press release announces plague confirmation.	CDC Director warns against over-commitment to Seattle and Chicago. EST Level I activation
		SNS readied for release to Chicago area.	
0900-1000 PDT 1100-1200 CDT 1200-1300 EDT		United Center-Blackhawks-Vancouver connection deduced.	
	Authorities strive to get accurate counts of victims.		
	Secretary of DHS gives threat update to nation via VNN, confirms terrorist attack in Seattle.		

Afternoon of D+1, Tuesday, May 13

TIME	WASHINGTON	ILLINOIS	INTERAGENCY AND FOREIGN
1000-1100 PDT 1200-1300 CDT 1300-1400 EDT	FBI investigation of crime continues. FRMAC beginning to develop long-term assessment and monitoring plan with EPA and HHS. Disagreements over need for, and utility of, Prussian Blue in combating radiation.	Environmental samples taken at O'Hare, Union Station, and United Center. IDPH Lab confirms plague bacterium samples from patient. Governor declares State of Emergency and requests activation of the SNS. IDPH declares Phase II Public Health Emergency to ensure authorization of certain emergency procedures Emergency. Lake County declares disaster.	State Department standing up JTF w/ CAN to work border and flight issues. Need to inform receiving countries that there may be a health problem in Chicago. HHS ASPHEP suggests plague was intentionally released, and suggests a look at the ventilator situation.
	VNN has DHS Secretary in telephone interview. He announces preliminary diagnosis of flu-like symptoms as "plague." VNN asks him what people in Code Red cities should do. Secretary articulates "snowday" concept.		
1100-1200 PDT 1300-1400 CDT 1400-1500 EDT	Teams of specialists search rubble.	Governor advised to request a National Medical Disaster System to get Federal assistance; mobilizes IEMA. Port of Chicago closed.	
1200-1400 PDT 1400-1600 CDT 1500-1700 EDT	Agricultural precautions announced. Detailed plan developed for shelter-in-place zone: those east of I-5 are released; those remaining west of I-5 to be evacuated.	Chicago and Cook County sign joint Declaration of Emergency..	CDC confirms plague. All NDMS response teams been activated for possible deployment. DHS Secretary recommends lifting transportation restrictions on airports and ferries in WA; HHS, DOE, EPA agree.
1300-1500 PDT 1600-1700 CDT 1700-1800 EDT		O'Hare International Airport closed (except to receive SNS). No school in Chicago.	HHS Secretary declares a public health emergency in the City of Chicago, allowing the department to provide Federal health assistance under its own authority.
	In press conference, DHS Secretary announces HSAS Red for entire Nation; plague in Illinois		
1500-1600 PDT 1700-1800 CDT 1800-1900 EDT	Shelter-in-place zone gradually being downsized.	Governor of Illinois sends letter to the President through FEMA Region V Regional Director requesting Major Disaster Declaration. All water, air, bus, rail, interstate traffic curtailed.	
1600-2200 PDT 1800-2400 CDT 1900-0100 EDT	King County announces implementation of snow-day like regime without specifically identifying or using the term "snow day." I-90 is open; I-5 open to through traffic.	FBI investigation initiated..	DHS/EPR/FEMA Headquarters recommends to DHS Secretary and the President that an Emergency Declaration be made in Illinois rather than a Major Disaster Declaration.

Morning and afternoon of D+2, Wednesday, May 14

TIME	WASHINGTON	ILLINOIS	INTERAGENCY AND FOREIGN
2200-0600 PDT 0000-0800 CDT 0100-0900 EDT		Steep rise in respiratory cases showing up at hospitals. Question arises as to whether pending local declarations are necessary given the IL Governor's declaration of a State of Emergency.	FEMA conference call with Regions to discuss numerous State inquiries regarding SNS push packages. TSA/FRA/STB conflict over authority to shut down rail traffic.
	DHS Secretary goes on VNN and confirms the disease outbreak as plague, with a terrorist origin.		
0600-0800 PDT 0800-1000 CDT 0900-1100 EDT		IDPH director authorizes distribution of drugs to first responders. National Disaster Medical System (NDMS) requested. Governor recommends that non-essential workers stay home and that public gatherings be cancelled. Counties declare emergency and "snow day." Plague's origin at O'Hare, Union Station, and United Center confirmed. DuPage County begins distribution of its pharmaceutical stockpile to first responders	
0800-0900 PDT 1000-1100 CDT 1100-1200 EDT	SeaTac, King County, Renton, and Paine Field airports re-opened with restrictions.	Governor suspends HIPPA, Blood Bank Act, and EMS Act, [Hospital] Licensing Act, and confidentiality of health statistics. SNS lands at O'Hare.	
0900-1000 PDT 1100-1200 CDT 1200-1300 EDT	City confronts problem of contaminated fire engines and police cars.	DMORT arrive at Hines VA Hospital. Eighteen hospitals at maximum capacity. Persons who have been at one of three epicenters advised to get prophylaxis. FBI JOC opens.	
1000-1200 PDT 1200-1400 CDT 1300-1500 EDT	USCG/FBI takedown of terrorists. Shelter-in-place zone now evacuated, re-named "exclusionary zone," inasmuch as it has been fully evacuated. AMTRAK announces contamination of passenger rail cars. USCG lifts no-sail order. Misgivings and arguments over exclusionary zone; some want to expand it, others to end it, Little radiation data. Agricultural control areas and check-points established.	Presidential Declaration of Emergency approved. Concern about level of demand relative to antibiotic supply. Chicago Office of Emergency Management requests National Guard. Area counties and Chicago begin to receive and break down SNS shipments. Area State parks closed. Many hospitals have no beds and/or are locked down against crowds.	Canada says that they have quarantined all those on flight from Chicago that brought plague to Vancouver.
	Casualty estimates developed.		

Evening of D+2, Wednesday, May 14

TIME	WASHINGTON	ILLINOIS	INTERAGENCY AND FOREIGN
1400-1700 PDT 1600-1900 CDT 1700-2000 EDT	New radiological readings indicate that DOH may recommend re-closing I-5 and I-90. National Guard activates 500 troops to support law enforcement.	25 refrigerated trucks called up to be used as morgues. Counties begin prophylaxis of first responders.	
1700-2100 PDT 1900-2300 CDT 2000-2400 EDT		Some counties close dispensing down for the night. VMI begins arriving in-State.	

D+3, Thursday, May 15

TIME	WASHINGTON	ILLINOIS	INTERAGENCY AND FOREIGN
2100-0500 PDT 2300-0800 CDT 0000-0900 EDT	Transportation restrictions lifted except in vicinity of nuclear plant.	Public activities curtailed until at least 1800 PDT. Interstate transportation still closed. FBI takedown of terrorists and terrorist lab.	Defense coordinating officers deployed to Seattle and Chicago. Increased security on incoming containers.
0500-ENDEX PDT 0800-ENDEX CDT 0900-ENDEX EDT		All SNS distribution sites open to the public. Mixed messages as to who should seek treatment. Plague bacteria reported still present at the three suspected release sites. Mixed messages on re-opening of the release sites. Non-terrorist-related crash at Midway. FBI investigation continues to ENDEX.	DOE requests activation of the VA Medical Emergency Radiological Response Team (MERRT).
	Transition back to HSAS Orange, except for Chicago and New York City.		

This page intentionally left blank

IV. ARTIFICIALITIES

Artificialities are manifestations of the exercise's non-real nature. As such, they are unavoidable, and not indications of a problem. However, false conclusions can arise if their natures and effects are not appreciated. This section focuses on the key artificialities that need to he understood to draw the appropriate conclusions from the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE). Exercise artificialities are placed in three hroad categories:

- Those that are inherent to the exercise design process;
- Those specifically related to the T2 exercise design; and
- Those that arose during actual exercise play.

The net impact of artificialities can be difficult to assess. For example, considerations must be taken into account for questions such as *did a particular artificiality make the response decisions or actions easier than they might have been*, or *did they unnecessarily complicate the response relative to a real-world operation*? For their part, the T2 exercise designers tried to strike a halance, compensating for one artificiality (e.g., a response team's need, ahsent a real emergency, to take a commercial flight) with another (e.g., the same team's seemingly premature departure).

Two questions to ask when considering an exercise artificiality are:

- What difference did it make to the participants' play; and
- What difference did it make to top officials' play?

A. Inherent Exercise Design Artificialities

Artificialities surface in any exercise involving the response to a (WMD event. The fundamental issue is that it is often impossible to exercise the full scope of a real-world event—ranging from an actual bomb detonation to shutting down transportation infrastructure to commanding the full-time attention of top officials. The result is that many exercise events or actions must be notional, or simulated, instead of actual. Despite the notional character of some events, government agencies and organizations played as though the events actually took place. This allowed the T2 evaluation team to examine critical decision-making and communication issues. In summary, as long as they are understood and accounted for in the analysis process, these limitations need not have a significant impact on interpreting the results of the exercise.

1. Top officials' play

By any standard, top official involvement in T2 was extensive. But in a real-life emergencies of the same magnitude of those portrayed in T2 top officials would be immersed in coping with the emergency, almost to the exclusion of all other activities, wbereas even in T2, top officials were present only internittently and largely on a schedule. In fact, the ability to schedule top official play was one of the reasons for pre-scripting some aspects of the exercise. Top officials devoted considerable personal time to the exercise. Some also designated individuals (e.g., a deputy) to

play their parts in the game when they were not available. The T2 evaluation team believes that top official play during the FSE was, on the whole, relatively unaffected by these artificialities of scheduling, availability, and substitution.

2. Limited scope of play

Many effects associated with a radiological dispersal device (RDD) explosion and the intentional release of Pneumonic Plague were not designed into or played in the exercise. Some of the most important include:

- Transportation gridlock in both Chicago and Seattle;
- Increased security manpower requirements resulting from the attacks, as well as the elevation of the Homeland Security Advisory System (HSAS) to Red; and
- The potential for population disruption, movement, anxiety, and fear.

Many of these are nearly impossible to simulate or would have unacceptable impacts on non-exercise participants.

3. Notional actions

Because of limits on the scope of play, the most apparent artificialities were those in which notional (or constructive) actions replaced real ones. Examples include the notional closure of I-5 near the Seattle RDD site and the use of paper patients in the Chicago metropolitan area hospitals.

4. Limited public involvement

In a real event, the public reaction can include clamor for more information, crowds of people who have fled their homes, traffic jams, or disruptive reactions at top officials' public appearances. Although T2 had people to role play patients in the Chicago metropolitan area hospitals and persons injured by the blast in Seattle, the general public was minimally represented, so reactions on the part of the public simply did not occur.[17] Neither traffic jams nor public demonstrations would be feasible, from a practical standpoint. Inasmuch as these could have an impact on the top officials' decision-making, and perhaps even on the actions of emergency personnel at the scene, to preclude their existence was to introduce a necessary artificiality.

The Washington venue did have a shelter facility set up at the White Center (a county recreation facility), through which many people passed, and three other shelters (one in Seattle and two in King County) were operated on a constructive basis (i.e., no refugee role players), but these activities were scripted and did not entail the important aspect of responding to an emerging public reaction.

Many important considerations would include but not be limited to those regarding public information, heightened public anxiety, and other psychosocial factors. Such issues would expand beyond the immediate affected communities. For example, other cities in America, not coping with an on-going emergency, would look for guidance regarding what might later happen

[17] Public awareness of T2 in Seattle did result in some outcry, such as some threatening-looking signs, of which nothing ever came.

in their cities. The lack of involvement from 48 non-affected states and hundreds of non-affected cities is an artificiality that must be taken into account when considering national top officials play.

B. Artificialities Specific to the T2 Design Process

The artificialities in this section either represent deliberate choices made during the design of T2 or are specific to this particular exercise (as opposed to exercises in general). These choices were made with the understanding that they would have impacts on exercise findings. The T2 evaluation team believes that these impacts are accounted for in the exercise analysis.

1. The known scenario

T2 was designed as a building-block process whereby the general exercise scenario was explored in a series of seminars, a large-scale game, and an Advanced Distance Learning Exercise (ADLE). This process was designed to promote learning among the agencies and organizations involved in T2 and, indeed, participants felt that they had learned a great deal even without the benefit of the FSE. It is important to note, however, that while the scenario was known, participants were not afforded access to the Master Scenario Event List (MSEL), which drove the FSE play.

There was some post-exercise criticism in the media about the overly scripted nature of T2 and the lack of free play. However, this turns out to be largely unfounded criticism. Figure 4 compares the times at which events in the MSEL were supposed to occur versus when they actually occurred. The figure shows that there was a substantial amount of free play.

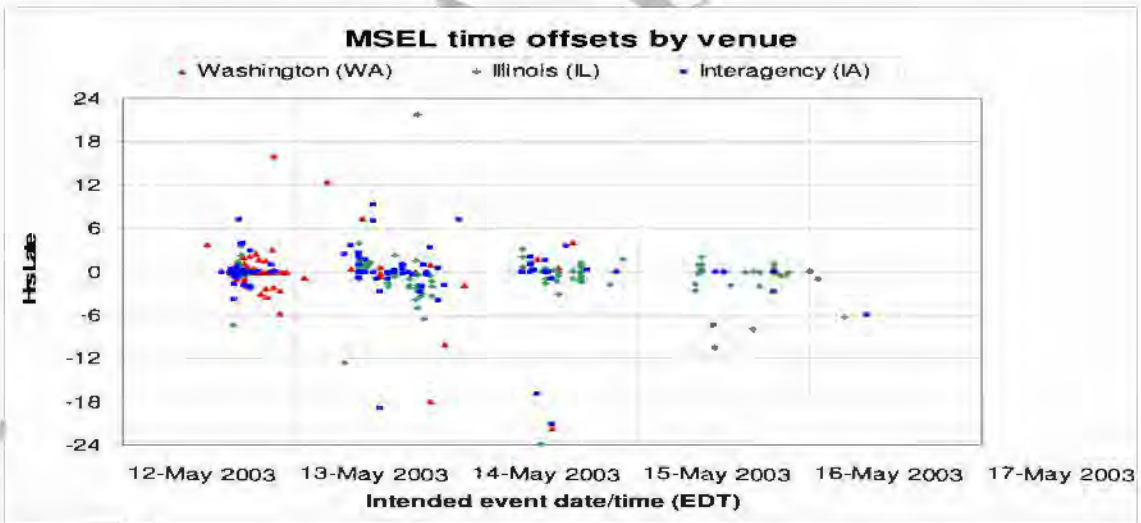


Figure 4. Variance of Events from MSEL Times

2. Scope of participation

A number of important organizations and governments were simulated. Two notable ones were the World Health Organization and the Government of Mexico.

3. VNN

Prior to the FSE, the Virtual News Network (VNN) staff and director repeatedly made the point that during the FSE VNN would be a reporter of the news, not a news-gatherer. But the full import of this policy was not clear to many until after the FSE was underway: prior to that time, some players appeared to assume that VNN would in some fashion seek out news, as well as report it.

VNN reporting was principally based upon assuming that MSEL events would happen as scheduled: reports (many of them included at the bottom-of-the-screen, known within the media as "crawlers") were put on screen straight from the MSEL, without any news-gathering to determine whether or not they had actually taken place. This practice resulted in at least one instance in which an event was reported before it actually took place.[18] Reactions to these events may have created some chains of anomalous events, but the effects do not appear to have been severe.

Some VNN coverage (e.g., some top officials' interviews) was by necessity pre-constructed and indicative of the MSEL, and thus did not accurately portray how the scenario was unfolding. Again, this style of coverage was completely consistent with VNN's prior self-characterization as "a news-reporting, not a news-gathering" organization.

Finally, the players—particularly those involved with Public Information—did not find themselves in a completely realistic media environment of reporters demanding the answers to questions. Only in news conferences did any such behavior occur, and even there it was not played to the degree of a real-world catastrophic event.

4. Spread of the Pneumonic Plague

Two key issues were not played in the T2 exercise: the actual epidemiological investigation required to pinpoint the location where individuals were initially infected and the impact of counter-measures (prophylaxis, population movement control measures) on the spread of the disease. In the former case, while the large number of infected individuals who attended a hockey game at United Center would have been a strong clue, the much smaller numbers infected at the transportation hubs could have been a greater challenge. In the latter case, the exercise ended before the counter-measures could have had their full impact on suppressing the transmission of the disease.[19]

The secondary population in a real epidemic largely consists of people who were in close contact with the primary population—family members, co-workers, and health care workers. In the T2 scenario, the secondary population was constructed on a geographical basis: the numbers of secondary cases in the Chicago metropolitan area and in the collar counties were proportional to the numbers of primary cases in each of those areas, but the association was no closer and the secondary population did not consist of close associates of the primary cases—family members, co-workers, health-care workers, and other first responders such as Emergency Medical Services workers.

[18] The RDD explosion itself was one such instance: it was scheduled for 1458 EDT (1158 PDT) in the MSEL, and VNN began to report on it at that time, but it did not actually occur until ten minutes later.

[19] At any rate, the exercise epidemiological profile was not developed to allow for the impact of counter-measures even if the exercise had lasted longer.

T2 did not have a tertiary population of cases, principally because the duration of the FSE was not as long as would have been needed for a set of tertiary cases to incubate and be present. Were a tertiary population to have been played, the secondary population role of healthcare workers would have been of the greatest importance, since this large secondary population would he important to spread of disease to the tertiary population. To the degree that the disease would have been spread within the population of healthcare workers, it takes a double toll, by increasing the population of the sick and decreasing the population of those able to care for them.

5. The radiological dispersal device and Seattle weather

Real radioactive materials were not released in the exercise. For the emergency workers to be able to respond realistically to readings from their instruments, these readings had to be pre-determined according to what the radiation levels would be, as functions of time and space, had an actual RDD been detonated. To predetermine these levels required atmospheric dispersion models (see also the description of these in the *Special Topics* section) to run in advance, which in turn required planners to make up weather prior to the FSE. FSE play was based upon this simulated weather rather than the weather that Seattle would actually experience on May 12, 2003. In addition, planners desired that the plume disperse material to the west.

6. Lack of 24-hour play

In a real emergency, activity would have continued around the clock, especially in the first 48 hours or so. During the FSE, some activities functioned around the clock, but others did not (e.g., importantly, the Seattle-area Joint Operations Center). As a result, participants were occasionally stymied when attempting to perform some function only to find that other participants were not playing at the time. These artificialities, particularly those that impacted decision-making and response activities, have been carefully noted in the exercise analysis.

7. Pre-positioning of responders

Various assets (such as teams from Department of Energy, Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), and other agencies) were pre-positioned in the venues for reasons of safety, logistics, and cost. The evaluation team was able to account for advance deployments and ensure they were accounted for in the subsequent analysis.

8. Varying Participation Schedules

Numerous city, county, and State agencies participated in the FSE at different times during exercise play. As a result some activities that would usually occur in a coordinated fashion were disjointed. This resulted in agencies reaching differing conclusions and decisions at different times thereby created some degree of confusion.

C. Artificialities That Arose During Exercise Play

A number of artificialities arose during the execution of the exercise. In an exercise as large and complex as T2, this is not an unexpected event, and they were properly accounted for in the analysis of the exercise.

1. Chicago hospital play and the Metropolitan Health Care Council

Chicago area hospitals participated enthusiastically in T2 play. Participation counted towards their accreditations' exercise requirement. The Metropolitan Chicago Healthcare Council (MCHC) was to provide role players to be Pneumonic Plague patients in area hospitals. At the same time, MCHC was to provide other role player patients, separate and apart from those participating in the FSE, for drills to be done by the hospitals as part of maintaining their accreditation.

The addition of the extra patients by MCHC was not matched by an addition of extra control personnel. Artificialities arose when safeguards put in place by the T2 designers to avoid the blending of these two role player populations were not followed. The principal result was a distortion of the Pneumonic Plague scenario, with the unrealistic and uncontrolled number of additional cases that reduced the fidelity of play for those participants engaged in tracking the progress of the outbreak. The attempt to maintain two sets of records added confusion and may also partly by the end of the day on May 13, 2003, control staffs in the Illinois and Washington, D.C. Control Cells implemented measures to mitigate the impact.

2. Issues with control

During the FSE, there were several instances in which controllers took it upon themselves to modify the scenario, and in which other exercises or events unrelated to T2 briefly were believed to be part of T2 play. Again, these instances were documented and accounted for in the analysis.

On D+2 somebody increased the threat posed by the *Yersinia pestis* plague bacterium, telling the Illinois venue players that their newest samples from the release sites contained live bacteria. *Yersinia pestis* does not survive for long outside of a host, so the presence of live bacteria at the release sites would indicate either a re-attack at the same site or a genetically modified *Yersinia pestis* that could survive lengthy exposure outside a host. In that neither a re-attack nor a modified germ was part of the scenario, the spurious report to the players qualifies as an artificiality. It had the potential to be an important one because it could have altered (but did not) the course of play and the decision-making of top officials.

The scenario contained an incident in which investigators at the RDD site were to find a bomb-like object, which their notional investigation would then reveal not to be a bomb. These events occurred, but later another controller pronounced the device to be a bomb, leading to its explosive destruction by a remote-controlled robot. The on-the-spot creation of a second bomb represented a departure from the MSEL and—because of the implication that if there could be a second bomb, there may be a third—could have altered decision-making up the chain of command.

Finally, there were several artificialities of control that occurred purely by accident, including at least two in which word of dire emergencies (e.g., the escape of a radioactive plume from a nuclear power plant in Ohio) actually leaked into FSE play from other simultaneously-running exercises, which were to remain separate from T2.

V. SPECIAL TOPICS

During the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE), several sequences of events attracted great interest as they unfolded. Many represented truly experimental and groundbreaking elements of the response to a radiological or bioterrorism attack. These elements of response tended to cut across multiple areas of analysis, and the T2 evaluation team decided that—given their salience—the best way to address them was to do so directly, telling the story and what was concluded from it. Some aspects of these stories also appear in their respective areas of analysis.

These special topics are:

- Alerts and Alerting: The Elevation of the Homeland Security Advisory System Threat Condition to Red;
- Declarations and Proclamations of Disaster and Emergency;
- Department of Homeland Security Play in T2: The Role of the Principle Federal Official;
- Data Collection and Coordination: Radiological Dispersal Devise Plume Modeling and Deposition Assessment;
- Play Involving the Strategic National Stockpile;
- Hospital Play in the Illinois Venue: Resources, Communications, and Information Sharing during a Public Health Emergency;
- Decision-making under Conditions of Uncertainty: The Plague Outbreak in the Illinois Venue; and
- Balancing the Safety of First Responders and the Rescue of Victims.

Some of these topics overlap, but each account is written so that it may stand on its own.

This page intentionally left blank

A. Alerts aud Alerting: The Elevatiou of the Homeland Security Advisory System Threat Conditiou to Red

1. Introduction

One of the most visible reactions to the events of 9/11 has been the creation of the color-coded Homeland Security Advisory System (HSAS). Real-world experience has included several transitions from Yellow to Orange, and back again.[20] The national threat level has never been lower than Yellow or higher than Orange. Since a transition to Red has not yet occurred outside of exercise play, the Top Officials (TOPOFF) 2 (T2) exercise provided an opportunity to implement and analyze the role and impact of the HSAS Threat Condition Red. The U.S. Department of Homeland Security (DHS) has initiated the HSAS Working Group to review advisory system, as directed by Homeland Security Presidential Directive (HSPD)-3 and to examine the HSAS issues observed during the T2 Full-Scale Exercise (FSE), many of which are also discussed in this After Action Report (AAR).

In the FSE the threat condition was elevated to Red on five occasions. The initial two were local elevations (King County and the City of Seattle, Washington) immediately following the RDD explosion. The others were HSAS elevations by DHS: The City of Seattle on May 12, 2003, in response to its local elevation; seven select cities late on May 12, 2003 (New York, NY; Los Angeles, CA; San Francisco, CA; Washington, D.C.; Houston, TX; Seattle, WA; and Chicago, IL); and finally, a nationwide elevation on May 13, 2003. On May 14, 2003, DHS downgraded the threat condition from Red to Orange nationwide except for New York City and Chicago.

T2 was groundbreaking in several areas with respect to the HSAS: It represented the first opportunity for agencies to experiment with the actions associated with an elevation to Red; it allowed for examination of the implications of elevating regions to Red; it included local jurisdictions raising their own threat conditions to Red; and it highlighted that additional refinement of the system is needed. This section attempts to document how these events unfolded during the T2 FSE and what happened as a result. It is intended to promote learning and improvements with the continuing implementation of the system.

2. Background

HSPD-3 established the HSAS, which is "intended to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response." The system uses colors (from green to red) to define threat levels from low to severe. Table 3 shows the HSAS

[20] The fact that the *National Direction and Control Seminar* and the Full-Scale Exercise each took place during Orange alerts underscored to the players and others the urgency, relevance, and realism of T2, whose scenario included a transition from Yellow to Orange and up to Red.

colors, labels, and the associated risks and the protective actions Federal departments and agencies should consider with each assigned threat level.

Table 3. Homeland Security Advisory System

Color	Label	Level of Risk	Protective Action Guidelines
GREEN	**LOW**	**Low risk of terrorist attacks**	Federal departments and agencies should consider the following general measures in addition to the agency-specific protective measures they develop and implement: • Refining and exercising as appropriate preplanned protective measures; • Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency protective measures; and • Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.
BLUE	**GUARDED**	**General risk of terrorist attacks**	In addition to the protective measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific protective measures that they will develop and implement: • Checking communications with designated emergency response or command locations; • Reviewing and updating emergency response procedures; and • Providing the public with any information that would strengthen its ability to act appropriately.
YELLOW	**ELEVATED**	**Significant risk of terrorist attacks**	In addition to the protective measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the protective measures that they will develop and implement: • Increasing surveillance of critical locations; • Coordinating emergency plans as appropriate with nearby jurisdictions; • Assessing whether the precise characteristics of the threat require the further refinement of preplanned protective measures; and • Implementing, as appropriate, contingency and emergency response plans.
ORANGE	**HIGH**	**High risk of terrorist attacks**	In addition to the protective measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific protective measures that they will develop and implement: • Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations; • Taking additional precautions at public events and possibly considering alternative venues or even cancellation; • Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and • Restricting threatened facility access to essential personnel only.
RED	**SEVERE**	**Severe risk of terrorist attacks**	Under most circumstances, the protective measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the protective measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific protective measures that they will develop and implement: • Increasing or redirecting personnel to address critical emergency needs; • Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources; • Monitoring, redirecting, or constraining transportation systems; and • Closing public and government facilities.

The original directive authorized the Attorney General to assign the threat condition. HSPD-5 amended HSPD-3, such that:

> *Threat Conditions shall be assigned by the Secretary of Homeland Security, in consultation with the Assistant to the President for Homeland Security. Except in exigent circumstances, the Secretary of Homeland Security shall seek the views of the Attorney General, and any other Federal agency heads the Secretary deems appropriate, including other members of the Homeland Security Council, on the Threat Condition to be assigned.*

The greater the perceived risk of a terrorist attack, the higher the threat condition. According to HSPD-3, *risk* includes both the probability of an attack and its potential gravity. Decisions as to what Threat Condition to assign should, therefore, take both of these factors into account. HSPD-3 states that the evaluation of the Threat Condition is qualitative and shall include, but not be limited to, the following factors:

- To what degree is the threat information credible;
- To what degree is the threat information corroborated;
- To what degree is the threat specific and/or imminent; and
- How grave are the potential consequences of the threat?

HSPD-3, as amended by HSPD-5, also authorizes the Secretary of Homeland Security, in consultation with the Assistant to the President for Homeland Security, to decide whether to publicly announce the threat condition level on a case-by-case basis. Threat conditions may be assigned for the entire nation, or they may be set for a particular geographic region or industrial sector.

HSPD-3 also directs Federal agencies and departments to implement appropriate protective measures according to the threat condition. Each department and agency is responsible for developing their own protective measures, and they also retain the authorities to respond, as necessary, with their specific jurisdictions as authorized by law.

The HSAS is only binding on the executive branch of government. It does, however, encourage governors, mayors, and other leaders to review their organizations and assign protective measures to the threat conditions, in a manner consistent with that of the Federal Government. For example, some states, such as Illinois have developed formal guidelines with specific security measures that are to be implemented under each of the HSAS color codes. In Illinois, the State Emergency Operations Center (EOC) determines the appropriate response actions and security recommendations after any elevation and transmits them to county and municipal agencies. The State of Illinois exercised this system during the FSE.

3. Reconstruction

The FSE scenario called for an elevation of the nationwide threat condition from Yellow to Orange. It occurred as scheduled by controller inject at 1000 Eastern Standard Time (EDT) on May 6, 2003, in response to scripted credible and corroborated information indicating a grave and imminent terrorist threat. By contrast, the transitions that took place during the exercise from Orange to Red occurred as player actions, not as Master Scenario Events List (MSEL)

injects, and accordingly happened when the players decided it was appropriate. Figure 5 depicts the various alert elevations to Red during the FSE, including local elevations.

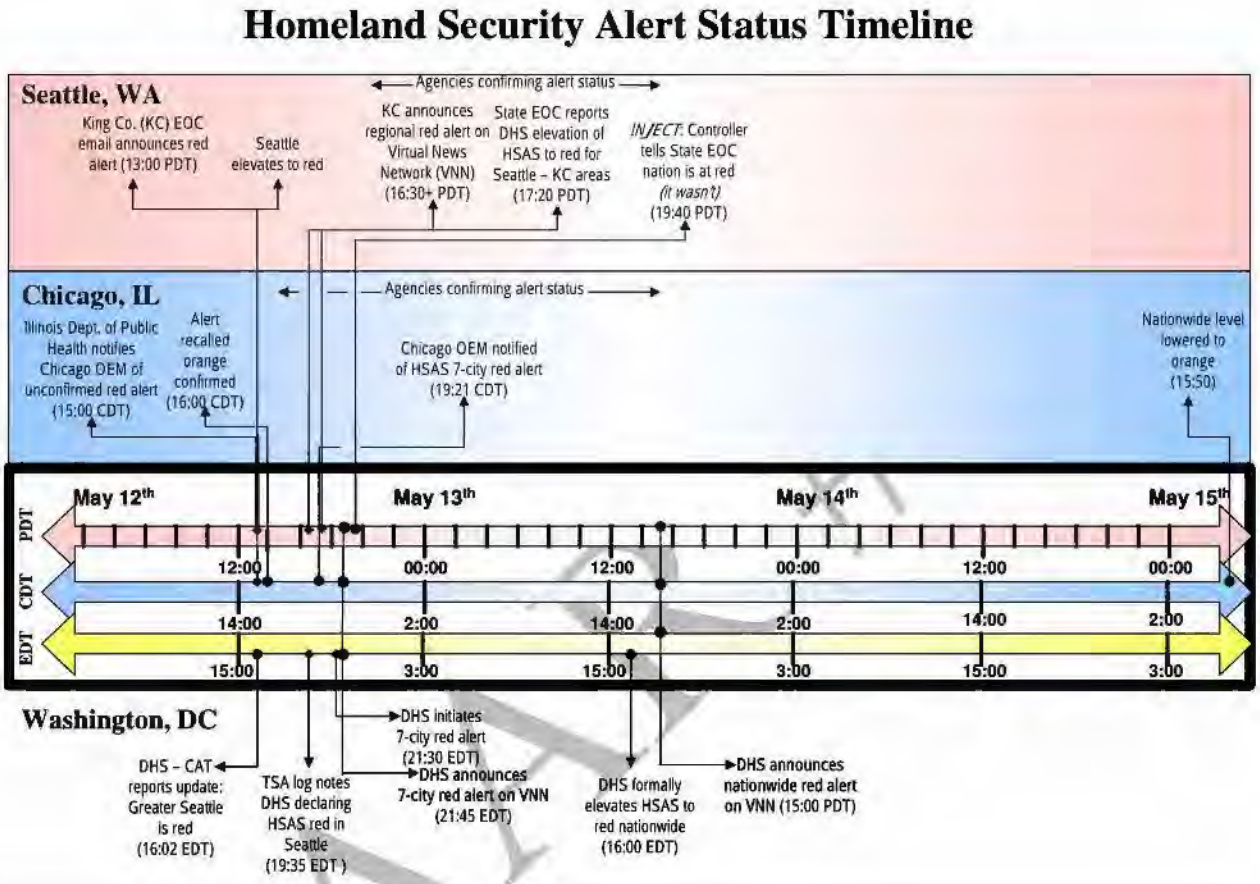


Figure 5. Homeland Security Alert Status Timeline

a. Local and regional threat condition elevations

Shortly after the radiological dispersal device (RDD) explosion, King County and the City of Seattle effectively elevated the threat condition to Red in their respective jurisdictions. The City of Seattle activated its EOC to Phase III immediately in response to the blast. The King County EOC posted its elevated threat condition at 1240 Pacific Daylight Time (PDT) on May 12, 2003 and distributed an e-mail announcing the elevation at 1319, stating, "The threat level is raised to Red." Local officials announced a regional elevation for Seattle and King County on the Virtual News Network (VNN) around 1630 PDT.

Data indicates that DHS learned of Seattle and King County's intent to raise their alert levels as early as 1600 EDT. Several data points suggest that DHS responded to this by initiating an elevation of the HSAS to Red in Seattle. The only formal documentation of this was found in a

DHS/Transportation Security Administration (TSA) log at 1935 EDT, which reported that DHS elevated the HSAS to Red in Seattle.[21]

Substantial confusion followed these first elevations. Many participants in all venues assumed the first local elevations were initiated by DHS and that they applied to the nation. Uncertainty regarding the alert status of King County, Seattle, and Washington State ensued for almost 24 hours as agencies sought to confirm the specifics. The confusion even spread to at least one of the exercise control cells. At 1940 PDT on May 12, 2003, a controller told the WA State EOC that the nation was at Red (which it was not at this time), fueling the confusion.

Meanwhile, the City of Chicago and the State of Illinois experienced brief, false elevations to Red. For example, around 1500 Central Daylight Time (CDT) on May 12, 2003, the Chicago Department of Public Health notified the Chicago Office of Emergency Management (OEM) of an unconfirmed Red Alert. The Illinois Department of Public Health (IDPH) notified the Chicago OEM of an unconfirmed Red Alert soon thereafter. This may have been triggered by the belief that the nation was elevated at the time of the Seattle/King County elevation or separate elevation within the health alert system which is also color-coded. Over the next two hours, the HSAS threat status was ultimately confirmed as Orange:

- At 1535 CDT the Director of the Chicago OEM advised that the elevation to Red was unconfirmed and gave instructions to "hold at Orange pending formal notification through the HSAS system";
- By 1600 CDT the Chicago and State EOCs had confirmed the HSAS threat level was still at orange; and
- At 1711 CDT, the Chicago EOC distributed a message that the HSAS threat level was still Orange.

b. Seven-cities threat elevation

Later in the evening of May 12, 2003, the Secretary of DHS decided to raise the HSAS threat condition for seven cities including Seattle and Chicago based upon intelligence that indicated a severe risk of terrorist attacks in those areas. A DHS Crisis Action Team (CAT) situation report and e-mail distributed at 2030 EDT noted that:

> *DHS advised that effective at 2130 EDT (1930 CDT/1830 PDT) on today's date, the alert level will be raised to Code Red for the following cities: Seattle; San Francisco; Los Angeles; Houston; Chicago; New York; Washington, D.C.*

Around 2145 EDT, the Secretary of DHS announced on VNN that DHS had done an assessment of the need to take additional preventative action "throughout the country" and had "raised alert in the six cities along with King County (WA), and the City of Seattle." This appeared to be pre-coordinated by DHS with other agencies, as many entities, but not all, knew before the formal announcement on VNN. Some were still confused about the status of Illinois and Washington in light of this, and there was some confusion in the WA State EOC as to whether this applied to the City of Seattle and King County as well.

[21] The analysis team attempted to confirm this information via phone calls but did not receive a response by the publication of this draft report.

Agencies were uncertain about the impacts of a DHS elevation of the HSAS to Red in Washington, and local jurisdictions and began inquiring about "what would DHS close" and the impacts on airspace and ports, among other systems. There were some breakdowns in communication: the Principle Federal Official (PFO) in Washington noted that there were no messages coming from DHS to the Joint Information Center (JIC) or Joint Operations Center (JOC) related to this elevation prior to the VNN announcement. Also, a Federal Emergency Management Agency (FEMA) log referred to "breaches of protocol" in notification procedures.

c. Nationwide

On May 13, 2003, VNN reported between 1445 and 1545 EDT that the Secretary of DHS was considering raising the entire nation to Red. At 1530 EDT, a member of the DHS CAT noted that:

> *The CAT leader passed results of meeting with Secretary Ridge—he will recommend to President that all three Chicago airports...rail/trains be closed, intercity buses be closed down, mass transit will remain open, highways will remain open. Also recommended red nationwide, but transportation systems nationwide will not be closed to keep supply chains open.*

The DHS Office of International Affairs received similar information from TSA.

At approximately 1600 EDT, the Secretary of DHS initiated a nationwide elevation to Threat Condition Red when it became clear that the entire country could be under attack. A DHS "ALERT AL-03-TOPOFF2-M" formal memorandum recorded this as follows:

> *The Secretary of DHS, in consultation with the intelligence community and the Homeland Security Council, raised national threat level to Code red nationwide as of 1600, May 13 due to the RDD detonation and the Pneumonic Plague release in Chicago and receipt of credible information that additional attacks may be planned...Federal Departments and Agencies, and State and local authorities, are directed to immediately implement protective actions identified in Operation Liberty Shield...*

The Secretary of DHS appeared on VNN at 1800 hours EDT to announce the elevation of the nation to Red.

Following this news, the Illinois State EOC initiated the State of Illinois alert system and provided detailed instructions to the City of Chicago and collar counties. Using a standardized communications system and operating procedures, Illinois' participating agencies initiated a response to the threat elevation.

The Director of the WA State EOC heard about this DHS action via VNN; he did not receive any formal notification from DHS before the Secretary's speech. He also did not receive any written guidance about the impact on transportation systems or whether public events should be cancelled. As of 1900 PDT, top officials in the WA State EOC had still not received formal confirmation of the elevation. The Joint Operations Center (JOC) contacted King County looking for a copy of the speech or formal documentation. The Seattle and King County EOCs also learned about the elevation through VNN and expressed some frustration at the lack of formal notification.

The apparent lack of formal notification led to continued misunderstandings about the scope of DHS's action. There was some speculation in the Seattle EOC that perhaps the latest announcement applied to Chicago only: "Suspect this message was garbled and pertains to Chicago only. Request DHS fax us paper on condition of Red Statement…" At 1700, a Seattle EOC data collector noted a DHS acknowledgement that it did not follow proper notification protocols: "DHS agrees that they did not follow procedures to notify top officials…"

There was widespread confusion at all levels of government regarding the actions to take in response to the DHS elevations to Red, as well as confusion regarding the actions Federal agencies were expected to take (e.g., closing airspace). Many Federal, State, and local (FSL) agencies looked to DHS for specific guidance, as the following four examples illustrate:

1. From notes on a discussion among local top officials in the Seattle EOC of the nationwide elevation to Red on May 13, 2003:

   > *What is working and what is not...what does stay at home for 48 hours mean? Who maintains water, power, and hospital services? etc...Will feds shut down the airports? Interstate commerce, Ports? We are not sure what 'go home for 48 hours' means? ...We need to go back to the Feds, DHS and ask for clarification on what is key and essential personnel...We need to determine what to say in a press release...*

2. Late the evening of May 13, 2003, the WA State EOC formally requested guidance through DHS/FEMA on what is required under a the HSAS Threat Condition Red:

   > *Specifically, the State needs clarification on what Protective Measures are contemplated for Federal facilities by Homeland Security ..." and "The State EOC is aware it needs to notify the public of its position based upon the Ridge position, but is not clear on what this position is.*

3. From an Environmental Protection Agency EOC discussion on Condition Red at 0800 on May 13, 2003:

   > *Security guidance says people are supposed to report to work unless otherwise notified. The question is what we tell employees. We need a decision pretty quickly as there will be panic. Action would be to call DHS for guidance on the Federal area.*

4. From the Veteran's Affairs Central Office on May 13, 2003:

   > *Does Safe Harbor address what to do when threat level increases in only certain places - clarification language to be added to op plan - we need to monitor other cities that have elected to raise threat level themselves & notify facilities...*

Even within DHS there was some uncertainty of what actions to expect and guidance to issue under Condition Red:

- "The DHS Emergency Preparedness and Response (EP&R) desk requested from agency as to what is expected of the States under Threatcon red"; and
- From the Homeland Security Center Incident/Information/Operational Response Report received from FEMA Emergency Support Team (EST) on May 14, 2003, at 0255 EDT:

The FEMA EST is requesting guidance as to what are the expectations of the states under Threat Condition Red. For the record, earlier tonight, upon notification that the entire nation was at a Code Red threat level, the EST followed the checklist included in the above referenced notification to simulate play in support of TOPOFF 2. We have subsequently received an inquiry from the State of Washington as to what is expected of the states at level Red. With this e-mail, we are forwarding this to your attention as your input will be needed to best answer these questions!

d. Downgrade to Orange for most of the United States

At 1615 EDT on May 15, 2003, FEMA e-mail traffic noted that the DHS Secretary directed the nationwide HSAS Threat Condition returned to Orange except for Chicago and New York City; these two cities remained at Red.[22] The first documentation of this notice within Illinois was from the Chicago Department of Health and Human Services (HHS) to the Chicago OEM at 1515 CDT. The Chicago OEM received formal notification from FEMA Region V at 1550 CDT.

4. Artificialities

- Some of the above data suggests an exercise control problem. For example, a WA State EOC shift change briefing stated, "controller inputs are not being backed by operational inputs." This reflects a problem with the flow of information through the control and play chains. There is at least one instance of controller interference with the WA State EOC's understanding of the threat level, which contributed to some of the confusion.[23] While players were expected to obtain information through proper channels, some of the data did suggest controller interference at various locations and times in what may have been misguided attempts to help the process.
- Not all agencies were fully staffed for the FSE as they would be under an actual threat condition of Red: A FEMA Regional Operations Center (ROC) data collector log noted:

  In reality the Disaster Field Office (DFO) and ROC would be fully staffed (at the Red threat level); we would have discussions with the State, county, etc. about what they're having to deal with…

- At 1515 CDT on May 14, 2003, the Command Group at the JOC in Illinois was informed by FEMA/DHS that the threat condition had been downgraded to Orange except for Chicago and New York City. They began to implement the appropriate changes when this was retracted and they were notified that the nation was still at Red. This may have been a situation where players were outpacing the MSEL.
- The Illinois State and Chicago EOCs closed for the night at 1700 and 1800 respectively on May 12, 2003. This resulted in an artificial delay in formal transmission of the news to the collar counties of the seven-city elevation.
- The absence of an active news-gathering mechanism, described in more detail in the *Artificialities* section of this AAR, may have contributed to some confusion regarding the

[22] The Washington venue was no longer playing at this time.

[23] From WA State EOC Data Collector log: "National Controller called EOC supervisor to tell him the national threat level went Red-Effective 1740. This was an inject.

elevations as well, specifically early on in local King County and the City of Seattle where local elected officials were not able to broadcast this message widely.

- The FSE did not exercise FSL agency Continuity of Operations Plans (COOP), which some agencies may have implemented had this been a real attack or if they were under a real Red Alert. Such plans involve the emergency relocation of offices to alternate facilities depending on the emergency and threat. If even a few key agencies implemented COOPs, the communications, coordination, and connectivity issues experienced by agencies during the FSE would have likely multiplied, as agencies are not familiar with other agencies' COOP procedures and these procedures are rarely exercised across the national response community.

5. Analysis

As the reconstruction makes clear, a number of critical HSAS issues arose during the FSE events. In particular, there was pervasive uncertainty over the status of threat conditions in the various jurisdictions. While some confusion was controller-induced, this does not account for the principal impact. There was uncertainty over what actions should be taken at Red. The rationale behind the elevations was not always clear to the players. Another issue apparent in the data was concern over the costs of maintaining a threat condition of Red. Finally, many critical public policy decisions were made during this period of uncertainty of threat conditions and public information on the subject was not clear.

a. Confusion about the threat condition status of jurisdictions

This is perhaps the most pervasive problem and the confusion appears to have grown with each successive elevation. When King County and Seattle first raised their local threat conditions to Red, confusion began to spread in Washington State. Many (including data collectors and, importantly, controllers[24]) assumed that DHS had raised the HSAS for the entire nation (the HSAS Threat Condition was elevated for just Seattle). Others wondered if Washington State was at Red (it was not until the nationwide elevation was initiated by DHS). Data suggest that as late as 0245 PDT on May 13, 2003, the WA State EOC was still trying to confirm the threat condition status of Seattle at Red and Washington State at Orange. The Washington National Guard log and JIC data collector logs finally confirmed a consistent understanding of threat status for the city, county, state, and nation by 0737 PDT on May 13, 2003, (Seattle and King County were Red, and the state and nation were Orange). Many assumed again the entire nation was elevated to Red when the threat status of the seven cities was elevated.

b. Confusion as to what actions to take under a red alert

During the FSE, there was widespread confusion at all levels of government regarding specific protective actions to be taken under HSAS Threat Condition Red. This included actions that should be taken by a particular agency as well as what actions others were implementing. Federal agencies such as FEMA, Department of Transportation, HHS, and others have well-developed action plans for Threat Condition Red. FEMA has checklists that have been developed, and it simulated the usage of them during the exercise. However, Federal plans do

[24] This is relevant to the analysis to the extent that some of the data collector accounts were inconsistent as their interpretations of messages broadcast on VNN differed as did participants. Further, controller confusion resulted in at least one false inject.

not all carry the same level of detail, and may not be widely or consistently understood by other Federal agencies, State and local governments, the private sector and the general public. Many agencies looked to DHS for clarification as to what actions they should take, and what actions the Federal Government would be taking, under a Red Alert.

The language in HSPD-5 states that the HSAS is only binding on Federal agencies and that those agencies are responsible for developing their own specific protection measures to meet the guidelines of the HSAS. Furthermore, HSPD-5 is not binding on State or local governments, but encourages them to develop their own protective action strategies. But this flexibility also means that no single agency at any Federal, State, or local level of government has a consistent and comprehensive understanding of the protective actions that might be taken by other agencies under Red. Further, the potential impacts of protective actions taken by an agency or jurisdiction on other agencies or jurisdictions are not well understood. The confusion is magnified when the Federal HSAS and State/local elevations intersect and are not synchronized. For example, Federal and State agencies in Washington were temporarily uncertain as to their status after the local Seattle and King County elevations to Red. When the nation was elevated to Red by DHS, State and local agencies were uncertain as to the impact on them.

Participants in the T2 After Action Conference (AAC) suggested the development of an escalating scale of operational response linked to the HSAS levels. This system would be defined by a federation of FSL agencies and would offer a comprehensive operational response framework that jurisdictions at all levels could use to help define their response plans for each threat level. Such an operational framework would help to increase the consistency of measures taken across the nation, while preserving the flexibility of the system overall. It would help to ensure that all jurisdictions, regardless of their potential specific decisions on how to respond to various elevations, are at least considering common families of protective measures in those decision processes.

c. Some confusion may be due to unclear language

While threat conditions under the HSAS may be set for a particular geographic area or industrial sector, it is generally referred to as the "national threat level," possibly contributing in some cases to assumptions that it applies to the entire nation rather than specific areas. During the FSE, the term *national* in reference to the DHS Threat Condition appeared to be interpreted two different ways:

- It applied to the entire nation (which was not the case in initial HSAS elevations); and
- It referred to the national threat level recommendation system, which could apply to specific localities/jurisdictions/regions.

The term *regional* was used and interpreted in as many as five different ways:

- DHS had raised the threat condition for some regions which were not clearly specified, and which may not have been along clear jurisdictional boundaries;
- DHS raised the threat condition for one or more local jurisdictions (e.g., King County and Seattle);
- Local jurisdictions raised threat conditions on their own;

- DHS raised the alert level for certain, specific cities (e.g., when the alert level was raised for seven cities, some referred to this as a regional elevation); and
- A regional Red Alert was instituted for Washington State, while the nation was still at Orange.

d. Formal notification procedures were not consistently employed or understood

Another potential source for confusion lies in the area of communications and coordination; formal notification procedures for changes to the HSAS Threat Condition, and State/local threat conditions were not consistently implemented or well-understood across FSL levels of government. Many participants relied on informal communications. While there is some evidence of formal communications, they were obscured in many cases by the volume of independent informal communications occurring in parallel. Even organizations that are part of the formal notification chain found it difficult to confirm and validate information they were hearing amid the volume of communications.[25] Most participants (with the exception of DHS) received much of this information from VNN, and relied on this information in many cases. If agencies had shared a common understanding of a formal notification approach, one might have expected to see similar approaches to validate the informal reports they were receiving regarding changes in the threat condition status.

Some attempts were made to validate information, but many organizations acted on information they received through informal channels. The DHS PFO in Washington helped greatly to dispel confusion over alert elevations and to improve communications overall once he was in position by acting as a direct conduit to DHS and helping to streamline communications.

e. Concern about the financial and other costs associated with implementing and maintaining High or Severe levels of the alert system

During T2, many agencies attempted to quantify the costs of implementing Threat Condition Red and many raised this concern at the AAC. Some agencies sought to obtain reimbursement for these costs through various means. The data show that DHS was concerned about the potential unintended consequences of threat elevations including new vulnerabilities that could be created by reallocating resources from one focus to another. Some of the issues being addressed by the DHS-initiated HSAS Working Group are the economic and social implications of an elevated threat level.

f. Uncertainty over rationale for the various elevations

Uncertainty may be related to both the lack of formal notification and the lack of understanding about what protective measures to take in response at red. Some agencies argued that specific information was needed to identify what actions to take. For example, the following comment comes from the WA State EOC: "People come in all alarmed because DHS wants to go to Red Alert nationwide. No one knows why but that requires Americans to stay home for 48 hours…"

The concern about the lack of specific intelligence accompanying many real-world threat elevations was also voiced at the AAC. Some of this is due to a lack of specificity or to

[25] At 2146 hours PDT on 12 May 03, a FEMA ROC Data Collector reports that "the State had received a message saying all of US on Red …been trying to track where info came from and get right info." This same log also noted a belief that the entire nation remained at orange when by this time seven cities had been elevated to Red.

information security in source intelligence, issues currently being addressed by DHS. But increased coordination between DHS and the states and localities on the nature of threats severe enough to merit increased elevations in the threat system to their jurisdictions, particularly to Red, are crucial to a response that minimizes unintended consequences and maximizes the use of limited resources towards an increased protective posture.

g. Many public policy decisions were made during this time of uncertainty

Numerous decisions were made during this period of uncertainty—some of which would have seriously challenged the agencies' abilities to maintain credibility and implement public policy objectives given the widespread lack of understanding of the threat condition status. This could have had dramatic impacts on messages to the public as well. For example, word of an elevation to Red that was later reported to be incorrect likely would have caused some alarm. Decisions to re-open transportation corridors, such as the airspace in Seattle, would have been confusing, in light of a national condition of Red or even a continued city-wide condition of Red. The potential public policy implications of elevations to Red at all levels of government further underscore the importance of a coordinated, synchronized, operational response to HSAS elevations.

h. Public information was unclear

Many of the issues highlighted above would have had impacts on the effectiveness, comprehensiveness, and consistency of messages delivered to the public by top officials. Participants reiterated at all of the T2 seminars the importance of consistency and comprehensiveness of messages for establishing and maintaining top official and spokesperson credibility. Top officials' public announcements, while limited, did not provide specific information to the public about what to do at Red or how agency actions and protective measures differ at Red, as Threat Condition Red relates to one at Orange. The DHS Secretary's speech that elevated the national threat condition to Red did not explain why people in Topeka, Kansas (for example) could be at the same level of risk as those in the affected areas or other higher-risk areas, such as New York City. In their public announcements, State and local officials did not clarify the local nature of the initial elevation to Red and the implications therein. Further, there was no mention in any of the public announcements of a synchronized FSL agency response to the elevations (at present this is an issue as described in part *b.* of this section).

A consistent and comprehensive operational response at all levels of government would be key to building confidence in the overall protective posture. Public perception of a comprehensive and consistent operational response would be especially important for top officials if, as was the case during the FSE and the Large-Scale Game (LSG), an attack were to occur in a jurisdiction that was under an elevated threat condition. The HSAS system cannot ensure against all future attacks, and is not one hundred percent failsafe. Its value and goal is two-fold: (1) increase the overall protective posture to reduce the risk of a terrorist attack; and (2) build public confidence in the government's ability to protect the public and provide a sense of safety and security.

Both the value and goal of the HSAS and the credibility of government top officials, depend upon a comprehensive operational response at all levels, as well as the public's belief that the government is indeed doing/has done everything in its power to effectively reduce the risk of such an attack. DHS may want to consider joint press conferences in future announcements of local or regional elevations of the HSAS that include the top officials of those jurisdictions, as

well to reinforce the public's confidence that a comprehensive response is underway. Further, to the extent that any part of the country, much less the entire nation, is ever at a sufficiently severe risk of attack to merit an elevation of the HSAS to Red, top officials must explain the nature of this risk as clearly as possible without compromising national security. Such information is critical to maintaining the credibility of the HSAS system and to obtaining the desired public response to such an elevation, which is a key component (along with FSL agency protective actions) to minimizing both the likelihood and potential human consequences of an attack.

A final issue with public information was the timing and delivery of the news regarding the unprecedented elevation of the nation to Red. This news was delivered at the end of the DHS Secretary's speech after numerous other general status updates and a recap of the previous day's "seven-city" elevation. Many would expect an announcement of this magnitude and gravity to lead to such a speech. Additionally, the public was not fully engaged by the Federal Government during the exercise about what actions it should be taking as the HSAS was increased. The American Red Cross, however, did post recommended actions the public should take under the different threat levels on its website, and established a call center for guidance.

6. Conclusions

HSPD-3, amended by HSPD-5, specifically recognizes "the roles and responsibilities of State and local authorities in domestic incident management" and their "initial responsibility" for incidents. The HSAS is described as a "flexible" system with the purpose of providing a "common vocabulary," and State and local jurisdictions have been encouraged to adopt the system. It is further described as a "national framework," intended to help unify various sector-specific alert systems already in existence.

The T2 FSE highlighted that additional refinement of this system is needed. Agencies at all levels were not certain what actions to take in response to Red, or what actions were being taken by other FSL agencies. As participants at the AAC emphasized, and as the FSE demonstrated, a more common and systematic, but flexible, framework for implementing protective measures is needed. Development of an "operational response" system, tied to the escalating alert levels of the HSAS, could help increase the overall protective posture taken at each level of government, and increase the overall situational awareness of top officials across a specific jurisdiction or

SUMMARY OF CONCLUSIONS—ALERTS AND ALERTING:

- HSAS elevations should be pre-coordinated and synchronized with affected states/localities. There was widespread uncertainty as to the HSAS status until the nationwide alert on May 13.
- Critical public policy decisions were made during a period of uncertainty on HSAS threat status.
- Top officials lacked "situational awareness" and a "common operational picture" of relative increase in civil protective posture in response to condition red. ***Agencies recommend development of a parallel system of operational response linked to the HSAS levels.***
- Increased coordination is needed between DHS and states/localities on nature of threats, to minimize unintended consequences and cost-effectively increase the overall protective posture.
- Agencies do not have or share consistent understanding of formal notification approaches for HSAS status changes.
- Public information messages regarding HSAS elevations should be clear, consistent, and explain comprehensive FSL response actions, as well as recommended actions for the general public to take.

region. Such a common operating picture across all levels of government requires improved communication and coordination; standard terminology and pre-designated action plans or checklists for all agencies may help in this regard.

Elevations of the HSAS should be synchronized (in purpose, place, and time) with States and localities, and their elevations in-line with the HSAS—specifically when alert conditions at these levels may differ, even if temporarily. Local communities will immediately implement Red-equivalent emergency procedures in the aftermath of any attack, as was done during the FSE, but coordinating these actions with DHS and the broader HSAS framework needs additional refinement. Further, elevations of the HSAS should be closely coordinated with the affected State and local jurisdictions beforehand. An HSAS elevation to Red will have impacts upon affected States and localities—States and local jurisdictions may feel pressure to respond even if they don't perceive the threat to merit such an elevation in their particular jurisdiction. Such consultation can help to ensure that protective actions are implemented in the most cost-beneficial manner appropriate to the nature of the threat.

Agencies did not share a consistent understanding of the HSAS status of the nation or their jurisdictions until the nationwide elevation on May 13, 2003. This was due to communications issues—both the absence of a shared understanding of formal notification procedures, as well as inconsistent language. In some cases, formal notifications occurred between DHS and the states, between states and local jurisdictions, and between State/local jurisdictions and DHS. However, this was not always the case and it did not appear to occur with consistency.

While the media is sometimes the first means by which government agencies will learn of major events and threat elevations, formal notifications are imperative for transmitting information as critical as alert elevations, and certainly one to Red. Agencies must all be fluent in formal processes and know to treat anything not received through them as unconfirmed. Periods of uncertainty could delay the implementation of some protective actions and impact public information. Not only might inconsistent messages and decisions impact the credibility of elected officials, it could undermine the effectiveness of public safety campaigns. Further, the extended time spent confirming the threat status through multiple channels diverted energy from other agency priorities.

Also, language must be clear and consistent. The term *national threat level* was assumed by some to refer to any threat elevations regardless of their geographic scope or the source of the FSL action. When people heard the national level was raised, many assumed this referred to its geographic scope and assumed the entire nation was at Red when it was not. In some cases elevations initiated by local or State jurisdictions were referred to as regional elevations and people were not clear about the boundaries. Some described the seven-city elevation as a regional elevation. The precise scope and nature of threat elevations, since they may vary, need to be explicitly clear to reduce confusion.

Finally, some implications of Red, such as agencies implementing COOPs, were not played and would have further complicated operations. In the event of an attack, many agencies would implement COOPs under the HSAS Threat Condition Red. This reinforces the need to have a tightly orchestrated set of procedures that all agencies understand. Future exercises should include continuity of operations and continuity of government objectives to address these challenges as well to ensure maximum realism.

B. Declarations and Proclamation of Disaster and Emergency

1. Introduction

During the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE), several declarations and proclamations of emergencies and disasters took place. Local jurisdictions in both exercise venues invoked their authorities to declare emergencies, and requested federal assistance under the Stafford Act (see below). These requests ultimately led to a Presidential Declaration of Major Disaster in Washington and one of Emergency in Illinois. In addition, the Department of Health and Human Services (HHS) declared a Public Health Emergency in Illinois under the authorities of the Public Health Service Act. This section discusses the events that led to these declarations, as well as related issues that arose during the FSE.

2. Background

a. The Stafford Act

Stafford Act declarations generally start with a request from a governor. Requests for declarations of both emergency and major disaster must "be based on a finding that the disaster is of such severity and magnitude that effective response is beyond the capabilities of the state and the affected local governments and that Federal assistance is necessary."[26] A *Major Disaster* is defined in the Stafford Act as

> *...any natural catastrophe (including any hurricane, tornado, storm, high water, wind driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this chapter to supplement the efforts and available resources of states, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.*

States may be reimbursed for up to one hundred percent of qualifying expenses under a Presidential Declaration of Major Disaster.

An *Emergency* is defined as

> *...any occasion or instance for which, in the determination of the President, federal assistance is needed to supplement state and local efforts and capabilities*

[26] The Robert T. Stafford Disaster Relief and Emergency Assistance Act, As Amended, 42 U.S.C. 5121, et seq., http://www.fema.gov/library/stafact.shtm.

> *to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.*

Federal assistance under a Presidential Declaration of Emergency is limited to five million dollars except in circumstances where the President determines that:

- Continued emergency assistance is immediately required;
- There is a continuing and immediate risk to lives, property, public health, or safety; and
- Necessary assistance will not otherwise be provided on a timely basis.[27]

Other differences include limitations in public assistance (emergencies allow only for emergency debris removal and emergency protective measures, and not for permanent repair and replacement work), disaster unemployment assistance, and crisis counseling. Here again, exceptions may be made if the President determines that additional assistance is necessary to "to save lives, protect property and public health and safety, and lessen or avert the threat of a catastrophe."

b. Public Health Service Act

The Secretary of HHS is authorized under the Public Health Service Act, 42 United States Code (U.S.C.) 201, et seq., to declare a state of public health emergency. This declaration enables HHS to delegate its granted authority, release funds and resources to prevent the proliferation of a communicable disease, and to plan an emergency medical response in the event of a disease outbreak. HHS is authorized to manage investigative and protective efforts, enter into contracts, assemble grants, disseminate information, and coordinate all other related actions reasonably necessary to respond to the emergency. The Act gives HHS and its delegated authorities, such as the Centers for Disease Control and Prevention and the Food and Drug Administration, wide discretion and independence in the management of such efforts.

A federal declaration by HHS allows for the release of federal resources, including both money and manpower. During the FSE, as a result of the Declaration of a Public Health Emergency in Illinois and in the absence of a Presidential Declaration of an Emergency or Major Disaster there at that time, HHS enabled the activation of several DHS response assets, including the Disaster Medical Assistance Teams (DMATs) and Disaster Mortuary Operational Response Teams (DMORTs).

c. State and local proclamations

State and local authorities under conditions of disaster and emergency vary by state and locality. Authorities for the jurisdictions that participated in the FSE are summarized here for context in understanding how various declarations unfolded.

State of Washington

In Washington, the Governor may declare a state of emergency pursuant to the Revised Code of Washington (RCW) 43.06.220. Through a "Proclamation by the Governor" the Governor is authorized to create curfews and curtail public gatherings; control the manufacture, transfer or

[27] Section 503 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, As Amended, 42 U.S.C. 5121.

possession of flammables and explosives; prohibit the possession of firearms except within a personal residence or business; designate the dispensing of alcohol as illegal and subject other goods to similar control measures; determine the use and closures of roads and highways; and anything else the governor reasonably believes to be for the safety and welfare of the residents of the State. During the FSE, the Washington Governor authorized the Washington Emergency Management Division to establish food control areas around suspected areas, and for others to issue embargoes and perform specific kinds of inspections. In addition, the proclamation activated the National Guard.

The Emergency Management Assistance Compact Act as codified in Washington State RCW 38.10.010 et seq., provides mutual assistance between states entered into the compact in managing any emergency or disaster declared by the governor of the affected state. The philosophy behind this compact is that few disasters remain within the neat confines of jurisdictional borders, and that many states have unique resources they can contribute to a neighhoring, compromised state in the event of an emergency. This Act estahlishes the rules for such mutual cooperation in emergency-related activities.

A county may, and in the event of a Presidential Declaration must, issue a local proclamation of emergency. During the FSE, King County released a proclamation on May 12, 2003 at 1351 PDT pursuant to RCW 38.52 and King County Charter (K.C.C.) Chapter 12.52, stating that due to an explosion, the presence of radiation and other related hazards, additional steps had to be taken to protect the life and property of the county's citizens. This authorized the designated departments of King County to enter into contracts and incur obligations necessary to combat the emergency at hand.

Finally, the Mayor of Seattle may declare a civil emergency through a local proclamation of civil emergency order and did so during the FSE on May 12, 2003, immediately after the explosion, in accordance with the Seattle Municipal Code, Chapter 10.02, the Charter of the City of Seattle, Article V, Section 2, and RCW Chapter 38.52. It, too, serves the purpose of releasing funds and delegating authority in an emergency situation. During the FSE, the proclamation delegated authority to city department heads (e.g., the police chief) so that the Mayor could coordinate the overall response effort. Additionally, the proclamation notified the puhlic of conditions where the exercise of certain rights may be curtailed, but only to the extent that the conditions make it necessary. A copy of the order was both made public and delivered to the governor of Washington and to the King County executive.

State of Illinois

Pursuant to the Illinois Emergency Management Agency Act[28], Chapter 20 of the Illinois Compiled Statutes, section 3305/7 (20 ILCS 3305/ 7), the Governor may declare by proclamation that a disaster exists. *Disaster* means, in relevant part:

> *...an occurrence or threat of widespread or severe damage, injury or loss of life or property resulting from any natural or technological cause, including but not limited to explosion, riot, hostile military or paramilitary action, or acts of domestic terrorism" (20 ILCS 3305/4).*

[28] Illinois ratified the Emergency Management Assistance Compact Act and codified it as 45 ILCS 151/5 (2203).

The Governor proclaimed a state of emergency for the greater Chicago area on May 13, 2003, at 1230 CDT. Upon such a proclamation, the Governor may exercise designated emergency powers for 30 days. Among these emergency powers are the abilities to suspend provisions of any regulatory statutes or procedures for state business; to utilize all available state resources; to transfer the direction, personnel, or function of state departments facilitating disaster response; to take possession of personal property; to recommend evacuation, and so on. The proclamation of disaster also activates the state emergency operations plan.

An Illinois county may declare a local disaster as determined by 20 ILCS 3305/11. A declaration may only be made by a principal executive officer of a political subdivision (i.e., a county) or by his/her interim emergency successor and cannot be continued in excess of seven days except with the consent of the governing board of the political subdivision. The effect of the declaration of a local disaster is to activate the emergency operations plan of that political subdivision and to authorize the furnishing of aid and assistance. The Illinois data indicated that four Illinois counties declared a local disaster at one point or another and decided to consolidate the announcement of the declarations into one.

3. Reconstruction

Figure 6 depicts the timeline of the various proclamations and declarations of emergency and disaster that occurred during the FSE.

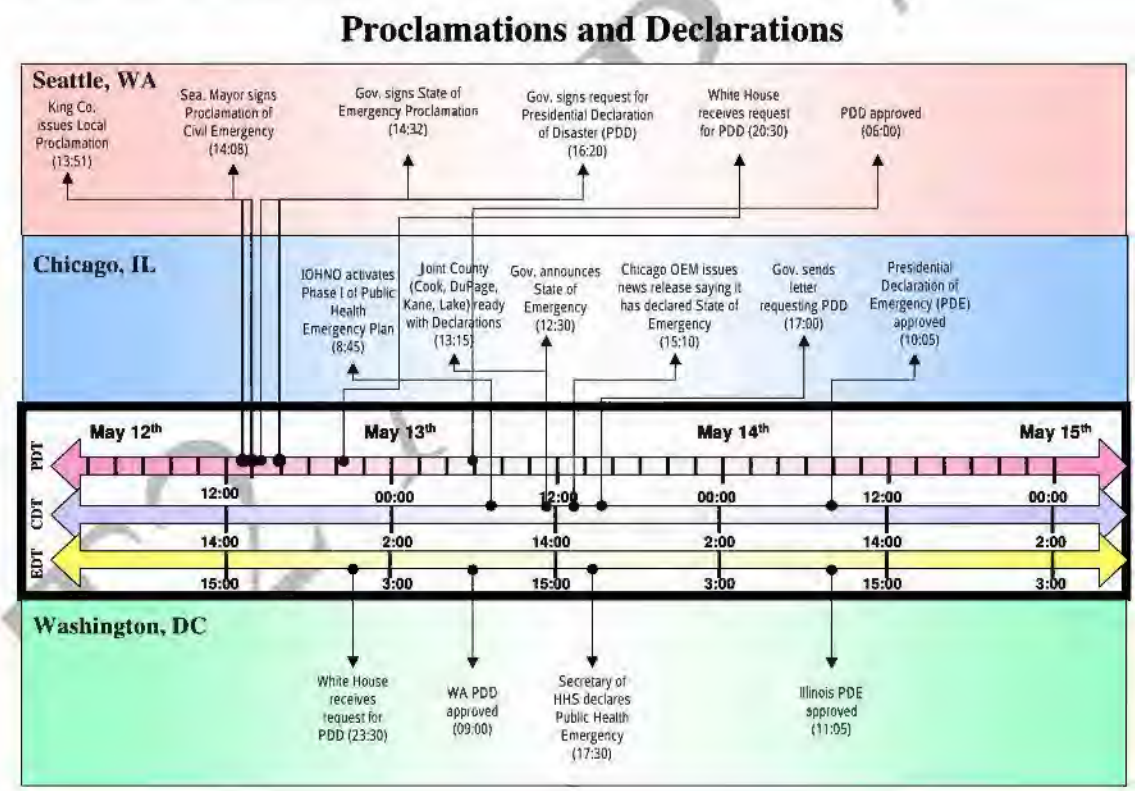


Figure 6. Proclamations and Declarations

a. Washington venue (all times Pacific Daylight Time)

In Washington State, local authorities initiated proclamations of civil emergency immediately after the explosion which occurred just after noon PDT on May 12, 2003. A primary purpose of the local proclamations was to bring in resources from outside the city and county, above and beyond those accessible through existing mutual aid agreements with emergency services departments in neighboring jurisdictions.

Shortly thereafter, the governor signed a proclamation declaring a state of emergency in western Washington, authorizing the establishment of food control areas and food embargoes by the Washington State Department of Health and Agriculture. The State Emergency Operations Center (EOC) received a copy of the proclamation at 1432 PDT, and it was forwarded to the Joint Operations Center by 1446 PDT.

The WA Governor signed a request for a declaration of major disaster under authorities of the Stafford Act at 1620 PDT on May 12, 2003. This request was received by the White House at 2330 EDT, and signed by the President (notional) at 0900 EDT on May 13, 2003.

b. Illinois venue (all times Central Daylight Time)

In contrast to the explosion in Washington, the disaster unfolded silently in Illinois. Cases of a mysterious respiratory illness first appeared on May 12, 2003. The first awareness of a potential pattern was observed around 1730 CDT on May 12 when the Pro-Net surveillance system[29] noted a cluster of respiratory cases at Edward Hospital in DuPage County. The illness was presumptively diagnosed as Pneumonic Plague on the morning of May 13 as cases began to mount, and a bioterrorism attack was suspected. Illinois Operational Headquarters and Notification Office soon thereafter activated Phase I of the Public Health Emergency Plan.

Just after noon CDT on May 13, 2003, the Chicago Director of the Office of Emergency Management (OEM) recommended a declaration for a state of emergency in Chicago, which authorized the city to take necessary actions, such as ordering people to shelter-in-place. Meanwhile, Cook, DuPage, Kane, and Lake Counties (the "collar" counties surrounding the City of Chicago) were initiating county-level declarations of emergency as well, and, together with FEMA, discussed whether to issue a joint declaration of disaster. The collar counties agreed that news of the county declarations should be announced jointly. At about the same time the IL Governor signed the Proclamation of a State of Emergency for Illinois. There was some question as to whether this proclamation made local proclamations of emergency moot, though they ultimately realized that local declarations were required to initiate local emergency authorities. A joint Chicago/Cook County Declaration of Emergency was signed at 1500 CDT and the Chicago OEM issued a news release announcing a state of emergency due to Pneumonic Plague at 1510 CDT.

At 1730 EDT on May 13, 2003, after consultations with Illinois officials and confirmation that the disease was Pneumonic Plague, the HHS Secretary declared a Public Health Emergency for Illinois. Meanwhile, the IL Governor sent a request for a Declaration of Major Disaster under the authorities of the Stafford Act to the President through FEMA Region V at 1700 CDT. Upon

[29] The Pro-Net surveillance system collects syndromic information from hospitals in DuPage County using a Web-based interface. The data are evaluated by software to determine if there are any unusual clusters or trends occurring. If an unusual spike in cases is detected the system alerts the local public health responders via a pager system.

receipt of the IL Governor's request for a Presidential Declaration of Major Disaster, FEMA Region V advised: "Although the Governor requested a major disaster declaration, under the Stafford Act definitions, an emergency declaration is FEMA's most appropriate immediate action." Accordingly, FEMA recommended that the President (notional) issue an emergency declaration, with "Individual Households Program and Categories A and B under Public Assistance [being] made available in the following jurisdictions: Cook (including City of Chicago), DuPage, Kane, and Lake Counties." A Presidential Declaration of Emergency was approved at 1105 EDT on May 14, 2003. There was some confusion among participants as to whether the request for a Declaration of Major Disaster was approved, but it was not.

4. Artificialities

The FSE artificialities did not substantively impact participant play or the conclusions in this topic area.

5. Analysis

The declaration of the public health emergency in the Chicago area was enacted with little confusion or difficulty in execution. However, it appeared that the state and local declaration processes in Illinois were at times confused. Members of the Illinois Emergency Management Agency and Illinois Department of Public Health for example, discussed whether a county-level declaration needed to be enacted in light of a state declaration of emergency, and there was some confusion among the collar counties as to the status of the different jurisdictions' declarations at various points in time. Also, there was some confusion in the Illinois State EOC as to whether the request for a Presidential Declaration of Major Disaster under the Stafford Act had been approved, which it had not—a Declaration of Emergency was approved.

Furthermore, although the process of obtaining a Presidential Disaster Declaration went smoothly in Washington, it was not as smooth in Illinois. Officials in Illinois requested a major disaster declaration to obtain maximum Federal assistance for the growing bioterrorism disaster, out of concern for the perceived five million dollar limit and other limits to Federal assistance in declarations of emergency. Some were unaware that the President can approve an expenditure of funds and approve services in excess of these limits under the conditions described above. For example, Illinois participants were not sure if the declaration authorized the Substance Abuse and Mental Health Services Administration (SAMHSA)/FEMA crisis counseling program. The FSE did not play out long enough to trigger the need for assistance in excess of those services allowed, or to allow for the Federal government to determine whether funds could be spent on programs not specifically named under Emergency Declarations of the Stafford Act.

It is interesting to note that the outbreak of plague in Illinois did not qualify as a major disaster by definition in the Stafford Act; biological disasters are not referenced in the Act. It is not clear from the FSE whether the difference in declaring an emergency or a major disaster would result in substantive real-world issues given the exception clauses under declarations of emergency described above.

6. Conclusions

Both of the simulated terrorist attacks in the FSE led to local declarations of emergency by multiple affected jurisdictions. The bioterrorism attack in Illinois was especially challenging in this arena with a widespread impact involving multiple counties, the City of Chicago and the State of Illinois.

SUMMARY OF CONCLUSIONS—DECLARATIONS:

In Washington, the proclamation and declaration processes went smoothly during the FSE. In Illinois, however, there was more confusion.

Future efforts should continue to explore the applicability of the Stafford Act to biological and other non-explosive terrorist emergencies that do not qualify as a major disaster, as currently defined by the Act.

While there was little confusion regarding the activation of the Public Health Act, the relationship between it and the Stafford Act, especially the authorities and resources that are brought to bear under them, should continue to be exercised.

Since there is no real-world precedent in which the Stafford Act has been applied to a biological disaster—or one involving non-explosive radiological, chemical, or biological weapons—it is noteworthy that during the FSE, the large-scale bioterrorism attack did not qualify as a major disaster. Future efforts, including exercises, should continue to refine the applicability of the Stafford Act to bioterrorism and other non-explosive disasters not explicitly defined by the Act, to increase Federal, State, and local (FSL) agency familiarity with its application to, and implications for, such disasters.

Finally, while the FSE did not necessarily indicate confusion with activation of the Public Health Act, or the declaration by HHS of a Public Health Emergency; the relationship between these authorities (and the resources that are brought to bear under them) and those available through the Stafford Act should continue to be exercised for maximum clarity at all levels of government.

This page intentionally left blank

C. Department of Homeland Security Play in T2: The Role of the Principle Federal Official

1. Introduction

The Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE) was the first opportunity for the newly created Department of Homeland Security (DHS) to exercise and experiment with its organization, functions, and assets. Figure 7 depicts the organization of DHS.

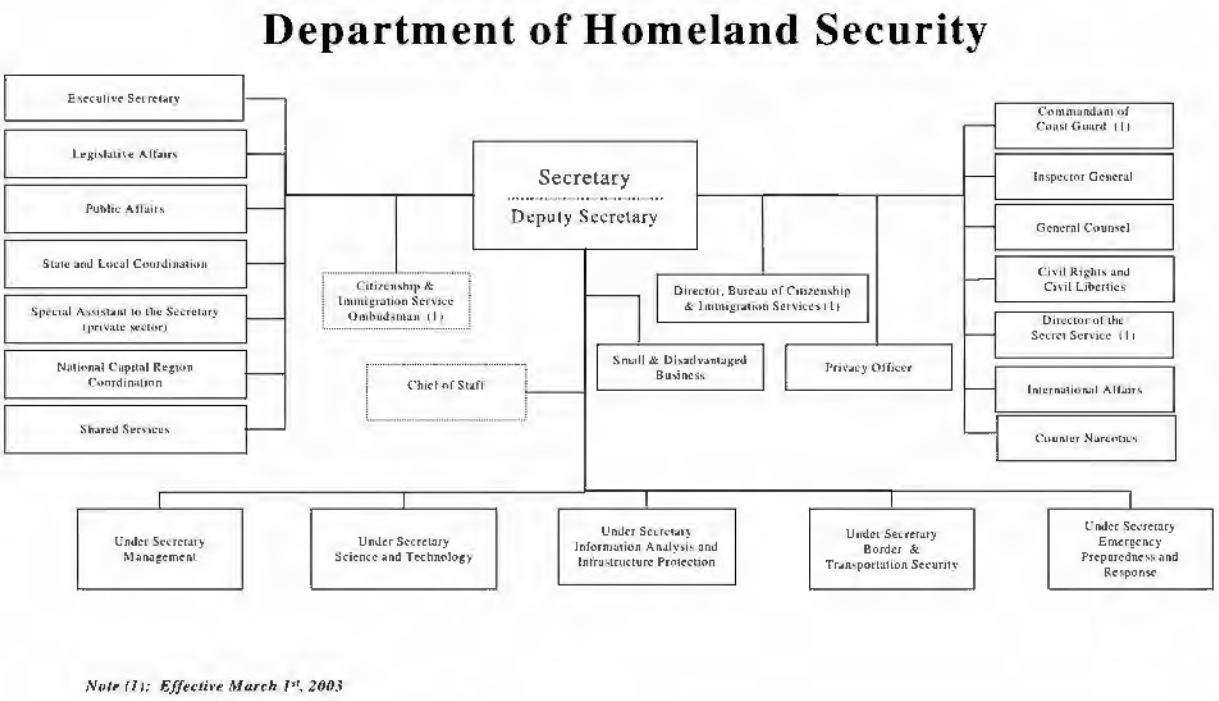


Figure 7. Organization of the U.S. Department of Homeland Security

Table 4 lists those DHS directorates, offices, and agencies for which the analysis team has data documenting their activities in the FSE. Table 4 includes, when available, a summary of the FSE activities of these organizations and the assets they deployed during the exercise. It is important to note that other DHS organizations, such the Office of Emergency Response, played important roles in the FSE, but data collectors were not present at their Emergency Operations Centers or Headquarters.

A number of DHS emergency response assets were set up or deployed for the first time during the FSE. These include new entities that report directly to the DHS Secretary: the Crisis Action Team (CAT) and the Principle Federal Official (PFO).

During the FSE, the CAT reported to the DHS Secretary or Chief of Staff. The CAT was the Secretary's assessment and advisory team, providing the information and recommendations needed to make decisions and advise the President. In addition to the DHS directorates, offices,

and agencies listed in Table 4 that had representatives in the CAT, liaisons from the White House, Federal Bureau of Investigation (FBI), Environmental Protection Agency, and Nuclear Regulatory Commission were also stationed in the CAT. The Department of Health and Human Services (HHS) and Department of Energy (DOE) liaisons were in the DHS Homeland Security Center across the hall rather than in the CAT.[30] This is surprising given that DOE was the lead technical agency for the radiological response in Washington and HHS was the lead technical agency for the public health response in Illinois.[31]

The DHS Secretary designated PFOs and deployed them to the Washington and Illinois venues. The PFO's role in emergency response was first implemented during T2, and is now being codified by DHS. Based upon PFO activities during the FSE, the PFO will serve a pivotal role in the response capabilities of DHS. To further support the efforts of DHS to define the roles and responsibilities of the PFO, this section focuses on the PFO activities, interactions, and lessons learned from the FSE. Because it is focused on the activities of individuals as opposed to organizations, the reconstruction presented in this section is much briefer than that presented in other sections. It is important to note that the analysis team had an analyst with the Seattle PFO allowing for a fairly detailed reconstruction of the PFO's interactions and activities. The reconstruction and observations for the Illinois PFO are based upon information from data collectors, and as a result, a detailed timeline for the PFO activities in the Illinois venue was not developed.

[30] HHS had personnel limitations during this exercise due to real-world commitments, including Severe Acute Respiratory Syndrome (SARS). This resulted in a choice to staff the Homeland Security Center full-time, but meant they did not have representation in the Crisis Action Team (CAT).

[31] For additional information about the CAT, see the *Stanford Report* in Annex B.

Table 4. Directorates, Offices, and Agencies within the Department of Homeland Security That Played in T2[32]

DIRECTORATE/OFFICE/ AGENCY	ACTIVITIES/ASSETS DEPLOYED
Border and Transportation Security (BTS) Directorate	• Bureau of Customs and Border Protection (CBP) activated the CBP Command Center • The Transportation Security Administration activated its Crisis Action Center • Immigration and Customs Enforcement/Federal Protective Services activated its Communications Center, Situation Room • Participated on Crisis Action Team (CAT)
Emergency Preparedness and Response (EPR) Directorate	• Activated the National Interagency Emergency Operations Center, Emergency Support Team at EPR headquarters • Deployed assets including Domestic Emergency Support Team, Federal Coordinating Officers, Mobile Emergency Response System, National Disaster Medical System, Strategic National Stockpile, and Urban Search and Rescue Incident Support Teams • Participated on CAT
Science & Technology Directorate	• Participated on CAT
Information Analysis and Infrastructure Protection Directorate	• Participated on CAT
U.S. Coast Guard	• Activated Crisis Action Center • Participated on CAT
U.S. Secret Service	• Activated Director's Crisis Action Center
Office of International Affairs	• Participated on CAT
Office of Legislative Affairs	• Participated on CAT
Office of Public Affairs	• Participated on CAT
Office of State and Local Government Coordination	• Participated on CAT
Office of National Capital Region Coordination	• Participated on CAT
General Counsel	• Participated on CAT
Private Sector	• Participated on CAT

[32] The offices and agencies in this table represent only those for which the analysis team has data.

2. Background

The concept of a PFO is laid out in Homeland Security Presidential Directive (HSPD)-5: "the DHS Secretary is named as the PFO for the management of terrorist attacks, major disasters, and other emergencies in the United States"[33].

The duties and responsibilities of the PFO are further elaborated upon in the draft National Response Plan (NRP):[34]

> ***Principle Federal Official.*** *The Federal official responsible for directing Federal operations in the United States to prepare for, respond to, and recover from domestic incidents; for directing the application of Federal resources in specific circumstances; and for managing any domestic incident when directed by the President.*[35]

The draft NRP continues, stating that the DHS Secretary can name a senior Federal official as the Secretary's senior representative at the incident. This person oversees the federal response in the field. The responsibilities of the Secretary's representative include:

- Coordinating and synchronizing the activities of primary Federal agencies and supporting agencies;
- Overseeing the allocation of resources for response and recovery;
- Coordinating the release and distribution of information; and
- Communicating with the Secretary.[36]

The draft NRP gives the Secretary's representative some authorities that traditionally were those of the Federal Coordinating Officer (FCO) and the FBI Special-Agent in Charge (SAC) under the existing FRP and U.S. Government concept of operations plan (CONPLAN)[37].

3. Reconstruction

a. Washington venue (all times are Pacific Daylight Time)

Mike Byrne, the DHS Director of National Capital Region Coordination for Emergency Response, was appointed the PFO in Washington. Figure 8 lays out a reconstructed timeline of his activities in the Washington venue. He notionally deployed with the Domestic Emergency Support Team (DEST), prior to the radiological dispersal device (RDD) explosion in Seattle, in response to exercise intelligence citing a possible terrorist attack at the Columbia

[33] Homeland Security Presidential Directive/HSPD-5, February 28, 2003.
[34] T2 did not exercise the draft National Response Plan.
[35] United States Government National Response Plan (draft)
http://www.nemaweb.org/docs/National_Response_Plan.pdf
[36] Ibid.
[37] Ibid.

Generating Station near Richland, Washington.[38] Mr. Byrne was notified of the proposed diversion of the DEST from Richland to Seattle on May 12, 2003, at 1235, and he arrived at the Joint Operations Center (JOC) in the FBI Field Office in Seattle at approximately 1700. At the JOC, he worked closely with the Federal Emergency Management Agency (FEMA) Region X Director, senior DOE officials, and the FBI SAC.

Upon arrival, Mr. Byrne established a unified command where all Federal agencies with jurisdictional authorities contributed to the process of determining overall incident objectives, selecting strategies, ensuring integrated operations, and maximizing use of all resources. To ensure that the federal response was coordinated and that action plans were consolidated, Mr. Byrne led regular briefings with his Command Group, consisting of the DEST and liaisons from key Federal, State, and local jurisdictions and agencies. These briefings focused on the status of the response, assets deployed, consensus building, and the development of recommendations to present to the State and local authorities.

Mr. Byrne also directed that all federal communications would be integrated so that there was one consistent voice speaking for the Federal Government. In addition, he worked to ensure that the integrated federal communications was consistent with communications coming from the State and local authorities. He instructed the FBI JOC to be more forthcoming with information to both State and local authorities and with the JOC Consequence Management Group (CMG). Mr. Byrne also initiated and led regular conference calls with top officials (or their representatives) from Seattle, King County, Washington State, and FEMA. In these conference calls, he discussed current federal support, offered recommendations, responded to questions concerning issues raised by the State, county, and city officials, and tried to assure Seattle, King County, and Washington State officials that they had the same information that he had.

He was also concerned about the apparent lack of integrated communications prior to his arrival between the Joint Information Center (JIC) and DHS and took steps to rectify the problem. For example, he discovered that DHS had raised the threat level to Red in seven cities, closed roads and airports, placed restrictions at border crossings *without a message ever coming to the Washington JIC or JOC.* To rectify the situation, he instructed the JIC to provide a liaison to the JOC CMG and to communicate more regularly with DHS.

Mr. Byrne also kept in touch with DHS Headquarters through regular conversations with the DHS CAT.

[38] From the U.S. Government Inter-agency Domestic Terrorism Concept of Operations Plan: "The DEST is a rapidly deployable, inter-agency team responsible for providing the FBI expert advice and support concerning the U.S. Government's capabilities in resolving the terrorist threat or incident. This includes crisis and consequence management assistance, technical or scientific advice and contingency planning guidance tailored to situations involving chemical, biological, or nuclear/radiological weapons." Note that the DEST is now a DHS-managed asset that supports the Lead Federal Agency during a terrorist threat or incident.

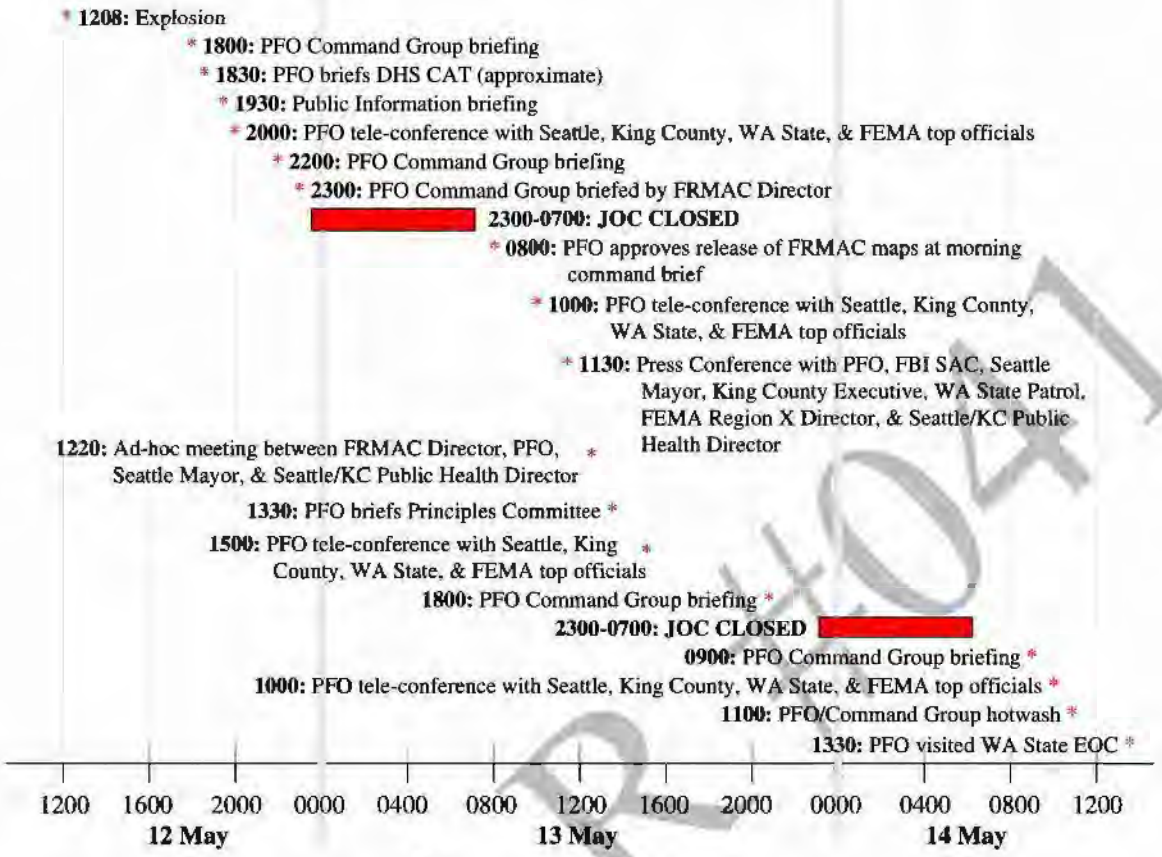


Figure 8. Outline of Principle Federal Official Key Events in Washington State (all times are Pacific Daylight Time)

b. Illinois

Wayne Parent, the Operations Coordinator for the Border and Transportation Security Directorate in DHS, was appointed the PFO in Illinois. In the Illinois venue, the PFO spent the first two days in the FEMA Regional Operations Center (ROC) and moved to the JOC when it stood up on May 14, 2003. At the ROC, he worked closely with the FEMA Region V Director. At the JOC, he worked with the Region Director (RD), the SAC, and the FCO.

As PFO, Mr. Parent ensured that communications were integrated, action planning between the SAC and the RD was coordinated, and that State and local officials that were actively involved. His approach was to foster consensus among the jurisdictions and agencies. To that end, a series of regularly scheduled teleconferences was held with Federal, State, and local (FSL) agencies. These calls featured briefings, coordination, de-confliction, and decision-making. Typically, Mr. Parent did not have to adjudicate among agencies; the teleconferences and follow-up discussions resulted in decisions reached through consensus.

Mr. Parent kept in touch with DHS headquarters through regular morning and evening conversations with the CAT leader. He also contacted the CAT leader when issues arose, with a total of four or five contacts per day. He provided an encapsulated situation report to the CAT during the evening conversation.

4. Artificialities

By design and consistent with the open book nature of the FSE, the PFO arrived in Chicago a week before the exercise and met in advance with many of the officials involved. In fact, HHS provided the PFO with a subject matter expert (SME) before he was officially appointed PFO. In addition, both PFOs had advance knowledge of the scenario. Thus, they had more situational awareness of the specific players and of the situations they would each be facing than a typical PFO would likely have in an actual incident. This is not a criticism of the PFOs; in fact, it likely enhanced the learning opportunity for DHS and all FSL agencies involved.

5. Analysis

a. The relationship between DHS and FEMA

The relationship between the PFO and the FEMA officials was different in the two venues. In Washington, Mr. Byrne's activities were consistent with his concept for the PFO role. This concept involved the development of a Command Cell, consisting of the PFO, FCO, FBI SAC, and State and local counterparts for the response phase of an incident. As envisioned, the PFO would prioritize and adjudicate between the often-competing needs of the crisis and consequence management sides of the response phase. This allowed the FBI SAC and the FCO to concentrate completely on their respective aspects of the response. Under this concept, the PFO truly became the one voice for the federal response. Mr. Byrne's view of the PFO role was clearly observed during the FSE. As PFO, he quickly instituted a unified command to manage the overall federal response and coordinate integrated communications and action planning, but left the FBI SAC to coordinate the crisis response, and left the FEMA RD and the FCO to coordinate the day-to-day activities of the federal consequence management assets.

It is important to remember that in Washington, although an RDD device was involved, the event unfolded in more of a traditional first responder fashion with a relatively well-delineated disaster site[39]. With the rapid discovery of radiation, federal assets quickly came into the exercise picture and, importantly, a JOC was quickly established. In Illinois, events unfolded more gradually as would be expected during a disease outbreak. There were no clearly defined disaster sites (although release sites were eventually identified) and the JOC stood up a couple of days into the event. Mr. Parent worked within the framework of a unified command to ensure that integrated communications were achieved and that action plans were coordinated, but did so in a less overt manner than Mr. Byrne.

The different approaches to the role of the PFO suggest that DHS should take this opportunity to clearly de-conflict and define the responsibilities of the PFO with respect to the FEMA RD and FCO in the final NRP. The relationship may differ depending on the circumstances, but general guidelines need to be formulated and implemented. In addition, the PFO roles and responsibilities defined in the draft NRP may or may not be appropriate during the recovery phase of disasters. Since the recovery phase was not examined in much detail during the FSE, further exercises will be needed to shed some light on this issue.

[39] The uncertainties that responders faced at the RDD incident site are discussed in detail in the *Special Topics* sections: "Data Collection and Coordination: RDD Plume Modeling and Deposition Assessment" and "Balancing the Safety of First Responders and the Rescue of Victims."

b. PFO Resources

During the FSE, both PFOs required additional technical support beyond their administrative and security details to accomplish their respective roles and responsibilities. In Washington, Mr. Byrne used the DEST and, in some cases, the JOC CMG to support his efforts. He informed the evaluation team that the DEST has the capability to support the PFO, FCO, and FBI SAC during the response phase of an emergency if they are all co-located as a Command Cell. This has the added benefit of reducing redundancy, as Emergency Support Function personnel would not be needed to staff both the JOC CMG and the FEMA ROC.

In Illinois, Mr. Parent was provided with an SME from HHS after a meeting with the head of the HHS Secretary's Emergency Response Team (SERT). Mr. Parent reported to the evaluation team that this support was essential to helping him understand the specifics of the bioterrorism event and the critical role that HHS would play in a real-world event.

6. Conclusion

The FSE presented DHS with an excellent opportunity to evaluate and exercise emergency response procedures, teams, and assets. During the FSE, both PFOs encouraged and facilitated integrated communications and coordinated action planning. They also both encouraged active communication with State and local authorities. While their leadership styles may have differed, the roles that each PFO had during the FSE may have also reflected, to a degree, differences in the problems that each encountered and that the terrorist attacks developed differently in the two venues.

SUMMARY OF CONCLUSIONS—PFO:

- The PFO was well received by Federal, State, and local authorities during the T2 FSE.
- The roles and responsibilities of the PFO vice the FEMA FCO, FEMA Region Director, and FBI SAC need to be further clarified in the final National Response Plan.
- The PFO requires a dedicated staff with the flexibility and expertise to support all emergencies.

While the concept of the PFO was well-received, the roles and responsibilities of the PFO compared to those of the FEMA RD, the FEMA FCO, and the FBI SAC still need to be clarified. In addition, the PFO requires a staff with the flexibility and expertise to support all emergencies, natural and terrorist-related. If the DEST is expected to support the PFO and the Federal response, DHS should consider providing enough resources to staff at least one additional team in the event that more than one federal emergency occurs at the same time, as was exercised in the T2 FSE.

D. Data Collection and Coordination: Radiological Dispersal Device Plume Modeling and Deposition Assessment In Washington

1. Introduction

During the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE), designers simulated the explosion of a radiological dispersal device (RDD) in Seattle, Washington. In the aftermath of an RDD explosion, the development of analysis products, including plume prediction models and radiological deposition maps, which show the potential impact of the radiation on people, agriculture, and the environment, is vital. These maps provide policy-makers and top officials with the information they need to make effective decisions.

In the initial hours following an RDD explosion, radiation experts rely on predictive plume models to give decision-makers a rough sense of how current weather conditions affect where the radioactive materials are likely to spread. As responders learn more information about the explosion—such as an estimate of the amount of explosives and the type(s) of radiological material used—additional data can be entered into the predictive plume models. Model outputs can then be used to update the prediction maps. During the FSE, different agencies and jurisdictions used one or more plume models to generate predictions, which led to both confusion and frustration among top officials in Washington State and Washington, D.C.

As the response progresses and empirical data are collected in the field, deposition or "footprint" data products are developed. For these products to be useful to decision-makers, subject matter experts (SMEs) must first interpret the data to determine the impact on people, agriculture, and the environment using Environmental Protection Agency (EPA) Protective Action Guidelines (PAG).[40]

All radiological data collected by Federal, State, and local (FSL) agencies should he coordinated so that SMEs can develop the most up-to-date data products, and top officials in different locations have consistent information upon which to base their decisions. For Federal agencies, the Federal Radiological Emergency Response Plan (FRERP)[41] assigns data coordination to the Federal Radiological Monitoring and Assessment Center (FRMAC). During the T2 FSE, however, coordinating data collection proved to be a significant challenge. As a result, FSL agencies that developed data products and deposition maps used different and incomplete data. A further challenge during the FSE was the distribution of the many data products generated throughout the exercise. In addition, confusion was apparent over the differences between maps

[40] EPA is assigned the responsibility for developing Protective Action Guidelines (PAGs) under various authorities, including the Radiological Emergency Planning and Preparedness Regulation (44 CFR 351). EPA coordinates the interagency development of the PAGs through a subcommittee of the Federal Radiological Preparedness Coordinating Committee.

[41] The Federal Radiological Emergency Response Plan (FRERP) (50 FR 46542), of 11-8-85, revised 1996.

generated from predictive plume models vice empirical data products and deposition maps. The impact on top officials was delayed decision-making or, in some cases, policy decisions that were made under conditions of uncertainty. Although decision-making under rapidly changing and ambiguous situations is always part of emergency response, overcoming the data coordination and analysis product distribution challenges can reduce the uncertainty observed during the FSE.

Two critical issues had a significant impact on the response observed during the T2 FSE:

- Coordinating the data collected by multiple agencies at FSL levels of government; and
- Developing and distributing analysis products—including plume model prediction overlays and empirical deposition, footprint maps—to subject matter experts (SMEs) and decision-makers by multiple FSL agencies.

In real emergencies and during the FSE, these two issues interact to impact decision-makers. Figure 9 shows what might be considered an ideal picture of the data collection, coordination, and product distribution process. Under most circumstances, data collection will take place in multiple locations and involve multiple agencies. The challenge is for all of these agencies to coordinate their data collection efforts and send all of the data to an agreed upon clearinghouse where it is interpreted, entered into a prediction model or developed into deposition maps, and then provided to SMEs and decision-makers. Again, for Federal agencies, this is the responsibility of the FRMAC as described in the FRERP.

However, if FSL agencies send their raw data to different locations, rather than a centralized location, and there is no coordination among the different agencies, then analysis will not be conducted with the complete data set. If the analysis and the resulting analysis products are not consistent, then top officials and policy-makers will have differing, and potentially conflicting, information. Such conflicts will impact officials' ability to develop consistent and agreed upon decisions. Follow-on legal implications and negative public perception are also potential results of a poorly-coordinated FSL response.

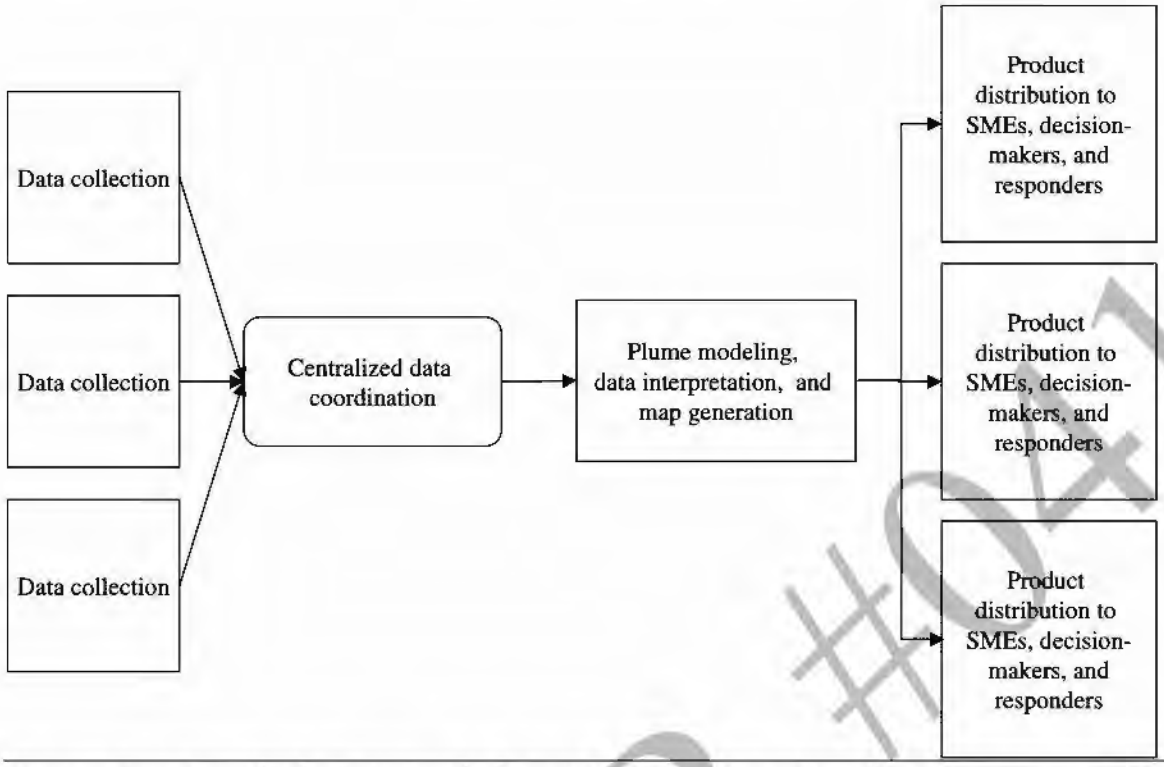


Figure 9. An Ideal Picture of the Data Collection, Coordination, Interpretation, and Dissemination Process

This special topic begins with a discussion of the FSL agencies and departments that have responsibilities or authorities under current FSL codes and inter-agency agreements to collect and coordinate radiological data; conduct analyses; and provide models, maps, and other analytic products in radiological emergencies. This background information is followed by a reconstruction of the events that occurred during the FSE and an analysis of the reconstruction. Finally, the last section contains conclusions based upon the analysis of the FSE and the existing codes and authorities.

2. Background

In the aftermath of an explosion containing radioactive materials, the detection of radioactivity will lead to a number of agencies being called to the scene. Some states, including Washington, have robust radiological incident management capabilities, and, therefore, provide State-owned assets to the incident. In addition, they can draw upon Federal assets from the Department of Energy (DOE), Environmental Protection Agency (EPA), Department of Health and Human Services (HHS), United States Department of Agriculture (USDA), the Nuclear Regulatory Commission (NRC), and others to augment their efforts.

Although capabilities for radiological detection across the United States and territories vary, the issues that arose during T2 are likely too generalized for many localities across the country. Therefore, it is useful to understand Seattle and Washington radiological detection capabilities and how their terrorism response plans are designed to integrate resources to create a unified

response. A discussion of the primary federal assets that have radiological response capabilities, focusing on agencies and departments that participated in T2, is also included.[42]

a. City and state response capabilities

Seattle capabilities

Seattle Fire Department (SFD) Hazardous Materials (HAZMAT) vehicles and equipment have dosimeters that detect radiation. SFD HAZMAT personnel are likely to be the first radiation data collectors to arrive at a scene with suspected radioactive materials.[43]

Washington State capabilities

- *Washington State Department of Health*:

In the Division of Environmental Health Programs, the Washington State Department of Health (DOH) maintains a Division of Radiation Protection. The division includes expert handlers of radioactive materials and incident management. DOH field team coordination is conducted from the Radiation Monitoring and Assessment Center (RMAC). The RMAC has the capability to provide dose assessment for field teams, collect and coordinate radiological data, and develop protective action recommendations and sampling plans[44].

In the event of a radiological incident, the Washington State DOH Public Health Laboratory supports the efforts of the Division of Radiation Protection to determine the immediate health risk to the public. The mission of the laboratory is to provide information to health officials as quickly as possible so that they have the data they need to assess the level of hazard to the public. The Radiation Chemistry Group rapidly performs radiological analyses to determine what radioactive materials are present in samples collected at an emergency site and can detect activity levels relevant to protective action guidelines[45].

- *Washington State Department of Ecology*:

Under the Spill Response Section in the Spill Prevention, Preparedness, and Response Program, the Washington State Department of Ecology maintains the Ecology Spill Response Team. While DOH has the overall authority in Washington State for radiological incidents, the Department of Ecology is often called upon for assistance since the Ecology Spill Response

[42] The evaluation team is unaware of any King County radiological data collection teams or formal modeling capabilities at the King County EOC.

[43] There are nationwide efforts to increase the percentage of US jurisdictions with radiological detection capabilities. In July 2002, the U.S. Departments of Energy and Justice co-sponsored the Homeland Defense Equipment Reuse program (HDER). HDER provides surplus instrumentation and equipment to State and local fire, police and other emergency agencies to enhance their domestic preparedness capabilities. In FY 2003, deliveries to the pilot program cities included shipments to Philadelphia, Washington DC, Chicago, Detroit, Houston, Los Angeles, and San Francisco. In June 2003, the program was scheduled to go nationwide allowing all US states, the District of Columbia, Puerto Rico and the four US Territories to participate in the program and receive equipment, training, and local long-term technical support.

[44] Washington State Department of Health, Division of Radiation Protection Plan and Procedures for Responding to a Radiological Attack, DOH/DRP, March 2003.

[45] Information obtained from personal communication with DOH Public Health Laboratory personnel.

Team carries radiological monitoring instrumentation in all of their HAZMAT response vehicles[46].

- *National Guard Weapons of Mass Destruction-Civil Support Teams*:

The Civil Support Teams (CSTs) are congressionally-mandated units of the National Guard whose mission is to support State and local authorities at a domestic weapons of mass destruction (WMD) incident site. The CST supports civilian authorities by identifying WMD agents, advising for response measures, short- and long-term consequences, and facilitating the request of additional resources. The CST is a State-owned asset that can deploy without a Department of Defense (DOD) authorization. The Adjutant General can deploy the CST to support the state's response or to support another state's response if requested by that state's governor.[47]

The CSTs are equipped with military standard radiation detection equipment. The survey team is also equipped with a handheld gamma spectrometer that provides the capability to identify specific gamma-emitting isotopes. The CSTs also have the capability to deploy with a mobile analytical laboratory system (MALS) to conduct on-site radiological isotope analyses.[48]

b. Federal response capabilities and assets

Department of Energy

The National Nuclear Security Administration (NNSA) administers the many DOE assets that can be activated to respond to a radiological incident. These include:

- *Radiological Assistance Program*:

In the event of a radiological incident, the Radiological Assistance Program (RAP) provides radiological assistance when requested by other Federal agencies, states, local, or tribal authorities. A request for assistance normally comes first into one of eight DOE regional coordinating offices, specifically the Regional Response Coordinator (RRC). The initial response is typically a regional team of specifically trained personnel and resources that support the local authorities. The RRC has the authority to request one or more of the DOE assets (e.g., Atmospheric Release Advisory Capability, Aerial Measuring System, FRMAC, Radiation Emergency Assistance Center/Training Site, and other RAP regions) to support the response and to facilitate coordination between the DOE assets and other responding agencies.[49]

- *Federal Radiological Monitoring and Assessment Center*:

According to the FRERP,[50] DOE is responsible for setting up and coordinating a FRMAC during the crisis phase of any radiological incident. Specific procedures are used to collect, analyze, assess, and disseminate data products useful to decision-makers. The efforts of all FRMAC

[46] Information obtained from personal communication with Washington Department of Ecology personnel.
[47] In Washington the commanding officer of the WMD-CST has the authority to self deploy his unit.
[48] This information was obtained from communication with LTC Thomas Hook, Army National Guard, Chief, Civil Support Team Program, National Guard Bureau Homeland Defense Division.
[49] Department of Energy, *Radiological Assistance Program*, (DOE 5530.3). Other information found at http://www.doe.bnl.gov/RAP/rap.htm.
[50] The Federal Radiological Emergency Response Plan (FRERP) (50 FR 46542), of 11-8-85, revised 1996.

members are coordinated through these procedures to maximize efficiency and minimize confusion in their advice to decision-makers. Without such a coordinated effort, conflicting data products and excessively technical information may complicate decision-making. Once the FRMAC is established, all activated Federal assets are incorporated, and State and local technical experts are invited to co-locate and provide support to the FRMAC. Following the emergency phase, at a mutually agreeable time corresponding to the requirements found in the FRERP, the NNSA will transfer the responsibility of coordinating the FRMAC to the EPA. However, the NNSA and other federal agencies continue to support and provide resources to the FRMAC.[51]

The FRERP also calls for the establishment of the Advisory Team for Environment, Food, and Health (Advisory Team, or A-Team), which, while not a DOE asset, is co-located with the FRMAC. The A-team includes representatives from multiple Federal agencies and departments, including the EPA, USDA, HHS, and other Federal agencies, as warranted by the circumstances of the emergency. The A-team's primary responsibility is to provide the lead Federal agency (LFA) with advice on environment, food, health, and safety issues that arise during and from the emergency. The A-team provides direct support to the LFA but does not have independent authority.[52]

- *Atmospheric Release Advisory Capability*:

Through the Atmospheric Release Advisory Capability (ARAC) program the DOE maintains the National Atmospheric Release Advisory Center (NARAC) at Lawrence Livermore National Laboratory (LLNL). NARAC provides atmospheric plume modeling tools and services for chemical, biological, radiological, and nuclear airborne hazards (both gases and particles) using real-time access to worldwide meteorological observations and forecasts through redundant communications links to data provided by the National Oceanic and Atmospheric Administration (NOAA), the U.S. Navy, and the U.S. Air Force. NARAC supports the Nuclear Incident Response Teams, the regional RAP teams, the Aerial Measuring System (AMS), the FRMAC, DHS under a DOE-DHS Memorandum of Agreement, and 40 DOE and DOD on-line sites. NARAC operational support of five cities and 53 state and Federal organizations across the country has been successfully tested under DHS and DOE support. NARAC can simulate downwind effects from a variety of scenarios, including fires, radiation dispersal device explosions, HAZMAT spills, sprayers, nuclear power plant accidents, and nuclear detonations. The NARAC software tools include stand-alone local plume modeling tools for end user's computers, and Web- and Internet-based software to reach-back to advanced modeling tools and expert analysis from the national center at LLNL. Initial automated, advanced 3-D predictions of plume exposure limits and protective action guidelines for emergency responders and managers are available in five to ten minutes. These can be followed immediately by more detailed analyses by 24/7 on-duty or on-call NARAC staff. NARAC continues to refine calculations as measurements are taken, until all airborne releases have stopped, and until the hazardous threats are mapped and impacts assessed. Model predictions included the 3-D and time-varying effects of weather and terrain. NARAC provides a simple Geographical Information System (GIS) for display of plume predictions with affected population counts and detailed maps, in addition to

[51] Department of Energy, *FRMAC Operations Manual Emergency Phase*, (DOE/NV 11718-080 UC-707), May 1997. Other information found at http://www.nv.doe.gov/programs/frmac/default.htm.
[52] The Federal Radiological Emergency Response Plan (FRERP) (50 FR 46542), of 11-8-85, revised 1996.

the ability to export plume predictions to other standard GIS systems. NARAC products can be distributed through a password-controlled and encrypted website, e-mail or fax.

The Environmental Protection Agency

The EPA responds to radiological incidents under both the National Oil & Hazardous Substances Pollution Contingency Plan (NCP) and the FRERP. EPA can serve as the LFA, or can support State and local governments and the lead Federal agency by:

- Conducting environmental monitoring, sampling, and data analysis;
- Assisting responders in ensuring protection of Health and Safety;
- Assessing the national impact of any release on public health and the environment through the Agency's Environmental Radiation Ambient Monitoring System;
- Providing technical advice on containment and cleanup of the radiological contamination; and
- Assisting in site restoration and recovery.[53]

EPA's On-Scene Coordinators maintain emergency response readiness, including survey and sampling equipment, for chemical and radiological incidents. In addition to a region's response capability, EPA Headquarters can also deploy its Radiological Emergency Response Team (RERT) to the accident scene as part of its radiological response. EPA's RERT provides additional specialized monitoring, sampling, and both mobile and fixed laboratory capabilities. As part of the A-Team, EPA's RERT members can provide State and local authorities with advice on protecting local residents from exposure to elevated radiation levels. Once the FRERP is activated, EPA radiological assets are expected to integrate with the FRMAC.[54,55]

c. Requesting federal assets

State and local governments, as well as tribal governments and private organizations, can request support from a number of Federal assets to support their response and recovery efforts following an explosion that includes radioactive materials. For example, the EPA receives their authority to respond to any release of a hazardous substance from the National Oil and Hazardous Substance Pollution Contingency Plan (National Contingency Plan)[56] and the Public Health Services Act, among others. The DOE has similar authority to respond to a radiological incident as outlined in DOE 5530.3[57] to be superceded by DOE O 151.1A.[58]

---

[53] Environmental Protection Agency, *Radiological Emergency Response Plan*, January 2000. More information found at http://www.epa.gov/radiation/rert/index.html.

[54] EPA's regional responders provided support to the local Incident Command System during the FSE. In addition, EPA deployed the Advance Units of its RERT. However, given the limited timeframe of the exercise and limited funding, EPA did not deploy RERT members who would have realistically only been able to arrive at the incident scene as the exercise drew to a close.

[55] Information specific to the EPA RERT is found at http://www.epa.gov/radiation/rert/rert.htm.

[56] Title 40 Code of Federal Regulation (CFR) 300, National Oil and Hazardous Substance Pollution Contingency Plan.

[57] Department of Energy, *Radiological Assistance Program*, (DOE 5530.3). Other information found at http://www.doe.bnl.gov/RAP/rap.htm.

[58] Department of Energy, *Comprehensive Emergency Management System*, (DOE 0 151.1A).

In combining the responsibilities and authorities defined in the FRERP,[59] Concept of Operations plan (CONPLAN),[60] HSPD-5,[61] and the Federal Response Plan,[62] the following command and control functions—relevant to data coordination and plume modeling—were followed for Federal agencies during the FSE:

- DHS was designated the LFA, and coordinated the response from all Federal agencies; and
- DOE and EPA were technical support agencies to the LFA for the radiological aspect of the response; DOE was further responsible for coordinating the activities of the FRMAC.

d. Coordinating the data

There are many responders that can collect on-site and off-site radiological data following an explosion containing radioactive materials. To develop reliable (i.e., consistent) and valid information for decision-makers, it is important that the data collection effort be coordinated both on the ground and in terms of how the data flows and is turned into useful information for decision-makers. Coordinating the data flow can ensure that SMEs have all of the available data to use for analysis. This is one step to ensuring that the output—the information provided to policy makers and top officials—is consistent and valid in terms of the empirical data. Coordination on the ground also helps to minimize the likelihood that multiple agencies will perform redundant tasks or repeat tasks because of conflicting data reports. This is vitally important in an incident where responders face a high-risk environment.

The Washington State DOH Division of Radiation Protection Plan and Procedures for Responding to a Radiological Attack describes how the DOH should coordinate their radiological response on-site and with the FRMAC. Prior to the arrival of the FRMAC, the State Health Liaison (SHL) facilitates communication between the DOH staff at the Washington State Emergency Operations Center (EOC) and incident command regarding appropriate protective measures and decisions. The SHL provides the WA State EOC with radioactive release data, weather data, radiological data collected by field teams, predictive plume maps, and dose projections. Once the FRMAC is established, the SHL or Deputy State Health Liaison (DSHL) relocates to the FRMAC and assumes the role of FRMAC liaison. The WA State DOH response plan leaves the details of the coordination effort up to the SHL (or DSHL) and the FRMAC, which provides for the flexibility needed for each individual response. The FRMAC liaison is responsible for coordinating the State's response with the Federal response and for maintaining communication with the RMAC, the WA State EOC, and the Joint Information Center (JIC). Furthermore, the FRMAC liaison is responsible for determining when and how Washington State's response will be integrated with the Federal response.[63]

Typically, upon arrival at a crisis, the FRMAC Director works to coordinate with State and local agencies through an advance party meeting. The goals of the advance party meeting are to ensure that Federal representatives in the FRMAC are up-to-date on the crisis, identify points of

[59] The Federal Radiological Emergency Response Plan (FRERP) (50 FR 46542), of 11-8-85, revised 1996.
[60] United States Government Interagency Domestic Terrorism Concept of Operations Plan.
[61] Homeland Security Presidential Directive/HSPD-5, February 28, 2003.
[62] Federal Emergency Management Agency, *Interim Federal Response Plan*, January 2003 (9230.1-PL).
[63] Washington State Department of Health, *Division of Radiation Protection Plan and Procedures for Responding to a Radiological Attack*, DOH/DRP, March 2003.

contact for state representatives, and develop protocols for providing data products to top officials and SMEs at state and local EOCs and relevant agencies. The advance party meeting is a critical step providing unique information during each emergency—different states have different relationships with county and local governments; the FRMAC representatives need to understand these relationships to provide effective support. The Federal response effort relies on state representatives to help facilitate these relationships. State and local radiation experts are also invited into the FRMAC to provide a liaison between the Federal response assets and the state and local governments. By having state, and potentially local, representation at the FRMAC, local decision-makers are still relying on their own people for recommendations. These SMEs, however, have additional support from the Federal Government.[64,65]

e. Plume Modeling and Deposition Maps

In an RDD explosion, the bomb throws radioactive material into the air; the resulting radioactive debris cloud is called a plume. In the early hours following the explosion, the National Atmospheric Release Advisory Center (NARAC), the National Oceanic and Atmospheric Administration (NOAA), and the Defense Threat Reduction Agency (DTRA) can generate a prediction of the plume boundaries using sophisticated models. There are also several less sophisticated models available to develop a plume projection. To generate predictions, agencies need some basic information about the explosion and the radiological material involved (defined as the source term), the weather, and the topography surrounding the incident site. As more information about the explosion becomes available, the source term and the initial prediction are refined. Top officials can use these predictions to make preliminary decisions involving first responder safety, safe transit routes, and protective action guidelines for the public. The first plume prediction generated for SFD on May 12, 2003 by the Lawrence Livermore Atmospheric Release Advisory Capability (ARAC) model overlaid on the map of the Seattle region affected by the RDD explosion is shown in Figure 10.[66]

[64] The Federal Radiological Emergency Response Plan (FRERP) (50 FR 46542), of 11-8-85, revised 1996.
[65] Information obtained from personal communication with FRMAC personnel.
[66] For a detailed discussion of plume dispersion models, see the *Stanford Report*, an appendix to Annex B.

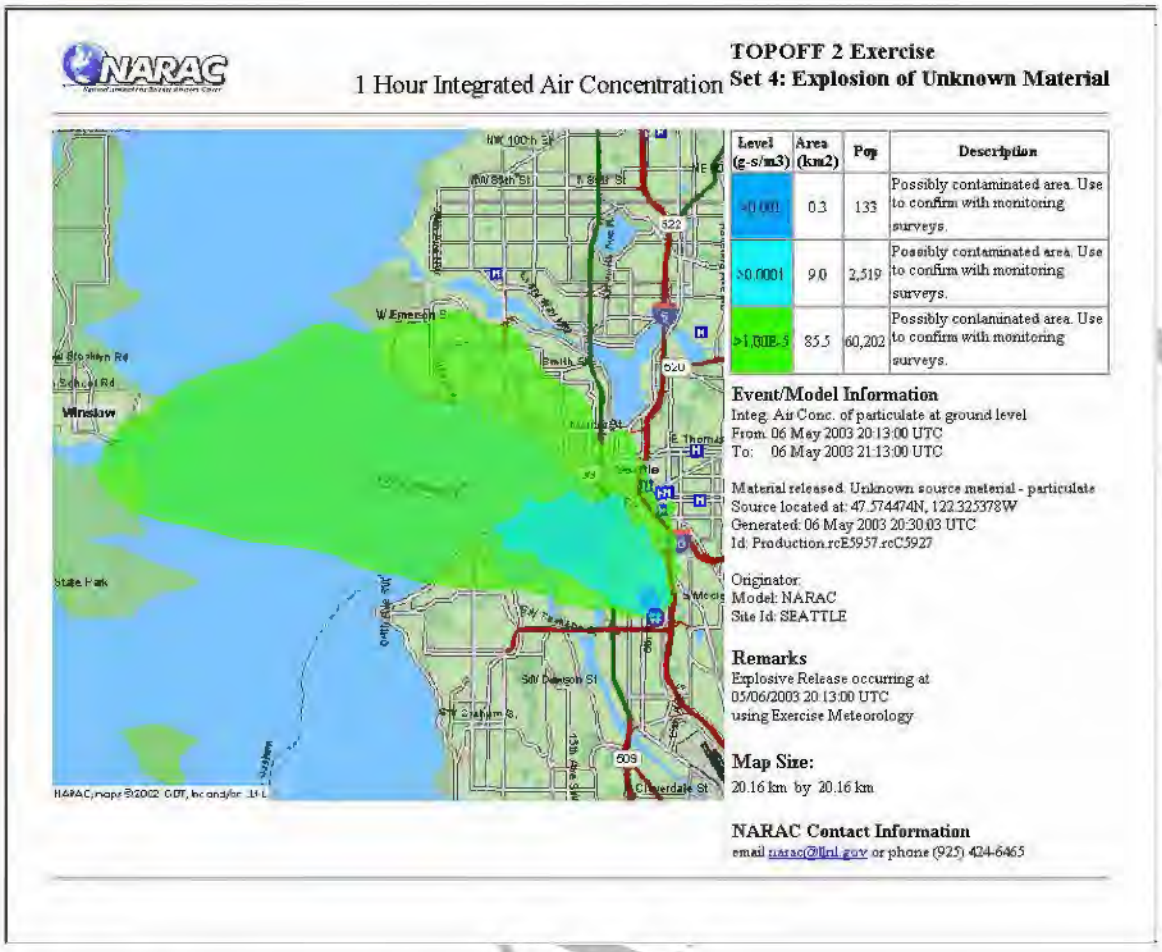


Figure 10. NARAC-Predicted Contaminated Areas

The plume predictions, alone, decrease in value after the first few hours following an RDD explosion. Knowledge about the type and amount of radionuclide released (as well as the physical form and chemical composition of the substance used) limit the modeler's ability to generate a plume prediction map that accurately reflects the release. The radioactive particulate matter that deposits on the surface during the passage of the plume can be measured by collecting empirical data with field-team and aircraft-based sensors. As more data are collected, a more accurate picture of the amount of radiological material deposited is developed. Initial measurement data can be used to update model predictions and produce a better prediction for areas that have not yet been surveyed. (For example, this was done during the FSE in the FRMAC using NARAC models to project areas that may have had low levels of food crop contamination in western Washington State.) Predictions updated with measurement data can also be used to make estimates of areas that have contamination below the measurement threshold of available instruments. When detailed measurement surveys are completed and the data analyzed, they can be used to determine the most accurate picture of the amount of radioactive material deposited. With these data, accurate assessments of protective actions can be made and used by top officials to confidently make informed decisions.

To be useful in managing the safety of victims or responders, the numbers characterizing the deposition of radioactive material on the ground must be turned into numbers characterizing the

dosage that a human would receive, and of more importance to top officials, into characterizations of the health impact of such a dosage. Figure 11 is a FRMAC data product that shows the radiological deposition on May 14, 2003 in terms of EPA PAGs. This product was generated based on a FRMAC assessment of measurements of the deposited radioactivity, and used the NARAC model to determined EPA PAG levels in between measurement points.

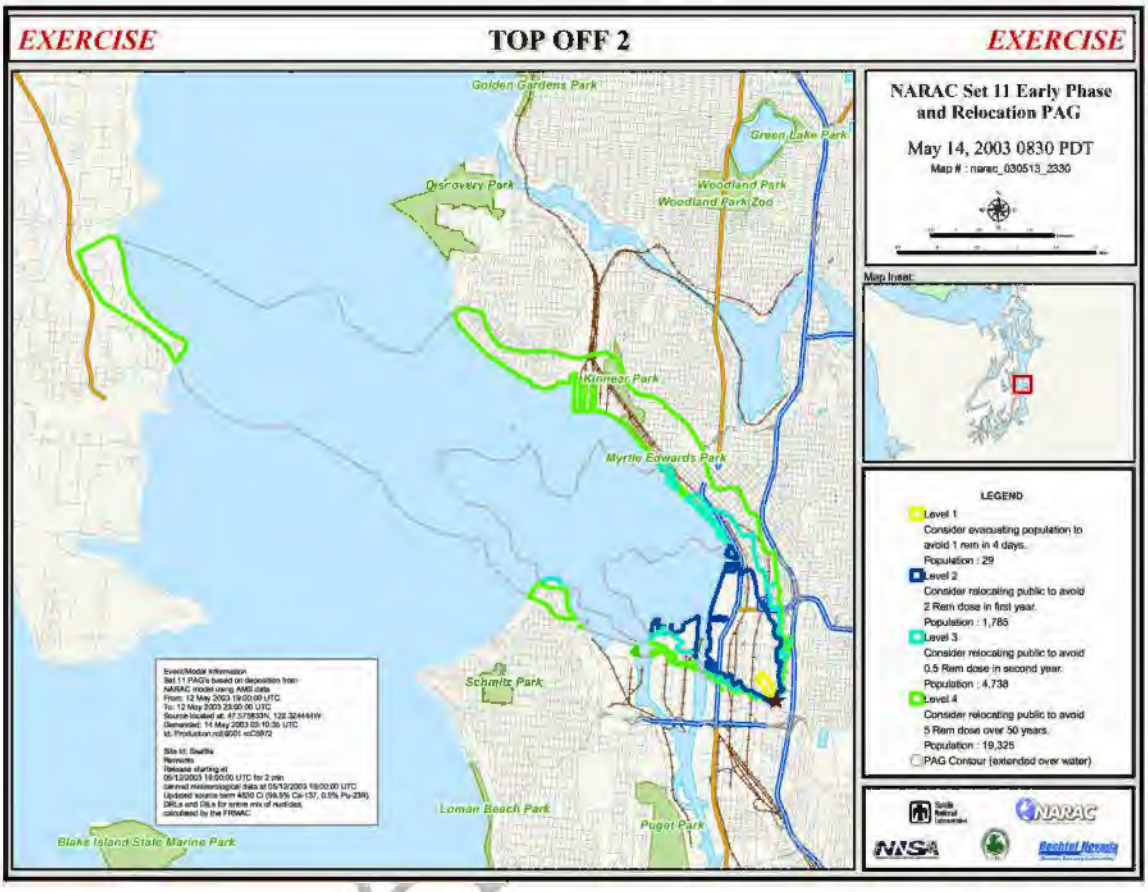


Figure 11. FRMAC Data Product Showing the Deposition of Radioactive Material in Terms of the Environmental Protections Agency's Protective Action Guidelines

Figure 12 describes the processes involved in developing plume predictions and deposition data products. It also highlights the differences between plume predictions and deposition, footprint data products and what each can provide the decision-maker.

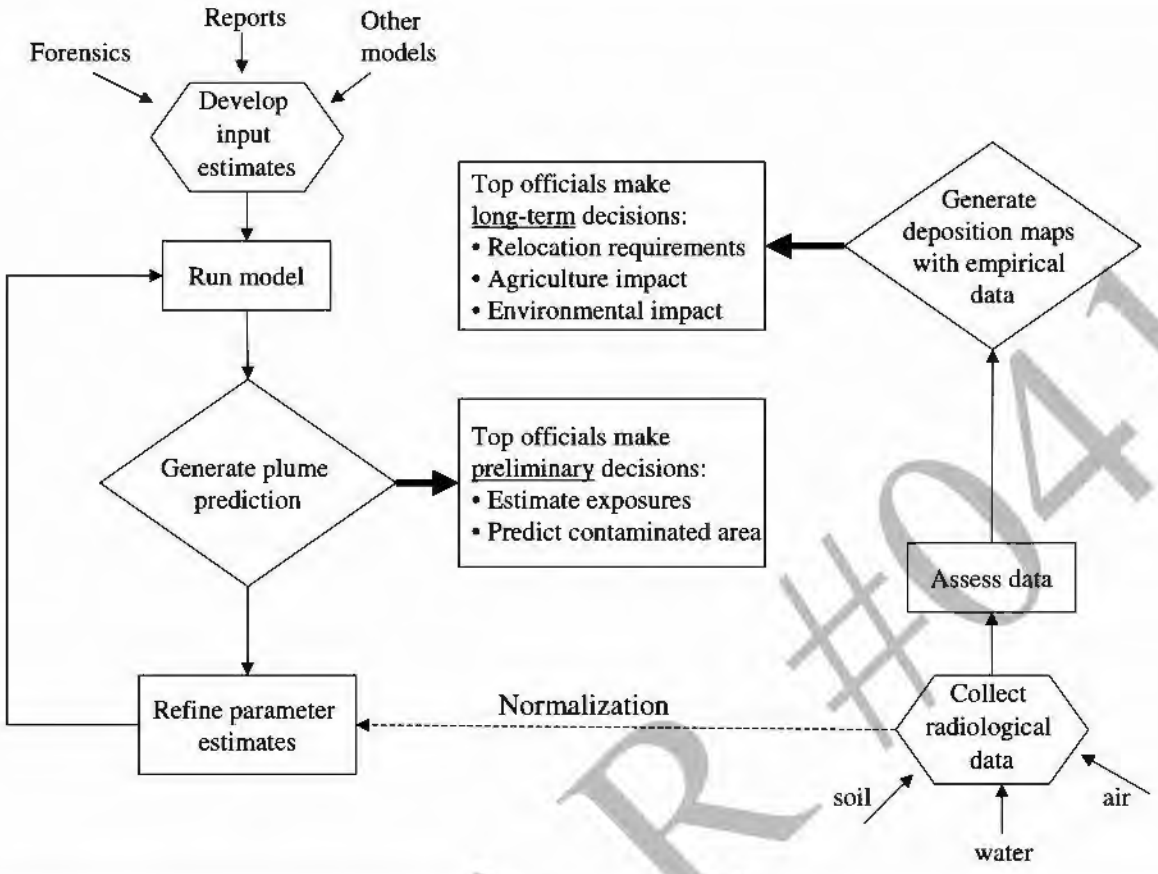


Figure 12. Processes for the Development of Plume Prediction and Deposition Maps

3. Reconstruction

The following teams all collected radiological data during the T2 FSE:[67]

- City assets
  - Seattle Fire Department HAZMAT
- State assets
  - National Guard 10th WMD CST
  - Washington State DOH RMAC and Field Teams
  - Washington State Department of Ecology Field Team

[67] The evaluation team learned that the ATF Bomb Squad carried radiation detectors that they used to collect data for their personal use. It is possible that there were other agencies whose personnel were also wearing radiation detectors. US Navy personnel from the Puget Sound Naval Shipyard were also tasked during the FSE to collect radiological data for the FRMAC. It is possible that the evaluation team is unaware of other agencies that collected radiological data during the FSE.

- Federal assets
  - DOE RAP Region 8 Team
  - DOE Aerial Monitoring System (AMS)
  - EPA Field Team
  - FRMAC Field Teams

As shown in figure 13, no single agreed upon agency served as a central clearinghouse for all of the radiological data collected by the different teams. Data were collected and sent to multiple agencies for analysis, but no one agency received all of the data.

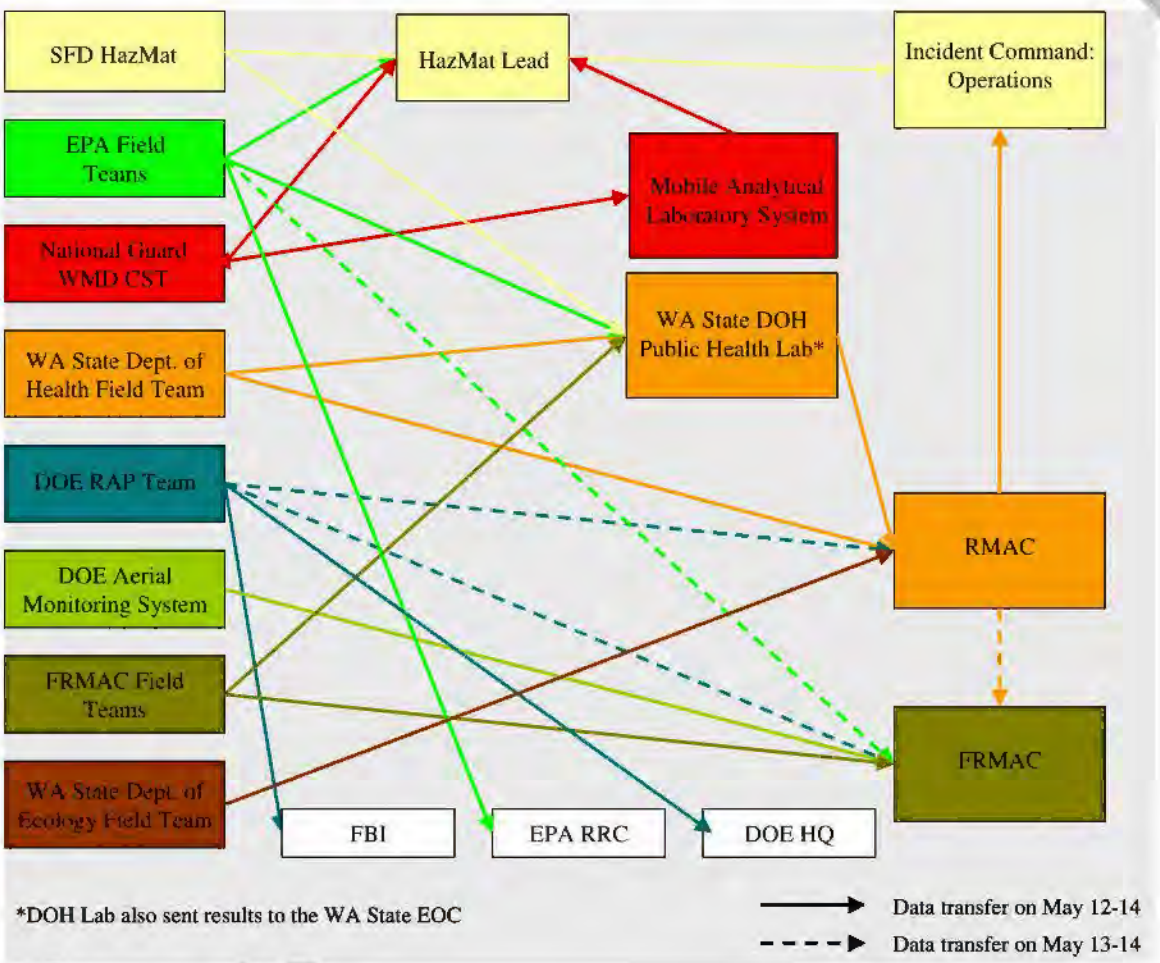


Figure 13. Data Coordination during T2 FSE

The following agencies/organizations generated and distributed plume predictions and/or deposition maps during the FSE:

- State and local
  - SFD/Seattle EOC
  - Seattle/King County Public Health EOC
  - King County EOC
  - Washington State DOH RMAC
- Federal
  - FRMAC
  - HHS Headquarters
  - NOAA
  - DOE Headquarters

Figure 14 indicates that many data products were produced by many different organizations. The distribution of these products also proved to be a challenge during the FSE.[68]

[68] According to a Washington DOH controller after the FSE, data was sent from the RMAC to the Seattle EOC, but the evaluation team could not confirm that information.

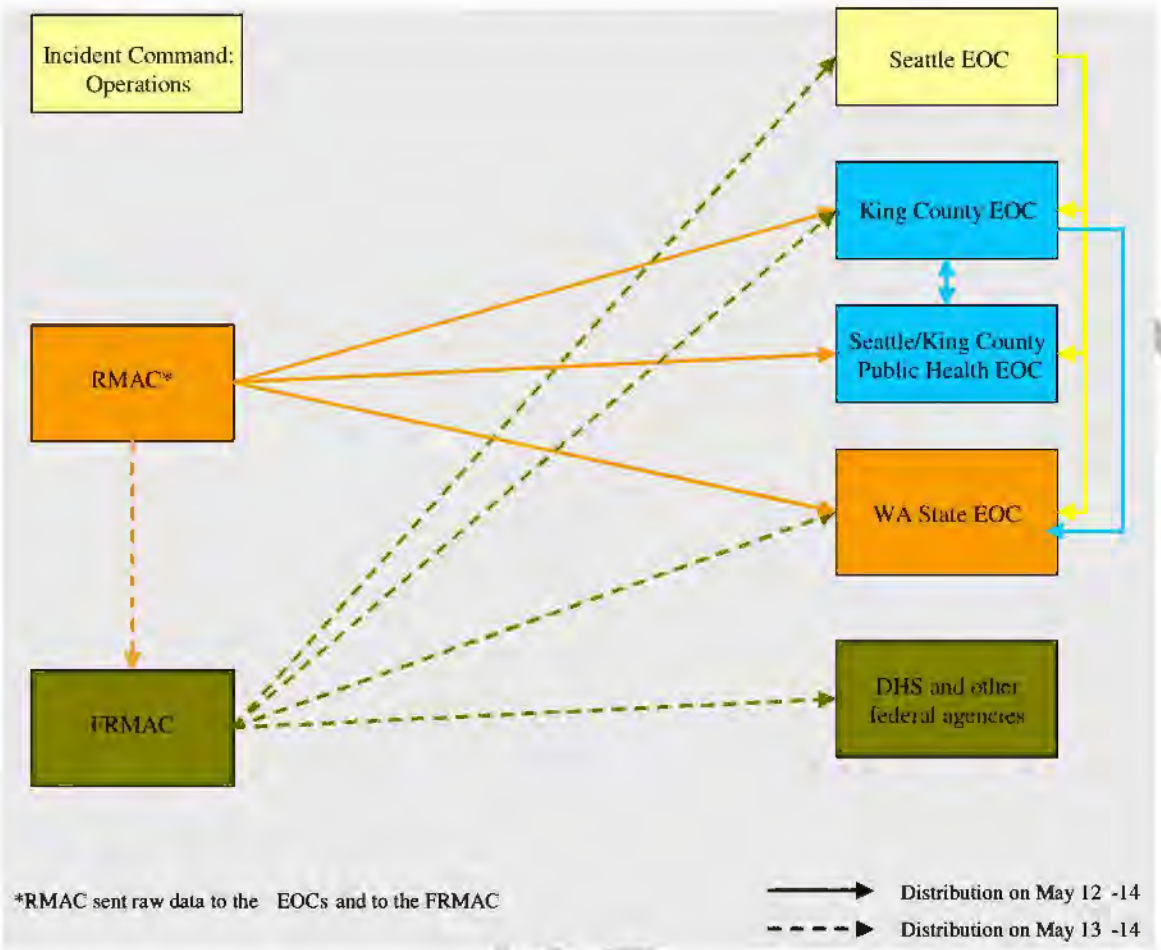


Figure 14. Data Interpretation and Distribution during T2 FSE

a. Seattle

Soon after the explosion, SFD generated a prediction of the plume using the ARAC model.[69] It is not clear, however, if the initial plume prediction generated by SFD ever left the incident site. All other plume predictions were generated by NARAC upon request and made available to agencies via the NARAC secure Internet site. Distribution of NARAC predictions to other agencies (beyond Seattle) required approval by the DOE Senior Energy Official, who was responsible for coordinating the use of DOE assets (such as NARAC) with other agencies. Agencies that had access to the NARAC secure Internet site included SFD, Seattle Police

[69] Seattle is the first city to pilot the Local Integration of NARAC with Cities (LINC) program. The program was a pilot project of the NNSA, and is now in DHS. It enables local responders to access NARAC's plume modeling capabilities. Using the system, the Seattle Fire Department (SFD) can receive NARAC plume model predictions using previously installed computer systems. The NARAC predictions can easily be distributed to multiple recipients. For more information, refer to *NNSA's Livermore Lab Partners With Cities and Counties to Track Biological, Chemical Releases*. Lawrence Livermore National Laboratory News Release, NR 02-05-08, May 22, 2002.

Department (SPD), Seattle EOC, Public Health Seattle/King County (PHSKC) EOC, King County EOC, WA State EOC, WA DOH, DHS, Federal Emergency Management Agency (FEMA), DOE, DOD, Department of Transportation (DOT), HHS, (NRC, and EPA.

b. Washington State

The Seattle EOC notified the WA State EOC that SFD responders detected radiation at the incident site at 1225 Pacific Daylight Time (PDT). The WA State EOC deployed the following assets:

RMAC

The WA State DOH deployed their mobile RMAC to the incident site shortly after the WA State EOC received notification that radiation was detected. By mid-afternoon on May 12, 2003, the RMAC gleaned enough information off the radio to develop a source term and generate its own plume projection using a modeling program called HotSpot. The RMAC also deployed field teams that were collecting data by 1530, and obtained off-site readings by 1900.[70]

The RMAC had considerable communications problems throughout the exercise—that could have just as easily occurred in a real incident. During the afternoon and evening of May 12, 2003 and the morning on May 13, 2003, the RMAC was only able to transmit data points to the WA State DOH staff at the WA State EOC via telephone. Those data points were plotted on a map at the WA State EOC. The RMAC also used the EPA's wireless Internet capability to send graphics to the DOH staff. However, the file was not recognized as containing graphics and was not opened immediately. At 1455 on May 13, the RMAC used the DOE Region 8 RAP Team's fax machine to transmit three pages of field team data. Because of the lack of resources at the WA State EOC to plot data and the considerable lag time to receive data, the Division of Radiation Protection Director began identifying significant data points and briefing them directly to decision-makers during conference calls.[71]

The RMAC also sent data to the King County and PHSKC EOCs and to the FRMAC during the exercise. The DOH liaison at the King County EOC began sending a courier to the RMAC to pick up their radiation data on the morning of May 13, 2003. Plotters in the King County Geographic Information System (GIS) section then plotted the data points on a map and forwarded it to the WA DOH staff at the WA State EOC. The DOH liaison at the PHSKC EOC received data over the telephone and plotted it on a map. By late afternoon on May 13, a DOH liaison went to the FRMAC to initiate a protocol for transmission of data. Because of communications problems, the FRMAC did not begin to receive DOH RMAC data until May 14.[72] The Seattle EOC does not recall ever receiving data or products from the RMAC or the WA State DOH.

DOH Public Health Laboratory

The DOH Public Health Laboratory was activated to analyze soil samples. They received soil samples from the DOH field teams, EPA field teams, and FRMAC field teams. To test their

[70] RMAC teams were likely on site earlier but there are no data to confirm this assertion.

[71] The reconstruction of events at the DOH RMAC was obtained through conversations with Washington DOH staff who participated in the exercise.

[72] Information regarding data transmission from the RMAC was reconstructed from conversations with Washington DOH and FRMAC staff who participated in the exercise.

internal policies and radiation analysis capabilities, the lab arranged to receive radioactive soil samples prepared prior to the FSE. For purposes of the exercise, these samples were tagged as though they came from SFD HAZMAT, EPA, and Harborview Hospital. The results were sent to the RMAC and to the WA State EOC.

Department of Ecology

At 2000 on May 12, the WA State EOC was prompted by exercise control to contact the Department of Ecology and have them deploy their HAZMAT team resources to survey the surrounding area. At 2312 a data collector observing incident command recorded the Operations Chief instructing the Ecology Field team to do off-site monitoring. The Ecology Field Team data were sent to the RMAC.

National Guard 10th WMD CST

The WA State EOC notified the National Guard 10th WMD CST to go on standby at 1230 on May 12, 2003. They were instructed to deploy to the City of Seatac and await further instructions. At 1345, the CST received notification from the WA State EOC to deploy to the incident site.[73] The CST advance team arrived at the incident site at approximately 1415, and the CST commanding officer met with the Incident Commander at 1420. The CST commanding officer was instructed to check in with the SFD Operations Chief and report directly to the HAZMAT Chief. After an initial assessment, the CST commanding officer brought in the rest of his team at 1445. The CST sent their data to the SFD HAZMAT Chief and to their MALS. They also collected ground samples that the EPA sent to the WA State DOH Public Health Laboratory for analysis. The CST was redeployed at approximately 1230 on May 13, 2003 and told to remain on stand-by in case there were follow-on attacks.

c. Federal data collection and modeling

The following Federal assets were deployed to Seattle and the surrounding areas:

EPA

At 1318 on May 12, 2003, EPA regional field personnel were dispatched to the incident site. When they arrived on scene, EPA personnel communicated with incident command and were tasked with monitoring the perimeter and taking air samples. EPA personnel began monitoring and sampling at approximately 1430; they continued to take air and soil samples throughout the exercise. EPA responders provided their data to incident command through the Incident Command System (ICS) reporting chain. EPA responders also provided data back to EPA Region 10 Regional Response Center (RRC). While EPA has procedures to provide off-site data to the FRMAC during a fixed-facility incident, procedures for integrating on-site data into the FRMAC were not been provided to the EPA field teams during the FSE.[74] As a result, while EPA personnel knew to send their data to the FRMAC, no data were sent to the FRMAC until May 14.

[73] The CST deployed to the exercise staging area prior to the start of the exercise. They waited there for the appropriate amount of time as if they were following the deployment orders described above.

[74] As will be discussed later in the section, EPA data was not provided to the FRMAC until May 14 because no advance party meeting was held during the FSE.

DOE Region 8 RAP Team

At 1335 and 1336 respectively on May 12, 2003, the Region 8 RAP received calls requesting assistance from the WA DOH and the Federal Bureau of Investigation (FBI). Within two hours, the team completed their pre-deployment activities and was en route to the Seattle area by 1458. Through discussions with both the FBI and WA DOH, it was agreed that RAP would initially put all their resources and effort to support the FBI. Upon arrival at the scene, RAP teamed up with the FBI Hazardous Material Response Unit (HMRU) Commander, informed him of team capabilities, and received a safety brief prior to commencing survey onsite. RAP supported the FBI until 2400 on May 12 and continued to support the FBI on May 13 until 1100. RAP received numerous requests for assistance from the Environmental Protection Agency (EPA), who were conducting on-site surveys, and the Disaster Mortuary Operational Response Team (DMORT). RAP fulfilled these requests and supported WA DOH with their requested priorities into the evening of May 13. On May 14, RAP was able to fulfill a request to join the FRMAC.

DOE AMS

A data collector at the WA State EOC recorded that the deployment order for the AMS was received at 1425 on May 12, 2003. The DOE AMS arrived over Seattle at approximately 1900 and flew a serpentine pattern to collect notional radiological data. The data were transmitted to the FRMAC at 2056. The AMS flew several more times over targeted locations during the FSE.

FRMAC

After some discussion among Washington State top officials concerning the need for the FRMAC, the DOH made a request to FEMA to deploy the FRMAC at 1434 on May 12, 2003. DOE Headquarters in Washington, D.C., approved the FRMAC deployment at 1549 that same day, and they departed from Nevada at 1600. At 2000 the WA State EOC received confirmation that the FRMAC was in place at Fort Lawton.

Upon establishment of the FRMAC, Field Monitoring Teams were deployed. At 2056 on May 12, 2003, the FRMAC began to receive simulated empirical aerial sampling data from the DOE AMS. The ground monitoring data obtained indicated the presence of an alpha emitter in addition to the gamma emitter identified earlier in the day.[75] With data still limited, the FRMAC Director briefed the initial results to the PFO at around 2300 on May 12 and recommended to the PFO that the affected people be evacuated. However, EPA advised the PFO that the Seattle Mayor's shelter-in-place order should not he revised, and that the decision could be re-examined in the morning based upon additional monitoring data. The PFO's final decision was to recommend to the Seattle EOC that they maintain the shelter-in-place until morning when a more thorough analysis would be completed. Before the PFO could pass his recommendation to the Seattle EOC, however, he learned that a decision had already been made by the Seattle Mayor to release those workers who had been sheltered within their businesses, and for residential citizens already sheltering-in-place to remain doing so.

The FRMAC did not have the time to complete a radiological deposition map that showed the health impact of the radiation dose on the public in terms of EPA PAGs before the Joint Operations Center (JOC) closed at 2300. FRMAC protocol required approval from the FRMAC

[75] Data collector logs show that the DOH Public Health Lab also identified the presence of an alpha emitter at around the same time.

Director, the Senior Energy Official (SEO), and the PFO—all of who were stationed in the JOC—before all analysis products could be distributed. Because the JOC was closed, the FRMAC could not obtain necessary approval to distribute the maps showing the radiological deposition to the other FSL operations centers until the following day.

At 0800 on May 13, 2003, FRMAC briefed the most up-to-date deposition map to the PFO. A more rigorous analysis revealed that an evacuation was not necessary, but a targeted relocation would be required. The PFO approved the release of the deposition map to the DHS Crisis Action Team (CAT). At 1000, FRMAC participated in a conference call with the PFO; the Seattle, King County, and WA State EOCs; and the FEMA Regional Operations Center (ROC). During that call, the FRMAC Director provided the EOC representatives with a summary of the data collected thus far. With this knowledge, in addition to the determination by WA DOH that the areas east of Interstate-5 (I-5) were contaminant-free, the Seattle Mayor was comfortable moving forward with his decision to release those residents sheltering-in-place east of I-5 and relocate affected residents west of I-5 for three days. Later that day, at 1220, the Seattle Mayor and the Public Health Seattle/King County Director met with the FRMAC Director and the PFO at the JOC to review the FRMAC deposition map.

After that meeting, the distribution of a consistent data product appeared to improve. Requests started to appear in the FRMAC activity log from the Seattle EOC and the WA State EOC for the most recent maps. The FRMAC responded to these requests anywhere from immediately (to DHS) to five hours, 38 minutes later (see Table 5). This timeframe provides a realistic sense of how long it takes for information to get out of the FRMAC once the contacts are established. Top officials and SMEs need to remember that the FRMAC is inputting data collected from many sources, and that before they distribute updated information, they need to input the data into their system, conduct an analysis of the data, and get approval from the appropriate authorities. This process takes time and is often shortened during training exercises.

Table 5. Request and Delivery of FRMAC Data Products

REQUESTING AGENCY	FRMAC PRODUCT REQUESTED	FRMAC PRODUCT DELIVERED	TIME DIFFERENCE
DHS	May 13 0851	May 13 0851	0:00
DOE Headquarters	May 13 0911	May 13 0920	0:09
FEMA ROC	May 13 0919	May 13 1239	3:20
DHS	May 13 0954	May 13 1359	4:05
Washington DOH	May 13 1137	May 13 1715	5:38
SFD	May 13 1143	May 13 1607	4:24
Seattle Mayor	May 13 1147	May 13 1402	2:15
Washington Department of Agriculture	May 13 1222	May 13 1735	5:12
WA State EOC	May 13 1318	May 13 1723	4:05
Food and Drug Administration	May 13 1901	May 13 2206	3:05
EPA	May 13 1909	May 13 2026	1:17
King County EOC	May 14 1055	May 14 1247	1:52

Many agencies and departments outside of Washington State contacted the FRMAC directly for maps and other data products on May 13 and 14, 2003. The FRMAC Event Log shows requests for deposition maps from DHS, Food and Drug Administration, EPA, and DOE Headquarters. These examples suggest that the Federal agencies participating in Washington, D.C., understood that the FRMAC would coordinate the radiation data and distribute the updated deposition maps. However, even though they had representatives in the A-Team—which was co-located with the FRMAC—deposition maps could not be sent to the Centers for Disease Control and Prevention (CDC) and the HHS operations centers.[76]

d. Federal agencies and department headquarters

The following Federal agencies used their own internal models to develop maps at their headquarters:

DOE

DOE Headquarters in Washington, D.C., accessed the same NARAC plume predictions as those used by agencies working in the Seattle area (such as in the Seattle EOC and the FRMAC), using the same secure Internet site as used by other agencies. As DOE was assigned initial management of FRMAC for radiological response, it is likely that their plume map was used to brief top officials.

[76] The evaluation team does not know if this was because of technical problems or if the Advisory Team did not have the permission to distribute the FRMAC products.

HHS

On May 12, 2003, HHS Headquarters in Washington, D.C., developed a plume prediction using DTRA's Hazardous Predicting Assessment Capabilities model. They used an unknown scenario to generate their inputs for the model. Observations by data collectors suggest that they developed the plume projections to identify HHS assets that might be required and eventually deployed. These maps were used to brief the HHS Secretary and DHS Secretary during the FSE. Since the model used to generate the HHS plume prediction differed from the one used to generate the DOE plume prediction, it is likely that the outputs differed as well.[77]

NOAA

NOAA also generated plume predictions during the exercise. They too used unknown scenario estimates to input into their model. In addition, NOAA used real weather patterns for their model rather than the canned weather planned and used during the T2 FSE. NOAA intended to run their model for training purposes only, and the resulting plume prediction was to be walled off from inter-agency play. Nonetheless, copies of the maps were faxed to the DOE Headquarters during the exercise. The addition of another plume prediction generated with yet another model and resulting in a different output from the two others may have added to Federal top officials' frustrations.[78]

EPA

The evaluation team does not have any data to indicate that the EPA Headquarters generated a plume prediction during the exercise. However, there are data that indicate that the White House contacted EPA Headquarters for a plume map.

4. Artificialities

A number of exercise artificialities contributed to the data coordination and analysis product distribution challenges were observed during T2. These included:

- The JOC was closed from 2300 on May 12, 2003, until 0700 on May 13, 2003;
- There was an insufficient number of controllers to provide injects to agency personnel collecting radiological data at the RDD incident site. This was especially problematic during the overnight hours of May 12 to May 13, 2003. In addition, the WA DOH RMAC did not have an exercise controller located in their facility;
- The FRMAC expected the affected area to become smaller over time due to the re-wetting of contaminated material. However, exercise controllers did not have the pre-scripted data to support the re-wetting process;
- The location of the FRMAC was unrealistic, as it was located in a contaminated area;
- While there will always be security at an incident site, particularly if WMD are suspected, security during the FSE was slow and cumbersome; and

[77] The evaluation team does not have sufficient data or plume prediction maps to compare the results from the different models

[78] Again, the evaluation team does not have sufficient data to compare the results from the different models.

- The events leading up to the RDD at the Columbia Generating Station would have caused most State assets to be deployed to Richland. This would have delayed their response to the RDD incident in Seattle by hours.

5. Analysis

a. Plume modeling

As described in the reconstruction, the Seattle EOC contacted NARAC soon after the explosion to have them generate a prediction for where the plume would travel. The resulting product was made available to the King County and WA State EOCs as well as the FEMA ROC and other Federal and State agencies. To add to the confusion, the State DOH RMAC generated another plume prediction using the HotSpot modeling program, once they obtained enough data to input a reliable source term.[79] As described in the reconstruction, the RMAC used EPA's wireless Internet capability to send their plume prediction to the WA State EOC. As a result, Seattle, King County, and Washington State top officials all had different information from which they could make their preliminary decisions. The evaluation team does not have sufficient data to determine whether each jurisdiction had multiple plume prediction maps or whether they simply had different plume prediction maps. In recognition of the fact that data availability is likely to be very limited early in an RDD response, WA State DOH, PHSKC, and EPA developed default PAGs, based on the existing PAGs, to use during an RDD event. The Seattle Mayor applied these "default" PAGs during the early hours of the incident, as decision-makers awaited the collection of the data required to effectively model the release. Therefore, it is not clear if the presence of different plume predictions affected local and State top official decisions in the early hours of the exercise.

In addition to the confusion in Seattle, several Federal agency and department headquarters developed their own plume predictions to make internal assessments concerning assets that might be required. These Federal agencies and departments all used an unknown scenario to generate input data and used different models to generate plume predictions. So even if the input data were the same, the output may well have differed. As noted earlier, the evaluation team was told that many of these agencies generated the predictive maps for internal purposes—either for training purposes or to provide them with some insight into what Federal assets might be needed for the response. Nonetheless, during the T2 FSE, multiple maps from the predictive models were presented to department and agency top officials in Cabinet-level meetings. This led to some confusion and frustration by top officials in Washington, D.C., as to which output was the correct one to use. Although the evaluation team did not identify that the existence of multiple maps produced any direct consequences upon decisions made during the FSE at the Federal interagency level or in Washington State, the issue may have contributed to delays in decision-making. This underscores the role of the FRMAC as the single place to coordinate and analyze data, and to provide authoritative data products to support decision-makers, in accordance with the FRERP. Decision-makers need to understand that this process takes time, and that the empirically-based data products provide more accurate information than initial plume predictions

Furthermore, it is easy to imagine the possible consequences of FSL governments producing many different maps, particularly if they have used different measurements and standards.

[79] The evaluation team does not have sufficient data or plume maps to compare the results from the different models.

While it didn't happen during the FSE, the media could have questioned the FSL governments' expertise and ability to make decisions.

In the region close to the incident site where protective action decisions are most important, estimates based on atmospheric models are very uncertain. For very large-scale decision-making (e.g., identifying the ingestion pathway), models may be more useful but are generally applied with conservative assumptions that reduce their usefulness. In the case of TOPOFF 2, projections exceeding FDA criteria out to 150 miles from an RDD in downtown Seattle were not credible and potentially could have resulted in unnecessary food protection actions.

Finally, and possibly most importantly, it appears that few decision-makers were informed of the fact that a plume prediction has a limited useful lifetime. As discussed in the introduction to this section, model predictions need to be continuously updated using real measurement data, and will be replaced by products generated primarily from measured data, once enough data are collected, interpreted in a manner understandable to top officials, and the resulting products distributed. During the FSE, top officials emphasized their frustration regarding the different plume maps. However, they did not ask for (or in some cases receive) updated information that relied on empirical data. This suggests there is a need for additional education among both responders and decision-makers regarding the timing and value of the different types of information following an RDD explosion.

b. Data collection and coordination

As described in the reconstruction, there was minimal coordination of radiological data collection between FSL agencies at the incident site or at off-site locations until the third day of the exercise. Many FSL agencies with various data collection capabilities arrived to the incident site at different times. As in any mass casualty incident, Incident Command has many responsibilities, including the primary mission of rescuing victims, all of which require the Incident Commander's attention. This can easily stress incident command capabilities, and limit attention to many tasks—particularly relatively specialized or complicated tasks.

During the FSE, there is evidence to support the fact that the Incident Commander tasked the EPA field team and the CST to work together to coordinate monitoring and sampling at the site, and report their data to the HAZMAT Chief. While there is evidence that WA DOH RMAC was in contact with Incident Command, it is unclear what information was shared. However, there is no evidence to indicate that WA State DOH RMAC coordinated their collection efforts with the Incident Commander or with the HAZMAT Chief. Rather, the data indicate that the Washington DOH RMAC, DOH field teams, and the Washington State Department of Ecology field team coordinated with each other on May 12, 2003, but not with the other local or Federal data collection agencies at the incident site. By May 13, 2003, the EPA and DOE RAP teams were also coordinating with the DOH RMAC.

The result of the on-site coordination failure is that no one agency at the incident site had all of the data. In addition, some responders entered contaminated areas to collect data that another agency had already collected, which meant they were exposed to more radiation than necessary. As a consequence, FSL responders, collecting data for different purposes, duplicated on-scene efforts. As an example, during the on-scene Hotwash, EPA learned that a bomb squad had sent robots into the most contaminated areas armed with radiation meters, which were then read from a distance using cameras. Because this data was not integrated in the incident command system

and shared with all responders, EPA field teams later collected these same data points again, resulting in perhaps unnecessary exposure of personnel to radiation. In addition, as the uncoordinated data left the incident site, different jurisdictions (i.e., Seattle, King County, and Washington State) had different data from which they developed information to make recommendations and decisions.

While coordination challenges on the ground and among agencies are to some extent expected early during the incident response, the arrival of the FRMAC (2000 on May 12, 2003) is designed to facilitate at least more organized off-site data coordination. As discussed in the *Background* of this section, one of the first steps the FRMAC typically takes upon arrival at a radiological incident is to hold an advance party meeting with representatives from the State and other Federal agencies. The advance party meeting is designed to facilitate relationships with relevant Federal, State, and local officials, and to put processes in place to facilitate the coordination of data and the distribution of information to all relevant agencies.

During the FSE, the advance party meeting did not occur. DOH staff at the WA State EOC made the decision to not send a liaison to the FRMAC based on how busy DOH personnel were in the opening hours of the FSE and a lack of understanding of the importance of the advance party meeting and co-location with the FRMAC. To further complicate issues, that decision was not communicated to the RMAC; so they were unaware that the FRMAC had even arrived. The lack of an advance party meeting meant that neither State nor Federal agencies had the opportunity to develop and agree on procedures to send data to a single analysis location—which presumably would be the FRMAC. As a result, the only data the FRMAC had on May 12, 2003 was from the AMS and from their field monitoring teams. As described in the reconstruction, the FRMAC did not receive data from the RMAC, EPA, or the DOE RAP Teams until May 14, 2003. The lack of on-site coordination also makes it unclear if the FRMAC ever received data collected by the SFD HAZMAT Team.

EPA participants suggested a possible means of supporting coordinated data collection efforts. They suggested that it would have been beneficial if all of the technical agencies collecting data at the incident site had come together to present unified recommendations on roles and responsibilities to the Incident Commander. They also suggested that it would have been beneficial for one of the technical agencies to volunteer to coordinate all of the data being collected on the site. Although this might have helped coordinate the data, it would require one of these support agencies to take the lead in coordinating the effort. A potential middle ground would be for Incident Command to track which teams are on-site collecting data, and task one of the support agencies to coordinate the effort. This would provide Incident Command with both the unified front they lacked during the T2 FSE, and an SME to coordinate and possibly provide expert advice. Further, this would give these critical SMEs greater visibility with Incident Command than they had during the T2 FSE, where they were working for the HAZMAT Chief—two levels below the Incident Commander.

Data collection, management, and distribution continue to be a challenge at nationally significant incidents. FRMAC procedures, which were developed primarily for radiological releases from a fixed nuclear facility, should be re-examined to ensure that they are effective in handling non-fixed facility incidents involving on-scene response by FSL responders. Although the plan was modified since its original inception, the procedures remain modeled on response methods appropriate for nuclear reactor disasters. Further, the Washington State DOH Procedures for Responding to a Radiological Attack is written to integrate into existing FRMAC and other DOE

plans. When applied to terrorist events, like that simulated during T2, there are differences that may impact the effectiveness of these procedures. These include:

- Disasters at nuclear facilities are likely to involve known radiological materials and estimates of quantities involved, whereas the materials and quantities used in terrorist-sponsored RDD explosions are not known until analyses can he completed, as was the case in the T2 FSE; and
- Terrorist activities are more likely to occur in major metropolitan areas with high profile, politically powerful, and well-equipped local governments; whereas nuclear facilities tend to be in rural communities with fewer response assets. In Washington, the DOH Procedures for Responding to a Radiological Attack only acknowledges a local jurisdiction's leadership role at an incident when "command shifts or transitions to local jurisdiction," rather than assuming that the local jurisdiction is in charge and that the State is a support agency[80]. This may stem from their experience or responsibilities for nuclear power facilities, or their internal expectations.

As DHS develops its plans for responding to radiological (and other) emergencies, it is imperative that they build in processes that allow State and local government capabilities to be coordinated with the federal capabilities. This is particularly important because state and local resources are likely to arrive on the scene and begin using their assets before the federal support arrives.

Another issue that deserves further attention is whether the FRMAC should release raw data sets to different agencies, or to continue to send out only data products. In T2, the FRMAC policy was to collect and analyze data locally, and only send out data products. A number of Federal and State agencies suggested that they need the raw data to conduct their own analyses, and that the FRMAC policies do not allow them to meet their missions. However, were data to leave the FRMAC, there is greater potential for many agencies to have incomplete or out of date data. This could further complicate the coordination challenge and increase the likelihood of inconsistent decisions and public information.

c. Data analysis, distribution, and impact on decision-making

Developing the most valid deposition maps possible requires that all data be sent to the SMEs who are interpreting the data. As far as the evaluation team has discerned, the radiological data collected by the SFD HAZMAT never left the incident site, and might not have been used to develop deposition maps. In addition, there is no evidence that any of HAZMAT data were sent to the RMAC or the FRMAC to support their analyses. Therefore, it is quite likely that none of the agencies analyzing radiation data were using all available data. This is one reason that different analyses could result in different information being sent to top officials. As described earlier, the WA DOH, Public Health Seattle/King County, and EPA recognized the likelihood of limited data reaching decision-makers early in an RDD response and developed default PAGs prior to the FSE. The Seattle Mayor used these default PAGs during the early hours of the incident.

[80] Washington State Department of Health, *Division of Radiation Protection Plan and Procedures for Responding to a Radiological Attack*, DOH/DRP, March 2003.

However, even if the data coordination challenges did not exist, analysis product distribution was another challenge for responders during the FSE. Prior to the arrival of the FRMAC, the WA State DOH, King County EOC, and PHSKC plotted rough deposition maps using data collected hy the WA DOH field teams.[81] As noted in the *Reconstruction* section of the AAR, lack of resources made it difficult, if not impossible, for these maps to be interpreted and reach decision-makers in a timely fashion. Therefore, significant data points served as key discussion points during conference calls to help top officials make decisions.

The impact of the lack of clear information led to significant frustration among top officials. A number of T2 data collectors observed the frustration and noted players' attempts to resolve the frustrations on their own. For example, at 2100 on May 12, 2003 a data collector at the Seattle EOC recorded that the Mayor's representative told the WA DOH that they wanted to make-up their own data to develop the information they needed to define an evacuation route. A data collector recorded similar statements at the WA State EOC. Although the evaluation team does not know whether Seattle or Washington State followed up on its quest to make up radiological data, these observations do illustrate the problem.

The evaluation team identified four potential contributing factors that may have led to the frustration experienced by the State and local top officials during the overnight hours of the exercise:

- It is likely that there was insufficient scenario data during the overnight hours (see *artificialities*);
- Controllers in the WA State EOC gave conflicting information to DOH personnel and also withdrew information that had been provided earlier in the exercise;
- As described in the reconstruction and in the previous section, there was also a lack of effective coordination, until the third day of the exercise; and
- It is possible that top officials did not recognize the real amount of time that it takes to collect, coordinate, and analyze data and present it in a meaningful fashion. Many top officials are used to participating in tabletop exercises where the data and information they request are made available much more quickly than would happen in real emergency—in tabletops, data and information are often available instantly.

The timing of the statements showing top official concerns on May 12, 2003, suggest that some of this frustration might have been alleviated if the EOCs had received the FRMAC analysis products sometime during the first night of the FSE. In a conference call at 2000, the PFO assured the State and local officials that the DOE would provide them with AMS data once they were received and analyzed. However, as described in the reconstruction, it took longer than the PFO expected for the FRMAC to complete the analysis of the AMS data; the analysis products were not completed until after the JOC closed for the night. This exercise artificiality may have led to, or possibly exacerbated, frustrations because local and State officials then had to wait a minimum of eight hours to receive the information they needed.

Although the JOC re-opened at 0700 on May 13, 2003, the FRMAC did not deliver their deposition map to the Seattle or WA State EOCs until mid-day on May 13. As a result of not

[81] The evaluation team does not know whether Seattle EOC or incident command were plotting data in a similar manner, or whether the various EOCs shared their deposition maps.

having the advance party meeting on May 12, 2003, the FRMAC did not have the appropriate contacts within the various EOCs. If the FRMAC had the contact information and the clearance to provide maps directly to Seattle, King County, and WA State EOCs, the FRMAC might have supplied them with the deposition data product map as early as 2330 on May 12, 2003. It is highly likely that had the JOC remained open throughout the night, the FRMAC would have received clearance to distribute the deposition maps and would have identified the appropriate contacts at the Seattle, King County, and State EOCs, as each jurisdiction provided liaisons to the JOC.

It appears that after the FRMAC deposition maps were distributed to State and local EOCs, there was less confusion over which information to use for decision-making. The distribution process was flowing well by the end of play on May 13, 2003, and continued rather effectively on May 14, 2003—at least in Washington State. Regionally, the players' were well aware of the problems, and found ways to resolve them. However, the concerns in Washington, D.C., did not seem to end, even after the exercise was over. Nonetheless, there is no evidence that activities at the Federal inter-agency level or the different data products provided to these top officials had any impact on the response in Washington State.

SUMMARY OF CONCLUSIONS—DATA COLLECTION AND COORDINATION:

- On-site and off-site data coordination during the FSE was minimal at best. As a result, no one agency at the incident site had a complete operational picture, and multiple agencies were performing redundant tasks. The development of National Incident Management System may help to facilitate the data collection and coordination processes in the future.
- There was much confusion during the FSE about the multitude of plume prediction maps among agencies and across jurisdictions. While it did not happen during the FSE, if agencies and jurisdictions produce inconsistent and conflicting maps, the media could question the governments' credibility and ability to make decisions.
- Officials at all levels of government need to be educated about the differences between plume dispersion prediction models and data products generated from empirical data. Officials need to be aware of how each can aid decision-makers and the limitations of both.
- FSL agencies and departments should be educated about the need to coordinate the data collection and distribution processes and the implications of a lack of coordination.
- Plans and procedures for radiological incidents were initially developed for emergencies at nuclear power facilities. To be effectively applied to terrorist events, these plans and procedures may need to be modified.
- On-site data collection may also benefit from the designation by the Incident Commander of a support agency to lead the coordination effort.

6. Conclusions

Several lessons can be learned from the data coordination and analysis product distribution challenges faced by responders and top officials in Washington State and Washington, D.C. Plume models provide a prediction of where the material in the explosion will travel. They can be useful in assisting decision-makers in making preliminary decision regarding likely areas of contamination. Once actual data from the incident are collected and evaluated, the value of plume models diminishes. Once responders learn what really is out there and where it is, predictions alone become less important. However, predictions updated with initial measurement data can be useful in estimating protective actions in areas that have not yet been surveyed, or in areas that have been contaminated below the measurement threshold of available instruments. During the FSE, WA State DOH and Federal SMEs could have provided top officials with this information. Additional educational opportunities might have been available in many months leading

up to the FSE.

On-site and off-site data coordination was minimal at best. For SMEs to develop the most up-to-date information and provide the highest quality recommendations, it is critical that they receive data collected from all relevant locations. During the T2 FSE, the coordination to send all of the data to one place was lacking. One aspect of the response that became clear during the FSE was that there are many assets witb radiological data collection capabilities at FSL levels of government that need to be accounted for in the data collection process. In planning responses to terrorist attacks, procedures need to recognize all of the possible responders, and work to ensure that they are coordinating effectively. The development of the National Incident Management System (NIMS) may help to facilitate the data collection and coordination processes in the future.

In addition to the FRMAC, many State and local government agencies have their own capabilities and responsibilities to generate plume predictions and deposition maps. In an emergency, State and local governments are likely to rely on their assets before Federal assistance arrives, and to continue to rely on them throughout the response and recovery. The Federal Government cannot prevent other FSL agencies from using their own models and developing their own predictions for internal planning purposes. However, FSL agencies and departments can be educated about the importance of centralizing the data collection and analysis product distribution processes and learning to work with the FRMAC to coordinate efforts during radiological emergencies and the consequences if that does not happen.

E. Play Involving the Strategic National Stockpile

1. Introduction

In Illinois, during the Top Officials (TOPOFF) 2 (T2), the arrival, breakdown, distribution, and dispensing of the Strategic National Stockpile (SNS) was played in unprecedented detail during the Full-Scale Exercise (FSE). It culminated in the dispensing of thousands of doses of simulated medication to role players at five separate sites, in five jurisdictions. However, perhaps of even greater interest than the actual distribution were the discussions and decisions leading up to the distribution activities. Officials had to determine:

- How to request the SNS;
- Who should receive the medications;
- How much was available;
- When and where to distribute it; and
- How to announce it to the public.

This account focuses on how the local municipalities dealt with the issues of providing prophylaxis to both first responders and the public. It also examines decisions made about the SNS at the inter-agency level.

2. Background

Created in 1999, the SNS is a national repository of medications and other supplies and equipment that can be deployed in the event of a terrorist attack. Formerly known as the National Pharmaceutical Stockpile, the SNS was renamed upon its transfer to the Department of Homeland Security (DHS) in 2003. The SNS is a multi-agency resource, with responsibilities split across DHS, the Department of Health and Human Services (HHS), and the Veterans Administration. According to a recent Memorandum of Agreement among the three departments:

> *The DHS Secretary shall, in coordination with the HHS Secretary and the Secretary of Veterans Affairs, maintain the Strategic National Stockpile.*
>
> *The DHS Secretary shall be responsible for the overall strategic direction, goals, objectives, and performance measures for the Stockpile.*
>
> *The DHS Secretary shall be the owner of the Stockpile and the assets (excluding personnel) of such Stockpile shall transfer to the DHS Secretary. The Stockpile shall remain in the physical custody of the HHS Secretary until deployed by the DHS Secretary.*
>
> *The DHS Secretary, in consultation with the HHS Secretary, shall direct the deployment of the Stockpile, determine pre-position locations and shall have the responsibility for authorizing the transfer of custody of Stockpile contents to State or local authorities.*

However, while giving ownership of the stockpile to DHS, the Memorandum of Agreement assigns management responsibilities to HHS:

> *In consultation with the DHS Secretary, the HHS Secretary in managing the Stockpile shall determine for the Stockpile the appropriate and practical numbers, types, and amounts of drugs, vaccines, and other biological products to provide for the emergency health security of the United States.*[82]

The Centers for Disease Control and Prevention (CDC) maintains the SNS within HHS.

The SNS consists of two parts: the 12-hour push package (push pack) and Vendor Managed Inventory (VMI). CDC maintains 12 push packs strategically distributed at ten sites around the nation. Upon release by the CDC, the SNS can deliver a push package to the site of an emergency in 12 hours or less. Thus, it can be deployed before the specific infectious agent has been confirmed. Each push pack contains more than 50 tons of supplies. Depending upon the infectious agent, a push pack can treat from several thousand to several hundred thousand people. In a large bioterrorism incident, the VMI can also be deployed. It's tailored to contain the specific medications to treat victims of a known agent. The VMI can arrive in the affected area within 24 to 36 hours. Either the VMI or the push-package can be shipped first, depending on the situation.

Illinois also maintains its own pharmaceutical stockpile, known as the Illinois Pharmaceutical Stockpile (IPS), and some localities maintain their own stockpiles of medications. The IPS is designed for use by immediate responders.[83] Use of these stockpiles was also played during the FSE.

3. Reconstruction

a. Overview

The SNS Operations Center (SNSOC) was activated at 1500 EDT May 12, 2003, based upon a directive from DHS. In a conference call at 2000 EDT, HHS Secretary's Command Center (SCC) directed that two SNS sites nearest to Chicago be readied for loading onto planes. It is not clear, however, whether the SNSOC received this directive. The SNSOC did receive a directive from DHS to pre-deploy a push package to the Chicago area, which it did. The City of Chicago, followed closely by the State of Illinois, requested the SNS early on the afternoon of May 13, 2003, immediately after a bioterrorism incident involving the release of Pneumonic Plague was confirmed. The next morning, officials publicly confirmed that there had been a release of plague at the United Center, O'Hare International Airport, and Union Station, and only at these three sites. At 1025 Central Daylight Time,[84] the push pack arrived at O'Hare. It was distributed to the local jurisdictions that afternoon, after which most jurisdictions issued prophylaxis to their first responders. The follow-on VMI supplies began to arrive at 1937 on May 14, 2003. The distribution sites were opened to the target population at 0800 on May 15, 2003, at the same time that the Virtual News Network (VNN) announced the distribution

[82] Memorandum of Agreement between the Department of Health and Human Services and the Department of Homeland Security concerning cooperative arrangements to prevent, prepare for, and respond to terrorism and major disasters, signed February 28, 2003 and March 5, 2003.
[83] Illinois Department of Professional Regulation State Board of Pharmacy, [Newsletter] Feb 2003.
[84] All times provided are Central Daylight Time, unless otherwise noted.

locations and listed the target population. Figure 15 depicts the timeline of events related to the request for and distribution of the SNS.

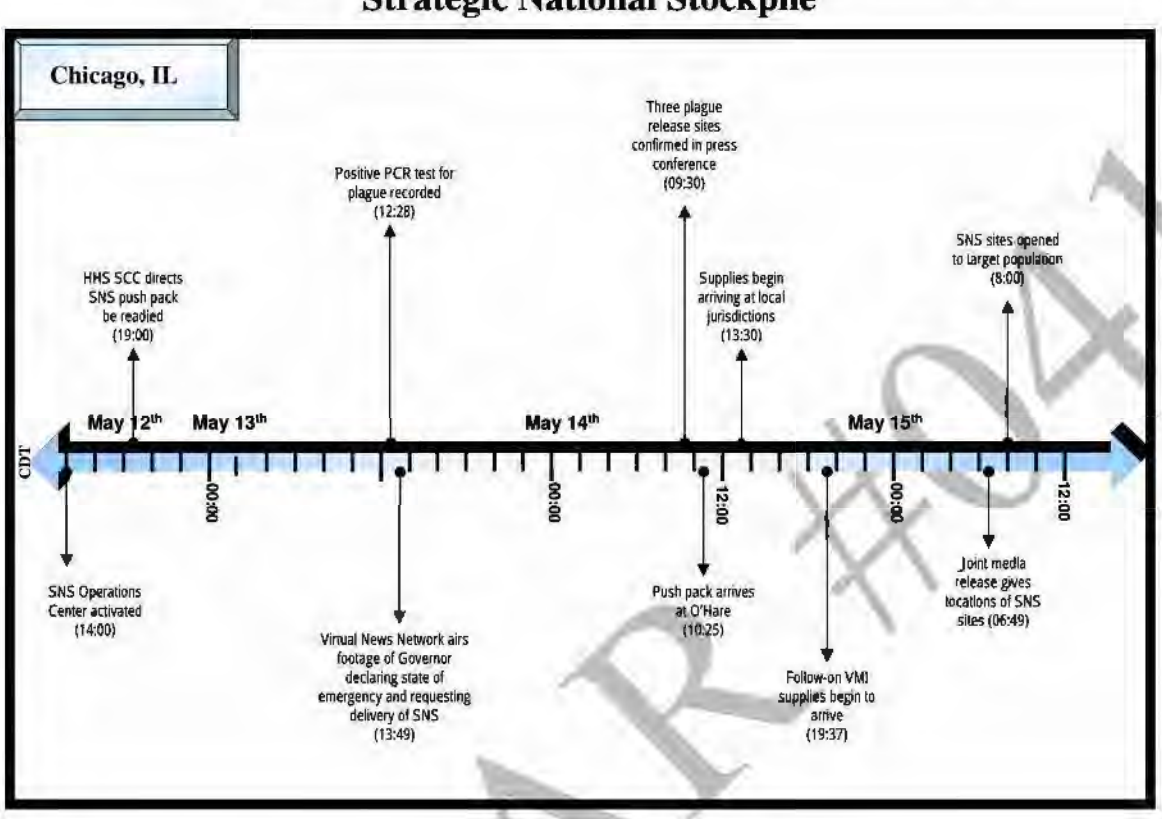


Figure 15. Timeline of Events Related to the SNS

b. Initial discussions

Decisions and activities relating to the SNS took place at all levels of government. On the morning of May 13, 2003, before diagnosis of plague, discussions began at local and State departments of public health (DPHs) about the need to provide prophylaxis and to request and activate pharmaceutical stockpiles—local, state, and national. The SNS also came up in discussions at the Federal Emergency Management Agency (FEMA) Region V Regional Operations Center (ROC); the HHS Region V Regional Emergency Operations Center (REOC); the County, City, and State Emergency Operations Centers (EOC); HHS Headquarters; DHS Headquarters; and the Strategic Information Operations Center (SIOC) in Washington, D.C.; and the CDC in Atlanta.

HHS had already alerted CDC to have the SNS ready to go. On May 12, 2003 at 1900, anticipating a rise in the threat condition to Red, HHS directed CDC to put the stockpile on planes, with the two closest to Chicago ready to go. At 1946, having heard that threat condition was raised to Red in seven cities, the HHS Assistant Secretary Public Health Emergency Preparedness told his staff to notify CDC to load the planes—a standard operating procedure for the CDC upon Red being declared.

At 0800 on May 13, 2003, CDC reported that the SNS was being deployed to Chicago. At 1030, the CDC Director reiterated public health priorities. One of these was to focus on the immediate needs of Chicago, as well as Seattle which had just experienced the detonation of a radiological dispersal device (RDD), but not to over-commit CDC resources, as there was a potential for multiple terrorism events in other parts of the country. In an 1100 conference call with HHS, the ROC, and the REOC, CDC reported that the SNS could be delivered to Chicago within an hour. At 1228 the Chicago, Illinois Department of Public Health (IDPH) lab recorded a positive Polymerase Chain Reaction (PCR) test for plague. However, it wasn't until 1415 that CDC received notification of the positive PCR; at that same time the confirmation of plague was announced on VNN.

On May 13, 2003, at 1730 EDT, HHS Secretary Thompson declared a public health emergency in the City of Chicago, allowing HHS to provide federal health assistance under its own authority.

c. Requesting the stockpiles

In Illinois during the afternoon of May 13, 2003, local jurisdictions and the state declared a state of emergency and requested the SNS. There was some confusion as to when declarations were officially declared by the individual jurisdictions. At 1253, the FEMA ROC log noted that the City of Chicago was requesting the SNS; a similar entry regarding an urgent request from the state was logged at the ROC at 1325. Discussions about requesting the SNS occurred at the DPHs starting about 1330. At the DHS Crisis Action Team (CAT) at 1430, there was discussion of deploying the SNS. A request from the City of Chicago for a push pack showed up in the Department of Homeland Security (DHS) Homeland Security Center (HSCenter) at 1528 and at the CDC around 1600.

At 1250, VNN aired footage of the Illinois Governor reporting that that he had declared a state of emergency in Illinois, requested a disaster declaration from the President, and requested delivery of the SNS. At 1410 the Illinois Operational Headquarters and Notification Office (IOHNO) reported that the Illinois State EOC would request the SNS (push pack and VMI) through the Governor's office; at the same time Cook County DPH checked with the state for procedures.

At 1515, IDPH notified the SEOC to ask for surgical masks and ventilators as part of the VMI request. Later that afternoon, in a conference call at 1655, discussion ensued about procedures for requesting the SNS. IDPH went directly to CDC, whereas the Illinois Emergency Management Agency (IEMA) went to the ROC. On May 14, 2003, at 0935, IOHNO logged specific requests from the VMI for Doxycycline, Ciprofloxacin, masks, and ventilators.

d. Who should receive antibiotics

Internal debates about a prophylaxis distribution policy for first responders, including non-governmental organizations such as the American Red Cross, and the public occurred in all local jurisdictions. These discussions were necessitated not only by the enormous logistical challenges of distributing medications to a metropolitan area whose population exceeds seven million, but also by the very real limits of the amount of medication that was immediately available.

In the end, all jurisdictions except Chicago decided to provide prophylaxis to all first responders. Chicago was unable to do this due to the sheer size of their first responder population, estimated

at 96,000, and because officials felt it would be politically untenable to provide medications to all of the first responders before the providing the same for the general public.

The distribution of simulated local pharmaceutical stockpiles was demonstrated in Chicago and DuPage County. Chicago DPH administered prophylaxis from its own stockpiles to Chicago DPH staff (on May 13, 2003, at 1640). DuPage County followed its protocols and administered its stockpile to its first responders and their immediate families (a decision made at 1326 on May 13, 2003) and County employees (distribution began at 0914 on May 14, 2003).

Within the Lake County EOC, there was a discussion as to how many people in each category should receive prophylaxis. They also discussed who would make the decision about how many people to provide prophylaxis for. In the end, they decided on all first responders per protocol.

Both Cook County and Lake County issued prophylaxis to first responders at 1600 on May 14, 2003; it is unclear whether they used the IPS or the SNS. Chicago, however, issued medications to a single shift of first responders only: those on duty during the early morning hours of May 15, 2003. They did not distribute the antibiotics earlier due to a miscommunication; they believed that all jurisdictions had agreed to delay distribution of the SNS to anyone until 0800 on May 15, 2003. Chicago learned that the other counties had already distributed to first responders via an email at 1926 on May 14, 2003, stating that all Cook County first responders had received prophylaxis. At that point they began to make plans to do their own, partial distribution to first responders. At 2039 on May 14, 2003, a broadcast fax advised the Chicago district watch commanders to pick up prophylaxis packages; they were distributed to police officers beginning at 0032 on May 15, 2003.

As far as prophylaxis for the general public, there was also a city/county divide. The counties initially decided to offer prophylaxis to their entire communities. Chicago, again, differed. In a conference call at 1300 on May 14, 2003, the counties and IDPH discussed the situation. That morning, the plague outbreak had been publicly linked to three locations: a terminal at O'Hare International Airport, the United Center, and Union Station. Ultimately, all realized that a common policy had to be adopted to prevent one jurisdiction from potentially being overrun by citizens of another that had decided upon limited distribution. That realization was helped along by a recommendation from IDPH, which called for a distribution targeted at the following:

- People who were in the United Center, O'Hare Terminal 3[85], or Union Station on May 10, 2003; and
- People who had household contact with any presumed or diagnosed cases.

Although some of the counties were unhappy with this policy and discussed overriding the decision, all eventually agreed to it.

Later that afternoon, at 1445, IOHNO noted that IDPH recommended and the counties concurred that an individual could pick up medications for other family members if he/she provided the required information.

Chicago's final decision, based upon a Chicago DPH recommendation, was announced at a 1730 EOC briefing: the first people to receive antibiotics were those in contact with cases, attendees at the venues, and first responders likely to be in contact with contaminated people (those on shift

[85] The release was later determined by consensus to have been Terminal 2, not Terminal 3.

when the drugs were distributed). They anticipated a quick backfill of antibiotics for the remaining first responders and their families.

e. How much was available

Confusion and contradictory information complicated officials' decision-making. First was the difficulty of determining the amounts in local stockpiles. Second were the issues about how much the state had and how the medication would be allocated. Finally, there were questions about how much would come from the SNS, when it would arrive, and how much each jurisdiction would receive.

An account of the confusion is documented here, focusing on the largest jurisdiction, the City of Chicago:

At 1715 on May 13, 2003, Chicago EOC requested 1.1 million doses of prophylactic antibiotics from IEMA, including 96,000 for first responders. Other jurisdictions requested lesser amounts; for example, Lake County requested 15,000 for its first responders and their families.

During a conference call starting at 1730, which included the FEMA ROC, IEMA, IDPH, and Chicago Office of Emergency Management (OEM), the OEM Director asked how many doses would he coming. IEMA replied, "enough, and will continue to re-supply." The city pressed for a number. IEMA said it was still determining the number. Chicago asked if this would be an open faucet, noting that its distribution schedule would depend upon the number of doses received. The ROC replied that the supply didn't seem to be a problem. Shortly thereafter, at 1818, the Chicago OEM director reported to his staff that the city was getting one million doses.

On May 14, 2003, IDPH decided that the stockpile would be broken out by jurisdictional populations. The IDPH Chicago office came up with these numbers for the initial distribution (a total of 45,800 doses[86]) for the entire region:

- City of Chicago 12,400 doses
- Cook County 12,500 doses
- DuPage County 10,500 doses
- Lake County 6,000 doses
- Kane County 4,400 doses.

At 0917, the county health departments received a fax with these numbers.

About an hour later, however, Chicago DPH reported to the EOC that IEMA and IDPH said the city would receive 30,000 from the Illinois stockpile and 30,000 from the SNS. The Chicago DPH reported this again at 1150. They were expecting 60,000 doses available for Chicago.

At 1030, the Chicago OEM requested clarification during a conference call that included IEMA, the IL State EOC, and the Joint Operations Center (JOC). IEMA replied that the city would get 30,000 from the IPS and 12,400 from the SNS. However, at 1154 IDPH told Chicago DPH that the total of IPS and SNS doses was 30,000.

[86] It is not clear whether by "doses" they meant regimens (i.e. pre-packaged 10-day treatment courses). Each push pack contains pre-packaged regimens of Ciprofloxacin and Doxycycline.

The crisis over amounts of antibiotics available was definitively over at 1937 on May 14, 2003. At that time the IL State EOC announced in an exercise inject that VMI had arrived and that local health departments and hospitals would continue to be supplied for the length of the event.

The lack of clarity over available amounts illustrated by the above sequence of events can at least partially be traced to agencies sometimes co-mingling state and federal supplies, and also to a failure to separate out, in number and timing, the relatively small amounts in the push pack compared to the continuing flow of VMI.

f. When and where would the supplies be available

At 1730, on May 13, 2003, during a teleconference between FEMA, CDC, IEMA, and the governor's office, it was announced that the SNS would arrive at 1000 on May 14, 2003.

According to an exercise inject, the stockpile arrived at O'Hare airport at 1025 on May 14, 2003. It was transferred to a warehouse at 1055, at which time CDC signed it over to local authorities. The supplies were broken down and started arriving at the jurisdictions at 1330. Jurisdictions had pre-planned sites for distribution of the SNS to the target population, and an agreed-upon time for opening them. The distribution sites opened to the public at 0800 on May 15, 2003.[87]

g. How were these decisions conveyed to the public

The public was informed that the SNS was available if needed by the Assistant Secretary Public Health Emergency Preparedness in HHS. At 1322, on May 13, 2003, the Secretary reported via VNN that the SNS was in the Chicago area and ready to be deployed. At 1527, VNN reported that the SNS was being rushed to Chicago.

A press release from the Office of the Governor early during the afternoon of May 13, 2003, indicated that antibiotics from the SNS would he distributed hy local health departments to those with symptoms or those exposed. People with symptoms were told to go to the nearest hospital. Those exposed to the symptomatic were told to receive antibiotics.

In a press conference at the Joint Information Center (0930 on May 14, 2003), the three release sites, O'Hare International Airport, Union Station, and United Center, were confirmed.

On May 14, 2003, at 0940, IOHNO suggested on VNN that anyone who was at the three release sites should get prophylaxis. In a 1030 press release from the Governor's office, the Director of IDPH gave the same advice. At 1230 on May 14, 2003, the DHS Secretary on VNN advised all employees at the three sites to go to their doctors to get antibiotics. Chicago DPH, however, issued a press release stating "insisting that all Chicagoans stay at home until further notice, except for those adults considered to be essential to public safety....[and] those experiencing symptoms."

At 1259, on May 14, 2003, VNN announced that the SNS had arrived in Chicago.

At 1345, VNN announced that only 30,000 doses were coming to the Chicago area, whereas at 1745, a HHS official on VNN stated, "Once the faucet is turned on, the flow [of medication] doesn't stop."

At 1407, on May 14, 2003, there was a conference call that included the JOC, as well as the City and State EOCs about how to use the media to encourage people to stay home instead of rushing

[87] The Lake County site opened at 0832.

to the distribution centers. The message would be: "Stay home unless you're in the exposed target groups; otherwise, going to the distribution site will increase your risk of infection."

At 1425, in a conference call between IOHNO and CDC, consensus was achieved that a release would be issued that evening stating that distribution sites would be made public on the morning of May 15, 2003.

At 0800 on May 15, 2003, VNN issued details on distribution, identifying the locations and the target populations, including a change in who should go for medications. Symptomatic people were told to seek medical attention. Persons exposed to people with symptoms, those who had been at the three release sites, and those exposed to them were advised to go to their local distribution center.

At 0830 May 15, 2003, VNN reported that SNS had plague treatment for 115 million people.

4. Artificialities

None of the pharmaceutical stockpiles were actually deployed. SNS provided their training, education, and display package at the request of Illinois State to allow Illinois to test its ability to receive and distribute a push package. It is an exercise artificiality that the push packages were deployed at all. In a real event, the SNS reaction to requests for SNS would have been to send VMI, since pneumonic plague was already identified. It is unclear what the public reaction to the targeted distribution scheme would have been[88].

For reasons of space availability, the T2 scenario required that the SNS to arrive on the May 14, 2003, and be distributed at 0800 on May 15, 2003. This schedule gave decision-makers the luxury of time to discuss and determine in concert how to distribute the medications, and they didn't even have to coordinate the time of distribution; it was given to them. In real life, pressures for a faster distribution would have made such coordination more difficult. With a compressed timeline and during a real emergency, jurisdictions might have made different, independent decisions and chaos could have been the result. In fact, discussions during this time period in the HHS SCC indicated continuing concern about the delays in opening the distribution centers.

Ultimately, the VMI was declared sufficient for the State's needs. The health departments discussed offering mass prophylaxis after they were told that the amount of antibiotics was no longer an issue.

5. Analysis

The SNS story spans five of the areas of analysis and the inter-agency and Illinois venues. It is first and foremost the story of emergency public policy and decision-making regarding the allocation of a scarce resource. It involved jurisdictional issues at the Federal and local levels. It is also the story of local jurisdictions coming to separate decisions and then coordinating them (with some help from the state) to reach a common policy. Successful distribution required a coordinated, well-thought-out and accurate public information campaign.

[88] Dr. Henry W. Fischer, III, in his book, "Response to Disaster: Fact Versus Fiction and Its Perpetuation—The Sociology of Disaster," predicts that panic would not ensue in a bioterrorism attack, but there is thankfully no data to draw upon to validate this prediction. Dr. Fischer does not specifically address the complications that could arise with the distribution of prophylaxis.

a. Decision-making

The key decisions regarding the SNS were who should get the antibiotics and in what order. To make those decisions, officials needed different types of information:

- Which antibiotics would be effective;
- How quickly would they need to be administered;
- How much was available;
- How long would it take to get the antibiotics; and
- How quickly could they be re-supplied?

During the FSE, decision-makers received conflicting information regarding the amount of antibiotics in the stockpile. Knowing the answers to the following questions would help officials better plan their strategy for distribution:

- Was there enough medication to provide prophylaxis to all first responders or would it need to be done in stages;
- If done in stages, would it be best (or possible) to provide prophylaxis to all those on duty and keep them on duty until sufficient supplies arrived for the rest;
- Or would it be better to give partial courses out to all first responders so that all could get started and then receive the rest of the course as more supplies became available; and
- How many sites should be set up for distribution to the citizens, considering the tradeoff between number of distributors (who also need prophylaxis) and number served?

Decisions made by the City of Chicago typify the importance of good information. Chicago, with its huge population, was the most hard-pressed jurisdiction.[89] It requested 1,063 million doses and waited for information from the state as to how much they would actually get. The state came back and said they could have 40,000 doses; however, it ended up with only 12,400. The city made distribution plans based on the 40,000 number. It chose not to provide prophylaxis to all first responders before reaching out to the public because it was concerned about adverse public reaction. Chicago decided instead to take a parallel approach, giving medications to current shifts of first responders, and at the same time providing medications for people who were at the three venues and the primary contacts of symptomatic patients. It is not clear if the city could actually have accommodated all of these people with the medications available to them at the time.

b. Resonrce allocation

The various pharmaceutical stockpiles constituted a scarce resource, at least until the VMI portion of the SNS began flowing. Some of the local jurisdictions had their own stockpiles, which they used to provide prophylaxis to different parts of their population: Chicago DPH gave antibiotics to its own staff; DuPage County administered its supply according to its phased plan,

[89] Cook County is almost equally large, but less data was available on their decision-making.

providing medication to first responders and their families and County staff and their families. The other jurisdictions apparently did not have their own stockpiles.

These differences raise policy issues. If some jurisdictions have their own stockpiles, should that be taken into account in allocating the supplies from other stockpiles? Such calculations appeared not to have been made, as the amounts provided to the localities from the state and local stockpiles were based upon population.

In addition, if the state issues guidance to medicate only first responders in advance of the general public, can a locality provide antibiotics to other segments as well out of its own stockpile? Would it then receive less from state and national stockpiles? Questions such as these become increasingly relevant as States and localities debate the advisability of establishing local stockpiles, given the difficulty of maintaining them.[90]

c. Emergency public information

Public information play regarding the SNS had successes and failures. Some pronouncements were made that could have caused some measure of concern and confusion among the public. Several of these may have been due to erroneous VNN statements and not inappropriate judgments on the part of the officials releasing the information. However, a story such as the one describing the 30,000 doses that would be coming to Illinois (when originally there was believed to be 60,000 doses) could have caused chaos at medical facilities. And early recommendations from IOHNO, IDPH, and HHS that people at the release sites should obtain prophylaxis could have caused serious problems.[91] These were made before the SNS had arrived and distribution sites had been set up. Tens, if not hundreds, of thousands of people who fit that description could have descended en masse upon medical facilities and pharmacies to get antibiotics that were not yet available. However, this problem is, at least in part, an exercise artificiality, as the consensus is that SNS play was artificially delayed.

In addition, conflicting advice was given about staying home and going out to get prophylaxis. Whereas IOHNO, IDPH, and HHS recommended that people at the venues obtain prophylaxis, Chicago DPH went on record "insisting that all Chicagoans stay at home until further notice, except for those adults considered to be essential to public safety....[and] those experiencing symptoms."

The crafting of a joint press release about the SNS distribution at 0649 on May 15, 2003 was crucial to the success of the distribution and ultimately to containing the plague. Officials had to do their best to draw out those people who needed prophylaxis, while discouraging those who didn't from coming out and taking the limited supplies and/or unleashing unrest at the distribution sites. They agreed not to release the SNS distribution locations until the morning of May 15, 2003, to minimize the potential for civil unrest and chaos at the distribution sites. The release described who should seek prophylaxis (those at the release sites on the dates indicated, and those within six feet of someone displaying symptoms); where they should go; and when

[90] In June 2002, then IDPH Director John Lumpkin spoke against local stockpiles. When DuPage County asked about receiving reimbursement for the thousands of dollars it had spent on its stockpile, the Director of IDPH replied that, "Counties should not keep individual stockpiles because Illinois has an arrangement with a pharmaceutical company that keeps a current supply available that could be distributed to a county within a short period of time" [from the minutes of a DuPage County Board of Health meeting (6 June 2002)].

[91] In the HHS statement, employees were singled out in the recommendation to receive antibiotics as they were presumed to have been exposed for a longer period.

they should arrive. It dissuaded those who hadn't been exposed from coming by reminding them that they would be safer at home, and stated that people with symptoms should go to the hospital, not the SNS sites.

However, this press release contained a flaw: it miss-stated one of the plague release sites. Confusion persisted throughout the FSE about which terminal was the release point at O'Hare International Airport. At various times, it was called Terminal 2, Terminal 3, and most frequently the International Terminal, which is Terminal 5. On May 14, 2003, around 1000, consensus was reached among public health departments that Terminal 2 was the correct terminal (which it was), hut this information apparently was not passed on. When announcing who should get prophylaxis, the press release listed the international terminal as one of the three release sites. This may have been in part an exercise artificiality, as the myriad of reporters who would have covered this incident in real life would presumably have identified the discrepancies in public statements. But had they not, thousands of potentially exposed individuals could have heen without drugs.

In addition, press releases about the SNS on May 14 and 15, 2003, contained conflicting information on the target population. There were several sets of somewhat differing guidance. The first concerned the dates of exposure. There were three variations:

- People who were at the sites on May 10, 2003;
- People who were at the three sites from May 10 to May 13, 2003; and
- People who were at the United Center from May 10 to May 14, 2003.

The second set concerned the description of who would receive prophylaxis. This set contained both internal inconsistencies and differences among jurisdictions. There were two variations. A press release from the DuPage County Board at 1811 on May 14, 2003, listed those exposed at the sites or those exposed to people with symptoms, and their entire families; however, this release also stated: "only people who have had direct close contact with infected patients should obtain antibiotics." A Chicago DPH press release at 0651 on May 15, 2003, listed those who were exposed at the sites and their close contacts, but only those household members who had been exposed to a person with symptoms. It's unclear whether these statements were actually released and whether the differences in them represented differences in distribution policy or not.

d. Coordination and communications

As noted earlier, miscommunication among the local jurisdictions caused the Chicago OEM to delay prophylaxis to its first responders while the counties went ahead with theirs. Had this played out in real life, it might have caused serious prohlems with the Chicago first responder communities. The Chicago OEM believed it had been told during a teleconference that none of the jurisdictions were distributing any prophylaxis until 0800 on May 15, 2003. This had financial repercussions as they had planned to dispense to first responders that evening; consequently, Chicago had police officers earning roughly one million dollars in overtime pay and doing nothing. When the OEM found out via routine e-mail that other jurisdictions had completed their first responder prophylaxis in the late afternoon of May 14, 2003, it put into play a partial distribution to first responders later that evening.

This misunderstanding can be traced to the medium of the conference call. Without written documentation of decisions reached, the potential exists for miscommunication. This was

observed throughout the FSE. During many teleconferences, roll calls were not taken, and it was unclear as to who was on the teleconference. In addition, on several instances different people heard different things and reached different conclusions about the outcome of the calls.

The conference call was useful as a means of coordination among agencies located far from one another and scattered among the EOCs. However, it was far from ideal as a reliable means of communication. These issues in the public health community were observed in TOPOFF 2000 as well, and were cited by the General Accounting Office in its September 2000 Report to Congressional Requestors titled, "West Nile Virus Outbreak: Lessons for Public Health Preparedness," and in which many officials reported problems in this area as the investigation into the outbreak grew. These problems could be ameliorated through strict adherence to roll call procedures and by designating one party to document any decisions reached and distribute them rapidly back to the participants via e-mail for confirmation.

e. Jurisdiction

The procedures and processes for requesting and receiving the SNS were a source of confusion throughout the exercise. Different jurisdictions took different routes to request this resource, and different agencies in the State also pursued their own paths. IDPH went directly to CDC, whereas IEMA went through the FEMA ROC; both of these are acceptable channels to request the SNS.[92,93] It is unclear precisely what initiated the flow of prophylaxis. The two directives, one from DHS and another from HHS, regarding the deployment of the SNS provide one example of a jurisdictional challenge raised after the creation of DHS.

As noted in the background section, responsibility for this resource is shared between DHS and HHS. According to the Memorandum of Agreement, the decision to deploy the SNS is made by DHS in coordination with HHS. During the FSE, both HHS and DHS were giving directives regarding activation and deployment of the SNS. The SNSOC coordinated the stockpile deployment with the CDC and the FEMA EP&R Director. There is no data to indicate that senior-level consultation occurred between DHS and HHS. This issue was complicated when HHS declared a Public Health Emergency, which would allow it to deploy resources on its own authorities and at its own cost.

The following questions specific to the SNS were brought out during the course of T2:

- What is the process for requesting pharmaceuticals from State and Federal stockpiles;
- Does each jurisdiction have to submit its own request;
- Through whom do they issue the request;
- Can they request from multiple sources; and
- How much does one jurisdiction's request affect those of others?

The question of process arose despite the fact that there is a well-defined process for requesting the SNS (that should be a part of every public health agency's SNS distribution plan per CDC

[92] It would be useful for DHS and HHS to clarify policies on how to request the SNS and educate the states on these procedures.
[93] Jurisdictional issues related to the SNS are discussed further in the *Core Area* on jurisdiction.

guidance). The official process involves a request from the governor or the mayor to the CDC, which then consults with DHS. There is no requirement for a disaster or emergency declaration.

6. Conclusions

The SNS was extensively exercised during the FSE. Local jurisdictions tested their ability to distribute supplies of antibiotics to their first responders and citizens. The state tested its ability to break down and secure the antibiotic stocks. Receipt, breakdown, distribution, and dispensing were completed successfully. But the SNS problem was far greater than the physical breakdown and dispensing of the push pack. It tested the ability of all levels of jurisdictions and agencies to make decisions, allocate resources, coordinate and communicate, and inform the public.

It is clear that work remains to be done in all of these areas. Pressures to make decisions under emergency conditions and tight timelines can be partially alleviated through thorough pre-planning and advance coordination amongst jurisdictions. The challenge is to figure out in advance the procedures for getting good information, sharing it widely, and making and documenting decisions in a coordinated way when operating under severe time pressure.

SUMMARY OF CONCLUSIONS—STRATEGIC NATIONAL STOCKPILE (SNS):

- Overall, the receipt, breakdown, distribution, and dispensing of the SNS during the FSE were completed successfully.
- The SNSOC coordinated the stockpile deployment with the CDC and the FEMA EP&R Director; there are no data to indicate that senior-level consultation occurred between DHS and HHS.
- Miscommunication among local jurisdictions caused Chicago OEM to delay prophylaxis to its first responders while the counties went ahead with theirs.
- Different agencies chose different avenues to request the SNS; this was a source of confusion throughout the FSE.
- Conflicting and confusing information was given to the public regarding who should seek prophylaxis and when, the plague release sites, and whether one should stay home or seek medical attention.

This page intentionally left blank

F. Hospital Play in the Illinois Venue: Resources, Communications, and Information Sharing during a Public Health Emergency

1. Introduction

In the event that a highly contagious and lethal disease is spreading throughout a population, hospitals and other health care providers will become the first line of defense against a large-scale health catastrophe. How hospitals work with each other and the State and local public health authorities is critical to determining whether they will be successful in caring for patients and limiting the spread of the disease. Top Officials (TOPOFF) 2 (T2) presented an unprecedented opportunity to examine the coordinated efforts of the medical and public health communities to react to and control the spread of a disease outbreak. Because of the large number of participating hospitals, communication and resource requirements were significant.

During the T2 Full-Scale Exercise (FSE) an outbreak of Pneumonic Plague was simulated in the Illinois venue. Hospitals from the City of Chicago and the surrounding region participated in the exercise by receiving patients, and sharing information about resources. Hospitals coordinated, or needed to coordinate, in the areas of staffing and personnel, patient accession, the numbers and types of disease cases, diagnostic and treatment information, and diagnostic and treatment resources.

Hospitals used a range of technologies to share information about patients and resources. These technologies included fax, voice, Internet, phone hotlines, and call trees.

This special topic examines two critical issues surrounding hospital play during the FSE:

- How the hospitals communicated resource and patient information during the exercise; and
- What resources the hospitals had available to respond to the outbreak.

2. Background

In the Illinois venue[94] 64 hospitals[95] participated in T2. These hospitals exercised the Illinois Department of Public Health (IDPH) Emergency Medical Disaster plan by responding to both simulated paper and actual patients that arrived at their emergency rooms or were reported to infectious disease personnel. After seeing the patients, the hospitals reported syndromic and other information to the IDPH command center, and the Illinois Operations Headquarters and Notifications Office (IOHNO), located during the exercise in Springfield, Illinois. IOHNO in turn worked with the IDPH and the Illinois State Emergency Operations Center (EOC) (also located in Springfield) to develop an overall picture of the medical situation.

The IDPH disaster plan set up a hierarchal reporting structure for hospitals in the affected counties. Hospitals do not report directly to IOHNO during a disaster. Instead, hospitals within

[94] City of Chicago, DuPage County, Kane County, Lake County, and Cook County.
[95] The evaluation team has data from 60 of the 64 hospitals.

a designated region report to a "POD[96]" hospital. The POD hospital consolidates information from the regional hospitals and then forwards it to IOHNO. Figure 16 illustrates this reporting process.

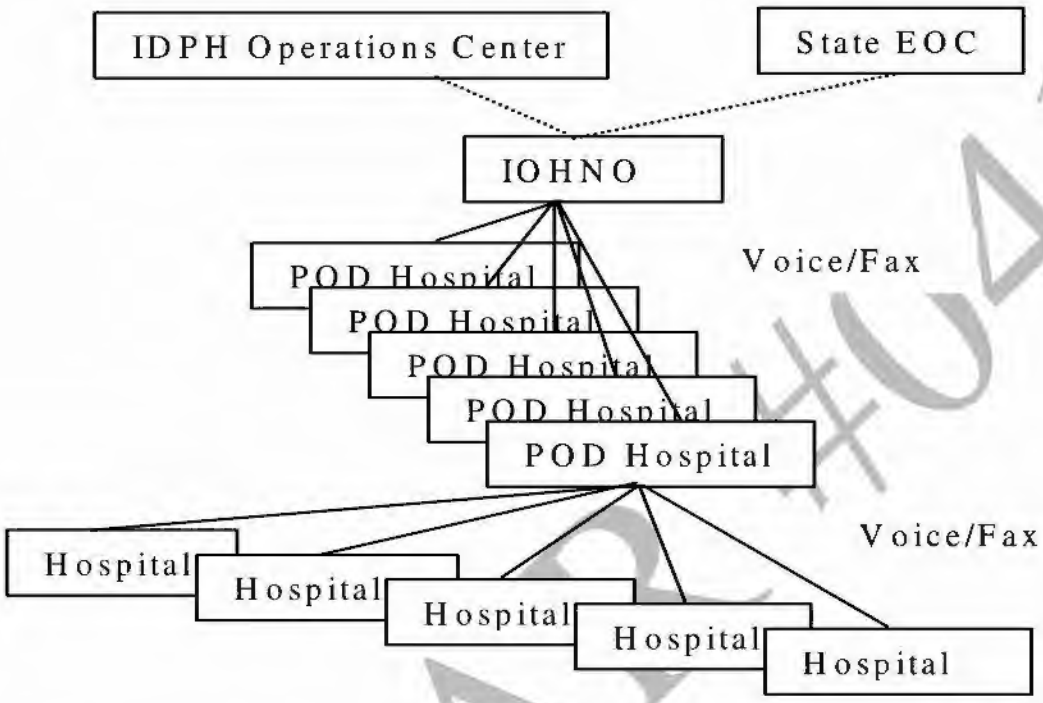


Figure 16. Reporting Architecture

The medical disaster plan was first activated at 0830 Central Daylight Time (CDT)[97] on May 13, 2003, in response to reported cases of Pneumonic Plague in DuPage County. The trigger was the result of an alarm on the DuPage County Pro-Net syndromic surveillance system. This system collected syndromic information from hospitals in DuPage County using a Web-based interface. The data collected are evaluated by software to determine if there are any unusual clusters or trends occurring. If an unusual spike in cases is detected the system alerts the local public health responders via a pager system. The initial alert on Pro-Net occurred at 1729 on May 12, 2003, due to an increase in respiratory patients at Edward Hospital, the first hospital to receive the simulated plague patients. In addition, the IDPH had sent a fax at 1545 to all hospitals on the subject of the TOPOFF Pulmonary Syndrome (TOPS). The fax was actually marked 2200 but was sent at the earlier time due to a controller miscue.

The detection of an unusual number of respiratory cases in DuPage County triggered Phase I of the Public Health Emergency Plan. Upon declaring a Phase I Emergency the POD hospitals are to contact hospitals within their regions and request information for the Phase I Disaster POD

[96] "POD" is not an acronym in this usage.
[97] All times referenced are CDT unless otherwise noted.

Worksheet. Table 6 lists the data elements collected on this worksheet. After collecting this information, the POD hospital is to transmit it to the IOHNO via telephone and fax.

Table 6. Data Elements from Phase I Worksheet

Emergency Department	Trauma Center	Adult Beds
Pediatric Beds	Total Other Beds	Total Units Blood
Ventilators Adult	Ventilators Pediatric	Ventilators Both
Field Bags	Decontamination Walking/hour	Decontamination litter/hour

The Emergency Medical Disaster plan data flow through the hospital emergency departments (EDs) then to IOHNO. During the FSE, patient data also reached IDPH through the infectious disease reporting system. By law hospitals have to report certain communicable diseases to their local health departments. This is usually done by the hospital's Infectious Disease Control Nurse who is to report incidents of diseases directly to the local (city/county) health departments. In turn the local health departments report to the IDPH Infectious Disease Control. During the FSE, the Infectious Disease Control personnel co-located with IONHO in order to facilitate coordination.

Activation of Phase II of the Emergency Medical Disaster plan occurred at 1235 on May 13, 2003. Phase II activation was based on diagnosis of Pneumonic Plague in the suspicious respiratory cases. The Illinois Governor declared a statewide emergency at 1230 on May 13, 2003. In addition to the IDPH and state declarations, numerous city and county emergency declarations occurred during this time period.

Phase II activation requires additional, specific, information be reported by hospitals within the POD regions. Upon notification participating hospitals report information on the number of patients currently in the hospital, the type of conditions these patients have been admitted for, and the number of available beds of different types. The data are documented in Table 7.

Table 7. Phase II Resource Availability Worksheet. Hospitals Report the Number of In-patient Beds Currently Available for the Following Types of Hospital Care Beds

Medicine	Psych	Surgery	Orthopedics	Burns
Spinal Cord	OB/GYN	Pediatrics	Negative Air Pressure	Total

These bed totals are reported to the POD hospitals by telephone and fax, collected, and in turn reported by the POD hospitals to the IOHNO.

3. Reconstruction/Analysis[98]

a. Communications and information flow

Throughout the exercise hospitals communicated with each other and the public health system to:

- Determine the status of beds, rooms, and supplies;
- Recall additional personnel as needed;
- Clarify the specifics of the exercise agent, including appropriate protection and treatment protocols; and
- Request assistance in the handling of the dead.

A variety of communication methods were employed during the exercise including phones, fax, in-hospital public address systems, pagers, radios, human runners, and amateur radio operators (HAM). These communications are summarized in Figure 17. The vast majority of all communications (eighty-six percent) were by either phone or fax. These transmissions included both those within each hospital and conversations/faxes to other hospitals and agencies within the emergency response community.

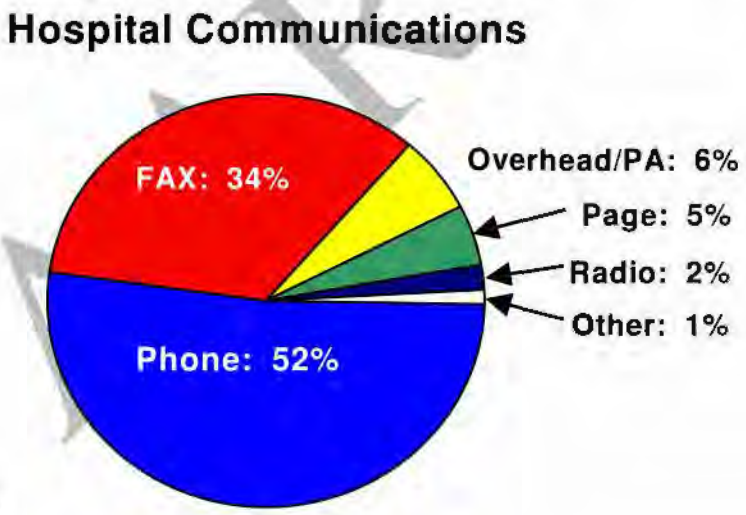


Figure 17. Hospital Communications (all transmissions, all targets)

Problems were noted with most of these communications routes. Telephone calls were hampered by problems with incorrect phone numbers, changes in contact phone numbers (at both

[98] This topic does not lend itself to a chronological reconstruction of events. The reconstruction is effectively an account and analysis of various dimensions of hospital response to the bioterrorism attack. For this reason, the Reconstruction and Analysis sections are combined.

the Illinois and Chicago Departments of Public Health) necessitated by extremely high in-bound call volume, and outbound call volume that caused difficulties in obtaining outside lines.

These problems caused delays in reporting resource information and also made it difficult for hospitals to recall staff through the use of phone trees. Call volume was the greatest problem; even exercise traffic exceeded some call switching capacities. For example, exercise traffic overwhelmed the phone system in south Kane County on May 14, 2003, necessitating the use of three HAM radio operators in order to maintain communications connectivity.

Faxes suffered from their own transmission and receipt problems due to call volumes. "Blast fax transmissions" from IOHNO, used to provide a wide variety of information and exercise updates, took up to two hours to complete. Some fax transmissions early in the exercise weren't reviewed immediately because the receiving fax was in an office locked for the evening or not easily read by ED staff. Because of this, some hospitals designated individuals to staff the fax machine.

Radios were used primarily to communicate within a single hospital or between hospitals and incoming Emergency Medical Service (EMS) units. In addition, radios were used for backup communications at both St. Therese and LaGrange Hospitals during phone outages in the ED.

A great deal of effort was made during the exercise to obtain and update the listing of available resources reported by phone or fax. As shown in Figure 18, at least twenty percent of hospital exercise communications consisted of this type of reporting. It is important to realize that not only do these reports take time to send, but it also requires a great amount of time to obtain the information contained in these reports. The information consists primarily of bed counts, ventilator counts, and the number of rooms available at each hospital. Those counts were obtained either through additional phone calls to floors throughout the hospital or via walking the hospital floors to obtain the counts. This type of inventory effort was repeated throughout the exercise – usually at three- to four-hour intervals—at each of the 64 participating hospitals.

The remaining hospital communications consisted of notifications, mostly those associated with deaths. In addition, normal ED operations required a wide variety of contacts inside and outside of the hospital. A partial list of the individuals or departments called from the EDs includes: the hospital Chief Executive Officer and Vice President for Medical Affairs, the Command Center, floor nurses, the Intensive Care Unit, Infection Control, the Pharmacy and Blood Bank, housekeeping, and transportation.

Communications were also required among numerous agencies and organizations outside of the hospital, including, among others, the coroner, the American Red Cross, the Poison Center, the IDPH, and the county Department of Public Health (DPH), and the county's Office of Emergency Management (OEM).

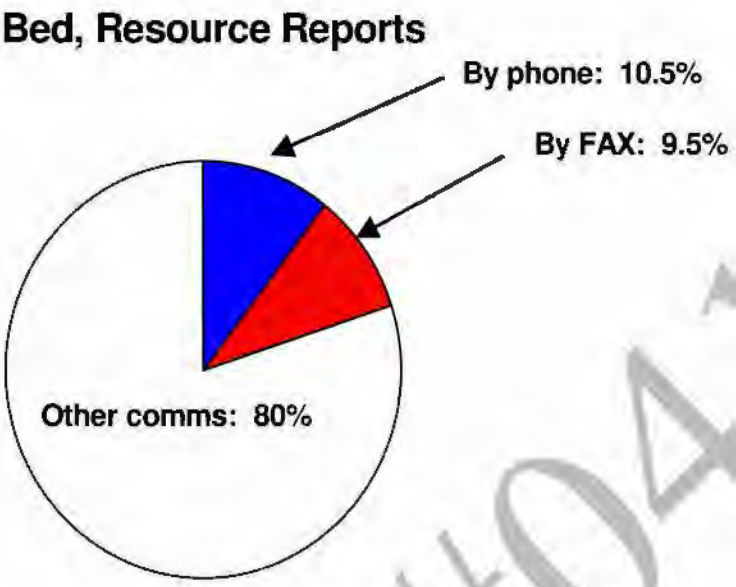


Figure 18: Hospital Resource Reporting

b. Beds

Twenty percent of all communications involved asking for and sending resource information. Counts of available patient beds were needed to determine if patient loads required additional resources, up to and including field hospital deployment. Therefore, as part of normal emergencies, individual hospitals provided bed counts to their coordinating POD hospitals, where the information was consolidated and sent to IOHNO.

During the exercise, a number of observations indicated that this process was difficult, at best. A data collector wrote, "An observation is this hospital is dealing with a large amount of paperwork—dealing with bed availability of POD hospital"

Some confusion existed as to the "why" of bed counts and the "which" of bed counts. For example, a data collector observed: "Discussion with physician about full disaster mode and purpose of meetings to know what beds available and sending patients as fast as possible to keep ER [emergency room] free."

The nursing supervisor talked to hospital staff about requesting a federal count, but there was confusion as to exactly which beds were to be included in the count.

At least six hospitals did experience maximum capacity situations, when either the entire hospital was full, or all the critical care beds or intensive care beds were in use. One hospital reached capacity at noon on May 13, 2003, two additional hospitals reached Intensive Care Unit (ICU) capacity shortly thereafter on the same day, and a fourtb later that same evening. The next day's play filled the fifth hospital's ICU beds by noon. By early afternoon on Wednesday May 14, 2003, the sixth hospital's ED doctor indicated, "We're coming to the breaking point." At the same moment, the bed placement nurse commented to Hospital Admitting, "We are running out

of critical care beds." Since Pneumonic Plague can cause severe respiratory disease, critical care and ICU beds will be at a premium if such a bioterrorism attack were ever to occur.

Types of beds needed to treat patients (as played during exercise)

During the exercise, a variety of bed types were specifically requested as part of normal medical treatment of the exercise patient population. These types included intensive care beds (ICU, Thoracic ICU, Mobile ICU, Pediatric ICU, and Surgical ICU beds), critical care beds in the Critical Care Unit (CCU), medical-surgical beds, other general medical floor beds, and pediatric beds. In addition to beds, monitoring capabilities were required for a portion of the patient population, and were requested as deemed medically necessary. The need for respiratory isolation and negative pressure rooms during the outbreak of a contagious respiratory disease was noted; the details of those specific requirements are discussed in the next section.

Bed use strategies and coordination

The FSE hospital play demonstrated the flexibility and creativity of hospital staff—as they juggled bed requirements for a significant influx of Pneumonic Plague patients. Different strategies were used to maximize the number of beds available to serve patient needs. For example, a wide variety of "other" beds were located throughout the hospitals and used for exercise patients. Throughout hospitals extra beds were found in Occupational Health, Ambulatory Care, Psychology, and Labor and Delivery. In at least five hospitals, additional beds were placed in the Endoscopy laboratory. The Physicians Treatment Center associated with another hospital was used for additional beds. One hospital also considered the suggestion that an entire wing be emptied, a suggestion that was not notionally implemented.

Significant numbers of personnel were directly involved in bed coordination efforts during the exercise. These included, but were not limited to, the following staff positions:

- Nursing Supervisor;
- Bed Coordinator;
- Bed Control;
- ED Charge Nurse;
- Nurse Manager;
- Case Manager;
- Doctors;
- Admitting;
- Maintenance;
- Registration; and
- Administration.

The coordination of this information was done through phone calls, fax, and hard copy tracking using dry erase boards throughout the exercise.

c. Staff

In addition to other resources, considerable staffing is required to respond to a major outbreak. The staff is required to treat and support the patient load, as well as support the administrative and command and control workload that will be placed on the hospital to support various coordination requirements. The FSE response proved to be no different. Staff phone trees were activated on both days of hospital play to recall doctors, nurses, and other staff to assist in the response efforts.

Staff recalls included not just doctors and nursing staff, hut also receptionists and administrative personnel to handle paperwork requirements, housekeeping staff, technicians, computer personnel, and security, if lockdown procedures proved necessary. These individuals formed the basis for an emergency labor pool.

During the FSE, there were also other functions to which hospitals did not always assign a particular staff member. These jobs included persons to staff the radio full-time, staff the fax full-time, staff phone hotline(s) for the puhlic, and assist in making phone calls.

Other infectious disease needs also require coordination to permit emergency personnel to work during an outhreak or a bioterrorism attack. These include childcare for the staff during the outbreak; one hospital's childcare facility notified the ED that they would stay late to accommodate staff needs. In addition, extended hours also mean that additional food and cots/beds are necessary during the outbreak.

d. Isolation rooms

Because of the recent Severe Acute Respiratory Syndrome (SARS) outbreak, the need for isolation and reverse pressure rooms has been highlighted, especially in the context of an unknown respiratory disease that may mimic SARS in its infectivity. These two types of requirements also played a role in the hospitals' responses to the T2 exercise epidemic.

Isolation Strategies

Three types of isolation levels were used in the participating hospitals. Initial patient presentations indicated the probable need for respiratory isolation and/or maintenance of the patient in a negative air pressure room. In addition, IDPH sent out an isolation directive on the evening of May 12, 2003. Later during the exercise, when the agent was identified as Pneumonic Plague, these isolation requirements were revised to the appropriate droplet protection level.

Because isolation rooms were in short supply, and at least two hospitals used up their supply of isolation rooms during the exercise, a number of alternatives were employed to provide patient isolation. Hospitals used lobbies, extra conference rooms, and Clinical Decision Units (closed units) among other spaces.

Negative pressure rooms are also normally in short supply. At least three hospitals used up their supply of negative pressure rooms at various points during the exercise. Again, hospital staff developed a number of alternatives to deal with the short supply including the use of spaces in radiology, same day surgery, the Endoscopy lab, and an off-site tent with negative pressure.

In addition, at least six hospitals contacted maintenance/facilities personnel to request additional reverse pressure rooms. Lastly, because both isolation and negative pressure rooms were in short

supply, at least eight hospitals placed their Pneumonic Plague patients in either isolation rooms or reverse pressure rooms.

Changeover to droplet isolation

As soon as the causative agent in a respiratory epidemic is determined, it should be possible to downgrade the isolation levels to droplet/contact precautions. The downgrading to the lower precaution level, however, did prove to be somewhat confusing and required confirmation. As seen in the following group of observations from May 13, 2003, one hospital took almost ten hours to be convinced; even after a number of checks, the Vice President for Medical Affairs had to convince the hospital ED staff that contact and droplet isolation was, in fact, sufficient.

- 1047: Nursing supervisor informed "we don't need reverse flow. We're assigning by unit for droplet and contact isolation," as per the Vice President for Medical Affairs;
- 1138: Infection Control manager here—confusion about whether patients need to be in negative flow versus contact and droplet isolation from ED staff/medical doctor (MD); Infection Control Manager leaves to go to Control Center to verify;
- 1140: Call from Control Center—"Dr. .... says we don't need reverse flow. We can do contact and droplet isolation" stated an ER Charge RN to staff/MDs in ED; and
- 2040: the Vice President for Medical Affairs clarified with ED staff/MD that reverse airflow isn't needed—contact and droplet isolation is sufficient.

e. Resources: masks, and Personal Protective Equipment

The recent outbreak of SARS has also generated a great deal more emphasis on the importance of respiratory protection for patients and about higher levels of Personal Protective Equipment (PPE) for hospital personnel who come in contact with them. For an outbreak of Pneumonic Plague, masks are likely to represent an important means for infection control. During the FSE, the following hospital personnel were identified as potentially vulnerable to infection and thus required some form of droplet protection: doctors, nurses, triage and front line ED staff, X-ray technicians, security, registrar, and volunteers.

Figure 19 provides a breakdown of the various types of PPE worn by hospital personnel as noted during the exercise. Each category indicates, at a minimum, that particular pieces of equipment were being worn. The category *PPE* does not specify any one piece of equipment; the observations in this category likely range from masks up to mask, gown, goggles, and gloves worn by the staff member(s) being observed.

Figure 20 provides a breakdown of the various types of personal protective equipment worn by the exercise patients as noted during the exercise. The same categories were used for this plot as for Figure 19.

Both graphs note small, but important percentages of persons who were not wearing any masks. For the hospital personnel it is likely that this six percent is somewhat of an overestimate, because some notations in the data indicate staff and some notations call out a single individual. The patient number is a more reliable figure, since patients were not grouped using a similar

staff-like term. Regardless, it is important that the numbers in this category, whether hospital staff or patients, are as few as possible.

N-95 masks

During the exercise, both N-95 masks and surgical masks were used for PPE. Some EDs started the exercise using surgical masks then switched over to N-95 masks as the outbreak progressed. Others used the N-95 masks, but required some amount of additional instructions to use. One hospital was observed as having had all their nurses fitted for N-95s. The hospital also had adequate supplies of these masks throughout the exercise. Another hospital commented that not enough sizes were available. Other hospitals ran out and had some difficulty re-stocking. In DuPage County, it ultimately fell to DuPage County's EOC to coordinate a re-supply of masks to their county hospitals.

Figure 19. Wearing of Protective Gear by Hospital Staff (Clean Up?)

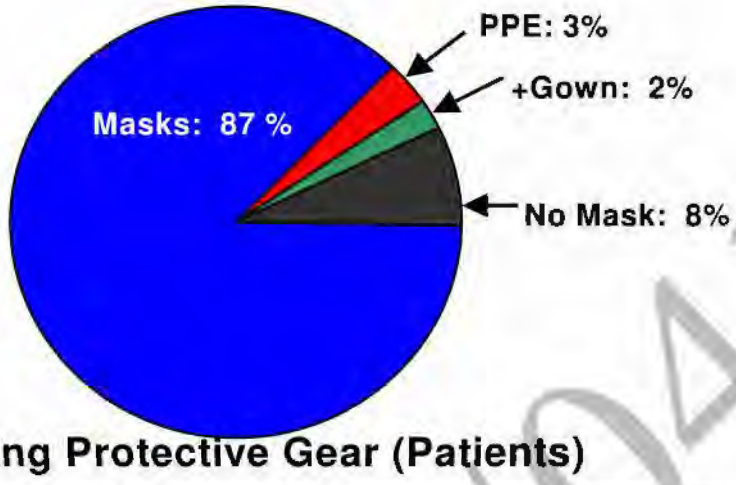


Figure 20. Wearing of Protective Gear (Exercise Patients)

f. Resources: handling of the dead

The FSE play included handling of the deceased and mortuary affairs. During the full five days of the exercise, 1,521 persons died as the result of the outbreak. Fewer exercise victims died during the three days of hospital play, but these casualties still stressed the morgue capacity for a number of participating hospitals. In fact, on the evening of May 13, 2003, three hospitals had reached their maximum morgue capacity.

Alternative morgues

A number of alternative morgue options were developed over the course of the exercise. These included other hospital sites (hospital garage, hospital barn, and a local ice rink) in addition to at least two different sizes of refrigerated trucks (truck capacity: 40 bodies; truck capacity: 108 bodies, based on exercise data).

These alternative morgues also required a morgue leader to set up and coordinate body storage and subsequent transport, as well as supplies such as body bags and duct tape. As part of this process, while such alternative morgues were being selected and established, temporary body storage was also provided for the hospital in the preliminary storage areas, which included:

- Increased stacking levels in the already full hospital morgue;
- Procedure Room;
- Urgent Care Area;
- ED; and
- Hazardous Materials Room

Some of these preliminary storage areas might have been refrigerated (one doctor ordered portable cooling units for this purpose) but the majority likely was not.

In DuPage County actual contact was made with the Union Pacific Railroad requesting refrigerated box cars to be used as temporary morgue facilities. Located immediately north of the county campus, the Union Pacific Railroad simulated the closing of a mainline track, and provided three refrigerated cars to expand the county's morgue capabilities.

Notifications/reporting of the dead

Deaths were counted and reported to the POD hospitals and then to IOHNO. This significantly increased the reporting requirements placed upon the hospitals. Along with a number of internal notifications, hospitals also sent this information to the County EOC, the County OEM, the Coroner, the Medical Examiner, the American Red Cross, the Funeral Director Association, and Funeral Homes (for the transport of non-infectious remains).

g. Antibiotics

Antibiotics were used as soon as the initial exercise patients arrived at hospitals. Figure 21 provides the percentage breakdown of antibiotics used to treat the patients throughout the three days of hospital play. The *Antibiotic* category includes all notations of *abx* in the data, where the data collector did not identify the specific prescription. The category *Other* consists of prescriptions of Chloramphenicol, Zithromax, and Amoxicillin, which were grouped for clarity. In addition to these prescriptions, eight percent of patients received two antibiotic prescriptions, primarily because medical personnel were suspicious of terrorism early in the exercise. Later in the exercise, two prescriptions were given because the centers for Disease Control and Prevention expressed concern that this strain of Pneumonic Plague may be resistant to traditional antibiotics.

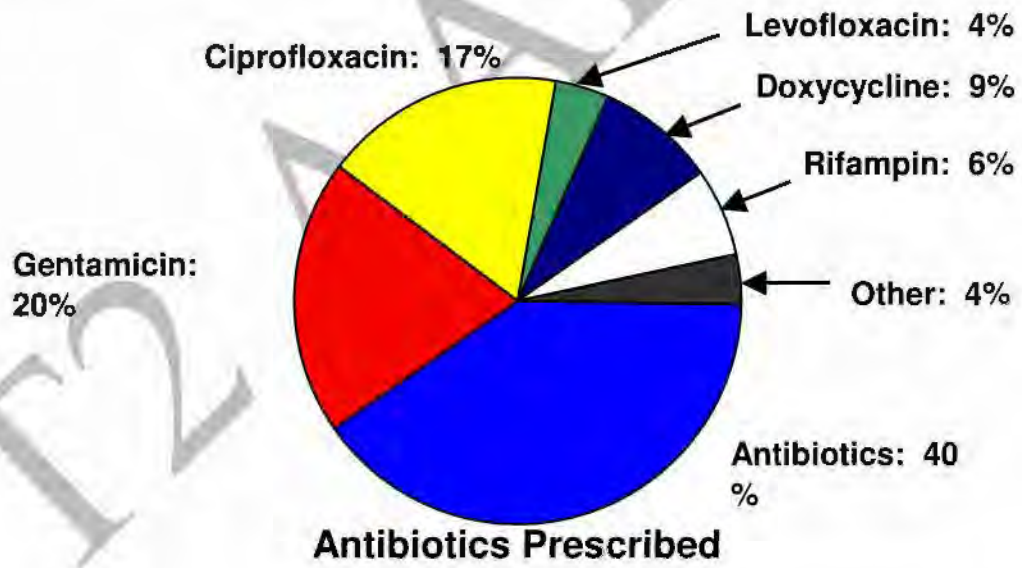


Figure 21. Antibiotics Prescribed during the Three Days of Hospital Play

In addition to both intravenous (IV) and oral antibiotics required for patients, hospitals provided either Ciprofloxacin or Doxycycline to their personnel once Pneumonic Plague was suspected and positively identified by IDPH. One hospital used Employee Health to manage the

distribution effort. Another hospital tasked Hospital Infection Control to determine the amounts of antibiotic supplies needed. A third tasked their Isolation Nurses with notifying the pool of personnel exposed prior to the discovery of the outbreak.

Per ED requests, hospital pharmacies determined the on-hand supplies of antibiotics for both patients and staff. For patients, stocks of the IV/oral supplies of Gentamicin, Streptomycin, Vancomycin, Ciprofloxacin, Levofloxacin, Chloramphenical and Doxycycline were checked. Pharmacies were also tasked with additional orders of Ciprofloxacin and Doxycycline. In addition, at least one pharmacy was tasked to call the EOC to request the activation of the county's stockpile of antibiotics.

h. Additional space requirements

In addition to the previously mentioned requirement for additional beds, isolation rooms, reverse pressure rooms, and increased morgue capacity, and other space was voiced during T2. These needs also included additional space to triage patients, space to enable the ER to be segregated by plague patients versus non-plague patients, and a separate site to handle the worried-well.

Hospitals utilized various spaces to meet the additional triage requirements, including break rooms, hallways, the entrance outside the ED, pediatrics ER, minor care, and the catheterization lab. For the worried-well, at least one option considered was the helicopter hanger. The Family Medical Center department of at least one hospital was used for segregating the ER.

i. Ventilators

Responding to a large outbreak of a severe respiratory disease will require the use of respiratory support for the most critically ill patients. As was true with the other resources examined in this reconstruction, ventilator supplies were also counted and their numbers provided to POD hospitals and then IOHNO. On the morning of May 14, 2003, IOHNO requested additional ventilators from the Vendor Managed Inventory of the Strategic National Stockpile. This request was based upon patient number projections, not upon the number of ventilators currently in use at the time. During actual hospital play, in fact, the supply of ventilators appeared to remain adequate. Only one of the seven hospitals, for which ventilator data were available, indicated a need for more ventilators early on the evening of May 13, 2003.

4. Artificialities

Several artificialities or artifacts of exercise play affected the analysis of hospital play:

- Multiple reporting chains, the plethora of patient statistics available (reports from the media, control injects, the hospitals, etc.), and the number people in the reporting chain all complicated patient reporting. In many cases, individuals were able to obtain patient statistics from sources not anticipated or known by exercise control. During an actual event, patient counts would be generated through the reporting, not from the interaction of the reporting chain with exercise control;
- In a real event the reporting system would be more complex, with requirements to report on the evolution of the patient population as well as the general statistics (affected, dead, etc.);

- The Metropolitan Chicago Health Care Council (MCHC) injected additional, unscripted, patients into the exercise during the early phases of the exercise. These patients were intended to assist MCHC hospitals maintain their accreditation. However, these patients were inadvertently configured to resemble T2 FSE scripted patients, resulting in a distortion in the numbers of patients reported; and
- During the FSE, some media play was scripted. This meant that in some instances the reported patient numbers were based upon exercise injects, not the actual numbers of patients reported to decision-makers. One example of this type of reporting occurred with the Office of the Governor of Illinois. Ground truth patient counts had been given to the Governor prior to the start of the exercise. Using these numbers the Governor taped several interviews or reports incorporating those numbers. However, when they were broadcast, the ground truth numbers were significantly different from the patient numbers held by the State and local governments and public health authorities.

5. Conclusions

During a crisis like the one simulated in the Illinois venue, communicating data and information is critical to developing an accurate and comprehensive picture of what is happening. Communications require both a robust transmission system and sufficiently trained personnel to ensure that the communications occur and that the results are verified, then passed to the appropriate locations within the receiving organization. T2 illustrated the diversity and complexity of managing response resources in the public health and medical environment. With 64 hospitals, five POD hospitals, and three separate but interrelated statewide organizations (IDPH, IOHNO, IL State EOC) all collecting data and attempting to coordinate actions, information and data flow requirements became intense.

SUMMARY OF CONCLUSIONS—
HOSPITAL PLAY IN THE ILLINOIS VENUE:

The T2 FSE exercised 64 hospitals in the Illinois venue making it one of the largest mass casualty exercise ever undertaken.

Hospitals still rely on telephones and faxes for data transmission vice electronic transmission. This manifested itself as a significant challenge during the FSE due to mechanical problems, inadequate staffing, and loss of data.

Hospitals should consider implementing a system in which data is entered digitally then transmitted electronically. This would eliminate many of the manual steps observed during the FSE and has the potential to minimize errors.

Because of the dual communications chains that exist, there is a need for organizations to coordinate the receipt and processing of information.

Hospitals and public health departments generally do not have the experience or the extra staff trained to handle large volumes of emergency communications. While personnel may be trained to operate particular fax or voice circuits, the existing infrastructure may not be adequate to sustain robust communications during a crisis of the type simulated during T2. Thus, as was the case in this exercise, problems develop when the system is activated.

During the FSE, the lack of a robust emergency communications infrastructure was manifest by a reliance on telephones and faxes for data transmission versus electronic transmission of data. It was also manifest in the loss of fax machines due to mechanical breakdown, inadequate staff to monitor them, or loss due to after-hour rooms that were locked. Likewise the lack of verified phone numbers for communications caused delays while emergency personnel looked for the correct numbers to report emergency data.

At the most basic level, it is possible to establish some principles for developing an effective emergency data communications system, which is essentially what was occurring as the hospitals reported syndromic, patient, and infrastructure information:

- Communications need to be robust and verifiable. It is critical that communications are being directed to the correct personnel or organizations (i.e., e-mail or telephone numbers must be correct) and that the receiving organizations received the right information. A record of the transmission is also required;
- Data should ideally be communicated over data lines, not voice or fax. Voice systems are good for person-to-person coordination (not necessarily organization to organization coordination), but neither voice nor fax are optimal ways to communicate numerical data. Using data communication techniques (e.g., e-mail, Internet transmission) leaves the data in machine-readable formats upon receipt;
- After they are generated, as few human hands as possible should touch data to minimize errors. For example, if information is copied down manually on a form, then the form is faxed (possibly degrading its readability) to a collection point, where it is then manually tabulated on another form, as is consistent with the IDPH emergency plan, and then entered into an information system for transmission, the potential for errors increases significantly; and
- Whether using data lines, voice, or fax, care must be made to ensure the security of the information being transmitted.

One way to overcome difficulties in the collection and reporting of data is to have data entered digitally at the point of origin, then transmitted electronically in digital form to all those who require the data. This would eliminate many of the manual steps currently involved in data generation at the hospital level, and provide for a more robust and verifiable set of data once it was received by one of the POD hospitals and IOHNO.

A larger issue, that was more difficult to document, was the movement of information within organizations once the information was obtained. The dual communications chain observed in the FSE, with the IDPH Infectious Disease Control receiving reports from local public health and IOHNO receiving reports from emergency departments at hospitals, is an example of the need for coordination within organizations for the receipt and processing of information.

The FSE resource requirements illustrated both the diversity of resource types required to respond to thousands of sick, dying, and dead, as well as the diversity of organizations looking for and providing resources. With 64 hospitals all looking for essentially the same set of resources, a wide range of potential solutions were developed to address the problem.

However, without adequate resource tracking it will be impossible to effectively allocate, expand, or acquire resources that address specific needs. Instead a general diffuse and untargeted effort to acquire resources will evolve as a result.

This page intentionally left blank

G. Decision-making under Conditions of Uncertainty: The Plague Outbreak in the Illinois Venue

1. Introduction

During a disease outbreak, whether naturally occurring or initiated through an act of terrorism, decision-makers must rely upon scientists, medical doctors, and the public health system for the information needed to make effective response decisions. Examples of such information include the progress of the disease, the behavior of the disease in various populations, and assessments of how the disease might be spreading. Often the early science on these questions is ambiguous or, in the case of historical diseases, open to various interpretations.[99]

Decision-makers must work to formulate the right questions, and then interpret the answers within the context of the logistical, political, social, public health, and economic aspects of the response. This is difficult under the best of conditions, and made even more difficult during a terrorism response operation due to the enormous media and time pressures that decision-makers will he operating under.

The Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE) provided a unique environment that can be used to examine decision-making under conditions of information uncertainty. During the FSE, public health officials initially knew neither the extent nor duration of the terrorist-induced epidemic of Pneumonic Plague. These facts permit an examination of several questions related to decision-making under uncertainty, such as:

- How was the extent of the epidemic estimated;
- What were the estimates;
- What techniques were used to provide these estimates; and
- Did these estimates subsequently affect decisions (requests for resources, other teams, and capabilities)?

This *Special Topic* examines these questions in the context of events that occurred Illinois venue during the FSE. During the early phases of the exercise, participants were only seeing the tip of the iceberg in terms of the eventual numbers of patients that would develop. How they oriented themselves to the evolution of the disease and what impact that had on planning were aspects of the exercise in which science and policy-making interacted.

2. Background Pneumonic Plague

a. Defining the information iceberg problem

During the FSE, a simulated outbreak of Pneumonic Plague occurred in the Chicago metropolitan area. To illustrate the challenge of estimating the long-term consequences of the outbreak, the plot graph in Figure 22 shows the T2 scenario's patient population hroken down into five potential pools: Not symptomatic, mildly ill, severely ill but not in a hospital, severely ill and in a hospital, and dead.

[99] Science: P. Anand; "Decision-making when Science is ambiguous" 8 March 2002, Volume 295, page 1839.

The plot shows the number of cases of Pneumonic Plague increasing along the negative y-axis, with time increasing along the positive x-axis. The figure is constructed this way to simulate a metaphorical iceberg, with x = 0 symbolizing the waterline. As the days of play continue from May 11 through May 14, 2003, only small fluctuations are seen in the number of persons diagnosed with plague. However, after May 14, 2003, the number of cases increases dramatically from less than 1,000 to more than 20,000.

This is termed the *information iceberg*, as the early presentation of the disease does not really foreshadow the potential size of the epidemic. The patients who present symptoms early in the epidemic are seen as the tip of the iceberg with their numbers appearing above the waterline, as they bring themselves into the hospitals for assessment and subsequent treatment. The remaining pool of patients remains under the waterline of the iceberg, where the graph ends on the last day of the exercise.

Understanding and successfully predicting the effect of the iceberg is critical to decision-makers. During the early stages of an outbreak, decision-makers are likely to see reports about only the early presenters, not the full number of exposed persons. It is absolutely critical to determine rapidly the scale of the outbreak. This is especially true in cases of potential bioterrorism where traditional epidemiological curves could be multiplied by multiple, continuing, or widespread initial exposures.

Public health officials, and other decision-makers, may determine the scope of the problem by employing epidemiological models based upon data reported by physicians, hospitals, and the public health infrastructure, as well as developing a clear understanding of the nature and transmission mechanisms of the disease; but they must also factor in additional assumptions in the case of bioterrorism.

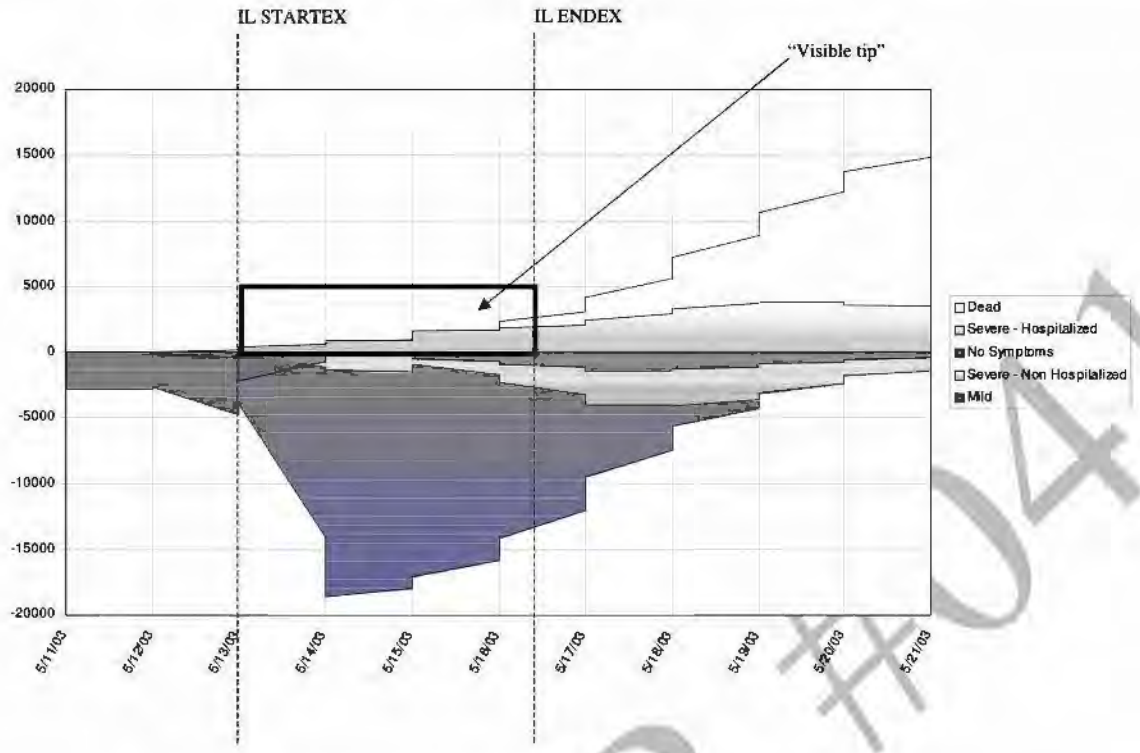


Figure 22. The Iceberg of Patient Population

b. Decisions using estimates and models

How do epidemiologists estimate the size and behavior of the disease

A common approach for approximating these elements is to use models to estimate the progress of the disease. However, incorrect, incomplete, or inaccurate data or assumptions and information input to a good model can result in sub-optimal results for decision-makers. It is important for decision-makers to understand that even with good data, models are only an approximation of reality. In the case of a disease outbreak, data on the disease does not appear instantaneously at exactly the right time for decision-making. Instead it may be delayed and may contain inaccuracies. Mechanisms may not be in place to collect the right data in a timely fashion. Finally, the models themselves are approximations of the actual process by which diseases spread. It is also important to note that models are even less reliable when dealing with diseases like plague, particularly Pneumonic Plague for which there is a paucity of data. Additional complications occur with diseases that are deliberately introduced and optimized by terrorists to achieve high mortality and morbidity.

The estimates that models provide may well change over time as more data become available. A number of T2 After Action Conference (AAC) participants indicated "neither decision-makers nor the American public understands models and, in particular, won't accept the fact that the answers keep changing." Continuous changes in estimates can be disconcerting to decision-makers, and the general public.

c. T2 Chicago venue scenario and patient breakdown

The FSE Illinois patient population consisted of an initial group of 3,100 individuals exposed to Pneumonic Plague. This group would ultimately infect an additional secondary population of 18,434 persons. When exercise brevity (five days) is compared with the designed epidemic length (eleven days, from original exposure to D+9), the impacts of the 21,534 affected individuals were not fully explored.

The affected population design was initially divided into five separate categories: Not symptomatic, mildly ill, severely ill but not in a hospital, severely ill and in a hospital, and dead. Subsequent changes to this original design were accomplished in consultation with Illinois Department of Public Health (IDPH). These changes were designed to provide a reasonable representation of the responses individuals would have to becoming ill with Pneumonic Plague. The additional breakdown laid out twelve separate tracks that determined when the patients would arrive at hospitals, or if individual patients would avoid hospitals and seek medical care elsewhere or not at all. The breakout of these tracks is provided in Figure 23, which is color-coded to indicate those patients who would be captured as part of normal hospital reporting protocols. The red script indicates those infected individuals who would remain largely uncounted by the hospital system playing in the exercise but who would eventually require care nonetheless.

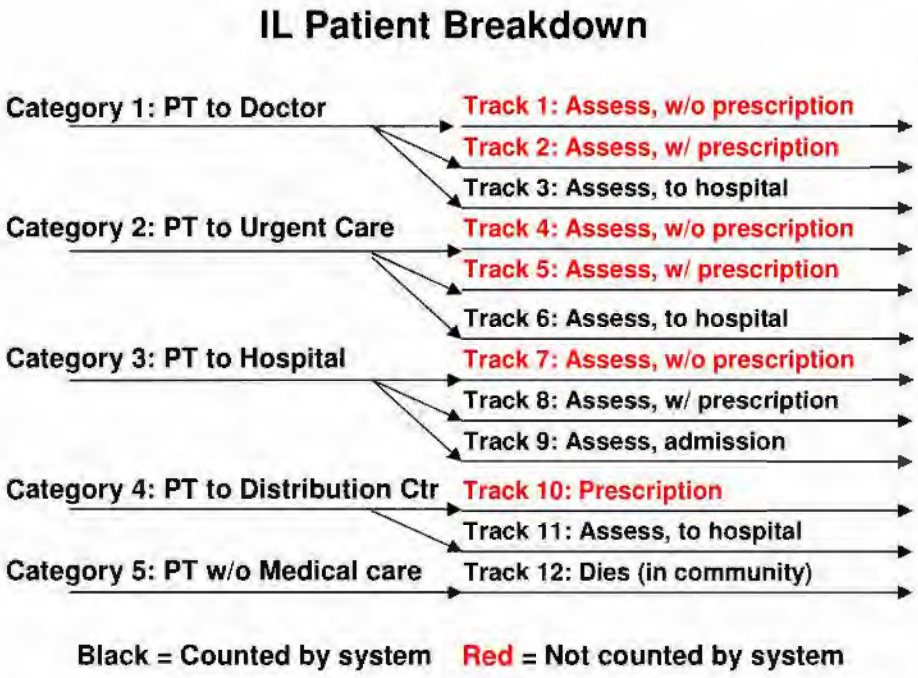


Figure 23. Illinois Patient Breakdown

Figure 24 summarizes the number of victims who were infected (both the primary and secondary exposures) and those who would be so severely ill as to require hospital treatment for the days of the exercise.

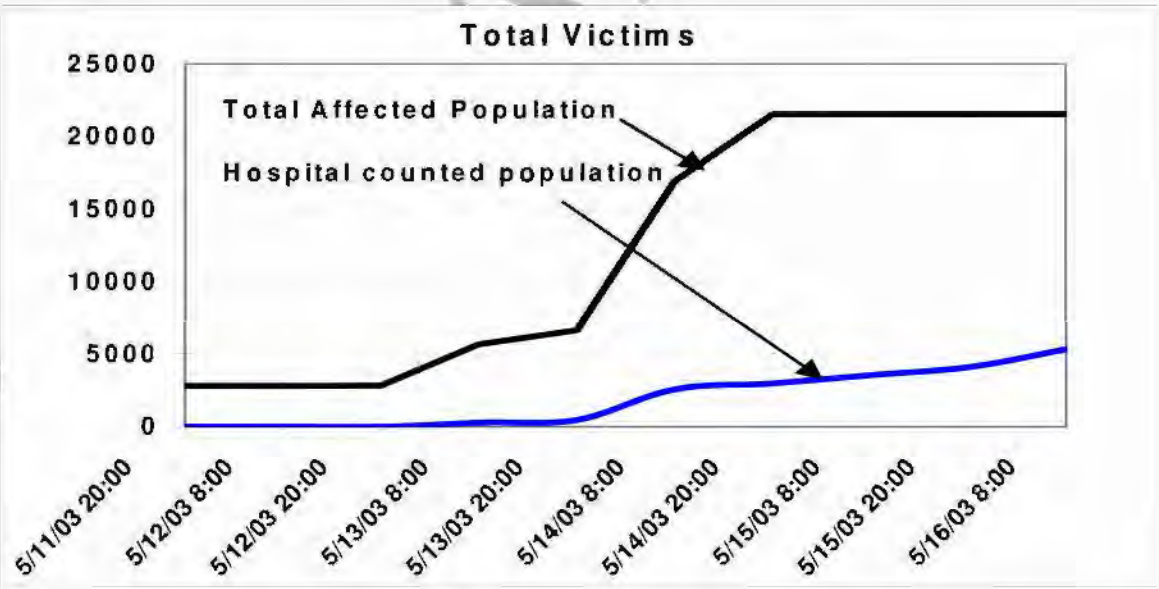


Figure 24. Total Exposed Population Compared With the Hospital-Counted Victims (All times Central Daylight Time (CDT))

3. Reconstruction (all times CDT)

a. How accurate was the data reported by hospitals

Patient counts reported by hospitals and physicians were lost during the exercise for a number of reasons. Patients may not have been counted because they did not report to hospitals or because the counts were corrupted somewhere along the way. This section discusses how information was lost to epidemiological modelers, public health officials, and other decision-makers during the exercise.

The data used to estimate the epidemic spread during the FSE suffered from three problems:

- Some data were simply not observed at the point of origin;
- If the data were observed, they may not have been reported accurately. For example, an accurate count of patients was incorrectly entered into a data reporting system; and
- The data may have been incorrectly defined. Even with accurate numbers, not all of the patients were placed in the correct category.

Figure 24 illustrates the problem of unavailable data: Some patients were not entered into any data system. These patients could not be added to any hospital patient counts because they either never went to a hospital or they were released upon assessment in the Emergency Department (ED) and not counted.

Table 8 summarizes the percent of victims who were eventually seen at hospitals but who remained out in the community until they received treatment at hospitals or from their doctors, or died from the disease. At the end of the exercise, approximately seventy-five percent of the exposed population remained unseen because they had not yet become more than mildly symptomatic.

Table 8. Percent of Infected Population Seen in Hospitals by Exercise Date/Time

TIME	TOTAL SEEN	TOTAL INFECTED	%
13 May 0800	283	5656	5
13 May 2000	460	6634	6.9
14 May 0800	2566	16885	15.2
14 May 2000	2977	21534	13.8
15 May 0800	3546	21534	16.5
15 May 2000	4084	21534	19.0
16 May 0800	5322	21534	24.7

Inaccurately reported data can be detected by comparing patient numbers reported and logged at the Illinois Venue Control Cell (VCC) with the ground truth scenario patient population. The patient data for the 1700 - 2400 timeframe on May 12, 2003,[100] is provided in Table 9. The numbers vary considerably from the ground truth, depending upon which source is consulted

[100] This is the time period during the exercise where the Metropolitan Chicago Health Care Council did not inject additional patients into the patient population.

(both hospital patient numbers and public health numbers were logged on VCC wall charts and the VCC controller log has also been reviewed).

As can be seen in Table 9, none of the logs of patient counts maintained by the VCC agreed completely with the ground truth patient numbers from the scenario. This may be the result of the complex way in which patient data was exchanged. Communications took place over fax, landlines, and cell phones. This led to a number of ways to log the data as well as a variety of different people reporting the data. Variance in the reporting source and the method of reporting probably represents part of the reason why patient counts vary.

It is also important to note that the 1700 - 2400 timeframe on May 12, 2003, represents data from the earliest part of the exercise. After this time, patient numbers climbed considerably. If reporting wasn't accurate early on, during a low volume of patients, it might be expected to lag behind actual counts under the more stressful conditions of higher patient volumes. Unfortunately, due to the problems encountered with patient numbers later in the exercise, it was not possible to determine whether the variance in patient counts actually increased as the exercise progressed.

Table 9. Reported Patient Numbers Logged at VCC as Compared to Actual Scenario Numbers (May 12, 1700 - 2400)

City/ County	Hospital Patients (Ground Truth)	Hospital Patients Logged: VCC Chart	Hospital Patients Logged: VCC Log	Public Health (Ground Truth)	Public Health Logged: VCC Chart	Hospital Deaths (Ground Truth)	Deaths Logged: VCC Chart
Chicago	**22**	**11**	**9**	**10**	**5**	**0**	**0**
Cook	**38**	**26**	**15**	**29**	**26**	**2**	**0**
DuPage	**19**	**0**	**5**	**16**	**5**	**1**	**0**
Kane	**10**	**6**	**0**	**9**	**6**	**0**	**0**
Lake	**13**	**0**	**0**	**12**	**0**	**1**	**0**
TOTALS	**102**	**43**	**29**	**76**	**42**	**4**	**0**

Another reason why the counts in Table 9 do not match is that the definitions of what was being reported do not necessarily match. As noted earlier, the ground truth scenario divided the patients into pools of those who would visit the emergency department (ED), those would subsequently be admitted, those patients sent to the emergency room by their doctor or by

another medical facility, and the dead. These specific definitions, however, were not adhered to by reporting hospital personnel and resulted in patient reports that, while counted in the totals, would not have accurately reflected the scenario.

b. Estimating the course and scale of the epidemic

During the FSE, participants used a number of approaches to produce estimates of the Pneumonic Plague epidemic. The results of these efforts helped determine strategies for antibiotic distribution, the need for additional antibiotics from the Vendor Managed Inventory, and the need to identify additional sites for patient treatment and handling of the dead. It should be noted that in the case of a terrorism attack, the progress of the disease would likely exceed that which would be encountered in a natural outbreak, suggesting that decision-making would need to be guided by a broader understanding of the threat environment.

The following sections describe several of the different approaches that were used to estimate the affected population during the FSE. These approaches are compared to the ground truth numbers for patient counts in the scenario, not for the purposes of critiquing them, but to indicate the ways organizations approached these types of problems.

Example 1 (Patient estimate). Illinois Operational Headquarters and Notification Office

Based upon the reported patient numbers at 1600 on May 13, 2003, (338 cases, 154 dead)[101], Illinois Operational Headquarters and Notification Office (IOHNO) personnel used a simple approach to estimate the numbers that might be presented to their hospitals over the next few days of the exercise. They chose a multiplicative factor (initially 5-6). This factor was a means to estimate how many additional cases each initial case could produce. This resulted in an estimate of 2,000 cases with 1,000 dead for a total of roughly 3,000 affected persons. The multiplicative factor was almost immediately doubled, producing estimates of 4,000 cases with 2,000 dead, for a total of 6,000 affected individuals.

The factor was doubled because IOHNO felt that the patient numbers were being significantly underreported. It is interesting to note that this rough estimate was within fifteen percent of the final actual total patient population at 1200 on May 16, 2003, (5,349 cases, 1,521 dead, total of 6,870), which overestimated the dead and underestimated the survivors.

Because the State of Illinois has a total of 8,263 beds statewide, some of which would be not be used for plague patients, this IOHNO estimate suggested that hospital facilities would be severely strained by downstream patient numbers. More significantly, this estimate was used to request two Disaster Medical Assistance Teams and one Disaster Mortuary Operational Response Team. IOHNO's approach depended heavily upon the expertise of those making the estimates.

[101] Note that this is out of the range of the May 12, 2003, data presented in Table 9. However, as was argued in the previous section, inaccurate early data counts are likely indicators of inaccurate counts throughout the exercise period. Thus, it is likely that these initial numbers, and all those quoted in these examples, differ from ground truth by an unknown but significant amount.

Example 2 (Patient estimate). Data obtained from the Chicago-area FEMA Regional Operations Center

Data from the Chicago-area FEMA Regional Operations Center (ROC) indicated that an estimate of the epidemic was provided during a briefing on May 16, 2003. The graph shown in Figure 25 is a copy of the graph used in the ROC. The numbers used were those reported by the IDPH.

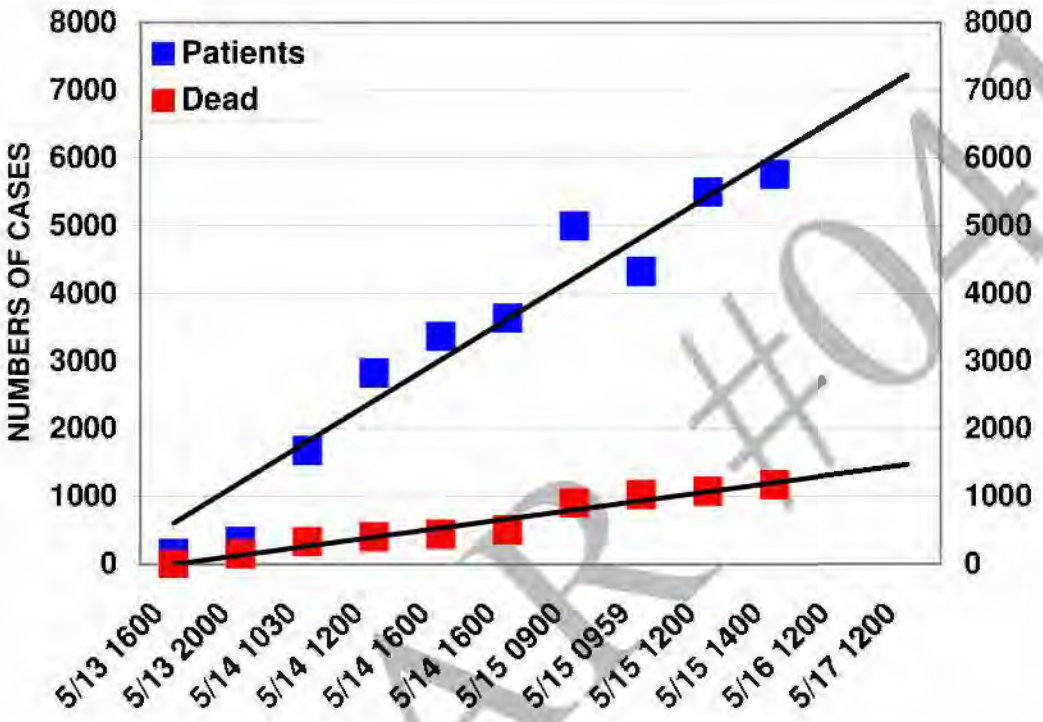


Figure 25. Chicago-area FEMA ROC Patient and Dead Estimates A significant problem is apparent from an examination of this graph. The data on the x-time axis are plotted at equal intervals. However, the actual time intervals on the plot are not equal even though they are portrayed that way. As a result, the straight line fit through the data is incorrect. Once the data are correctly plotted with respect to time (see figure 26), they are more correctly seen as clustered groups of data, not equally spaced in time.

The plot in Figure 26 indicates a patient population of 8,200 at 1200 on May 16, 2003, that would increase to 11,000 persons on May 17, 2003, (compared to 7,200 in the previous figure). Similarly, the estimates of the dead, 1,700 increasing to 2,200 on May 17, 2003, are significantly different than the original estimates shown in figure 25. In fact, if the estimates in figure 25 had been used, they would have underestimated both the patients and dead by approximately fifty percent for May 17, 2003, the day following the conclusion of the exercise. While this approach overestimates the number of sick and dead patients compared to ground truth at 1200 on May 16, 2003, it does give a better sense of the developing scale of the outbreak that would have become apparent if the exercise had continued passed May 16, 2003.

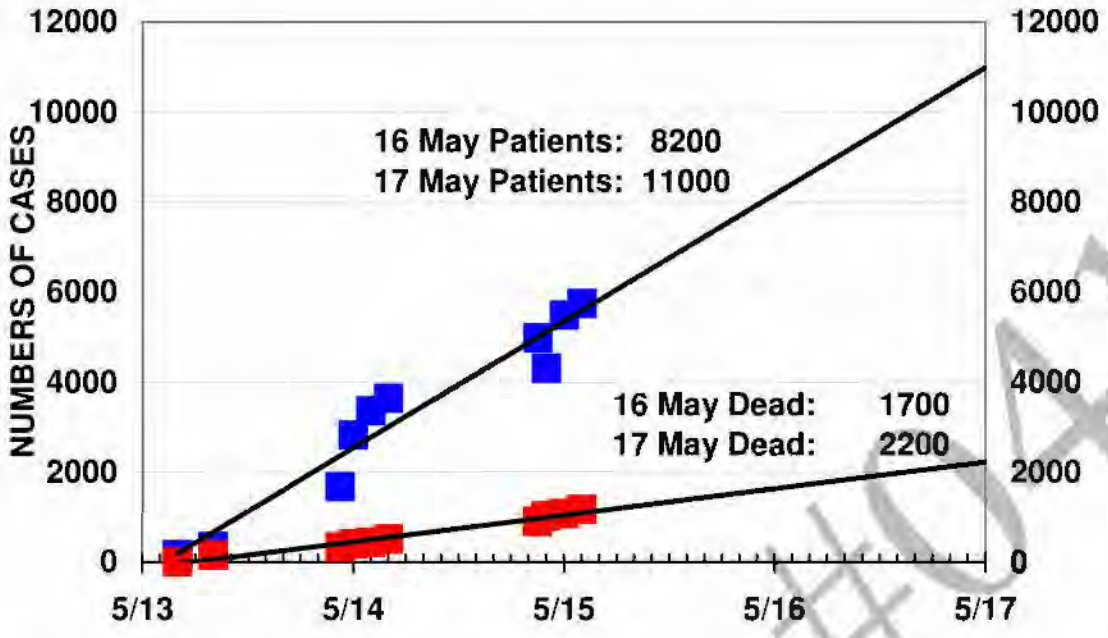


Figure 26. Correct Plot of Patient Numbers and Dead Numbers Versus Time

Example 3. DuPage County Emergency operations Center

The DuPage County Emergency Operations Center (EOC) called in a Geographic Information Systems (GIS) analyst to help estimate the number of DuPage County citizens who could have been at each of the three release sites in the Chicago area. The EOC suggested that this information could provide some indicators of which Strategic National Stockpile (SNS) distribution sites (located around the county) might be busiest and which hospitals might be seeing more patients. The first set of estimates was based upon raw numbers of people from specific areas of the county who were at the United Center during the Saturday night game. The GIS analyst got this information from the United Center ticket box office based upon zip codes. Next, the analyst collected data for the numbers of county resident who ride the single train line coming out of Union Station that passes through DuPage County. The analyst used the average Saturday traffic on that line and counted the number of people who got off at each station in the county.

DuPage County accounted for one percent of the people who attended the hockey game and for fifty-two percent of the people who left Union Station via the train line. Estimates of DuPage County–O'Hare traffic were not developed because of limited time and the greater number of variables. An estimated seventeen percent of the total people infected at the first two sites were from DuPage County. Following his presentation to the EOC, the DuPage County Office of Emergency Management said that while GIS is not usually tapped in an emergency response, that would have to change based upon how seemingly valuable their skills and data could be.

The final report by the DuPage count analyst discussed the methods and results and is quoted here in full:

> *During the exercise, it came to light that the State of Illinois pharmaceutical supply was limited, and we needed to identify the approximate number of DuPage County residents exposed to the biological releases and what portion of the county they reside.*
>
> *There were three biological releases in the City of Chicago; Union Station (released 8:00 am, United Center (during a Blackhawk's playoff game), and O'Hare International Airport (International wing)*
>
> *For the Union Station data collected we asked Metra to provide us with train ridership information on the Burlington Northern Line for the total trips leaving Union Station to DuPage County on an average Saturday. Metra provided the totals as well as the breakdown per train station in DuPage County. The Burlington Northern Line is also the only commuter line in DuPage County that leaves from Union Station.*
>
> *The United Center data was provided by the Blackhawk's Director of Ticket Operations. The data reflected the last game of the season, a month prior to TopOff2, and was a sold out event. This event would provide us with the most accurate information we could have hoped possible. The attendance count was provided to us for each zip code contained in DuPage County.*
>
> *Information was not available for O'Hare International Airport in the time frame available.*
>
> *These numbers were tabulated and mapped out displaying the concentrations of potentially infected residents.*
>
> *These estimates were calculated to provide the State of Illinois with a percentage of potentially infected residents so DuPage County would receive the bare minimum amount of pharmaceuticals from the underestimated Illinois stockpile.*
>
> *The data gathered here reflects DuPage County residents only. Intended to provide rough estimates for pharmaceutical acquisition, and to provide a general overview of the concentrated areas in DuPage County. For an actual statistical analysis, this information would have been passed along to an epidemiologist for rate of spread calculations and probability modeling. A 3 hour window was given for data collection, tabulation, and display.*

Given the parameters analyzed—the final estimate of the total exposed population, of which nineteen percent would have been DuPage County residents—was 25,706 persons. The actual scenario numbers totaled 21,534 persons, 3,100 in the initial population and 18,434 in the secondary population. The advantage to this approach was that it avoided all the significant problems in the patient population data and, in addition, provided an estimate not based upon projections, merely on normal use data—which is likely to be a better data set, unaffected by either exercise play or unannounced real-world attacks.

Other efforts

In addition to the efforts described above, two other efforts were identified that attempted to model the epidemic spread. There were also isolated events where decision-makers attempted to deal with the uncertainty involved in the response. This section covers all of these isolated events.

Statements were made at the T2 AAC that indicated the Illinois Crisis Action Team (IL-CAT) modeled the epidemic. Further information about the results of this modeling is not available, as the data collectors in the Joint Operations Center did not capture it.

The Centers for Disease Control and Prevention (CDC) apparently also estimated the scope of the epidemic on the second or third day of the exercise. At the AAC, it was reported that the CDC modeled the epidemic using the number of reported cases (from IDPH), the known incubation period (two to seven days, normally two to three days), and a rate of transmission of three secondary cases per primary case. In actuality, the rate of transmission used in the scenario depended upon the site of exposure: seven secondary cases per primary case at the United Center and eight secondary cases per primary case at Union Station and O'Hare International Airport.

Unfortunately additional data were unavailable to the evaluation team other than what was discussed at the AAC. Thus at the time of preparation of this draft report, there is no indication about the methods used, the results obtained, or whether decisions were made based upon the information. The report indicated, however, that the resulting predictions were within approximately ten percent of the final patient numbers.

In addition to modeling the epidemic outbreak, other estimates were made by officials. These "back of the envelope" calculations were important in several decisions, particularly for decisions regarding resource allocation.

At 0915 on May 14, 2003, the Chicago DPH determined that the SNS would be distributed according to the city's and county's population. The initial planned distributions were: Chicago–12,400 doses; Cook–12,500 doses (6,250 Doxycycline, 6,250 Ciprofloxacin); DuPage–10,100; Lake–6,000; Kane–4,400.

The reason that public health officials decided to distribute according to population, versus actual number of cases, was they lacked confidence in the accuracy of the number of cases being reported. Likewise they did not have a clear understanding of how many patients would ultimately be affected in each county. They did, however, know how many potentially affected persons lived in each county and saw that as a way to estimate the vulnerable population versus the infected or exposed population.

On May 14, 2003, Cook County DPH needed to know how many persons working at hospitals in Cook County would need prophylaxis. Instead of attempting to determine the potentially exposed population at each of the 22 county hospitals, Cook County DPH simply took the two largest Cook County hospitals, averaged the number of persons who would need prophylaxis, and then applied these numbers to the rest of the 22 hospitals. This over-estimated the need for prophylaxis, but resulted in a quick answer that would allow the prophylaxis to be distributed.

4. Artificialities

Several artificialities affected the analysis of this subject:

- The Metropolitan Chicago Health Care Council injected additional, unscripted, patients during the early phases of the exercise. These patients were intended to assist hospital accreditation. However, they were inadvertently configured to resemble T2 scripted patients, resulting in a distortion in the numbers of patients being reported. Because these patient numbers were not recorded, it complicates an understanding of how patient counts and epidemiological models played into the scenario; and
- During the exercise some media play was scripted. This meant that some patient numbers were reported based upon exercise injects, not the actual numbers of patients being reported to decision-makers. One example of this type of reporting occurred with the Office of the Governor of Illinois. Ground truth patient counts had been given to the Governor prior to the start of the exercise due to an exercise artificiality necessitating the pre-taping of top official statements. Using these numbers, the Governor taped several interviews or reports incorporating those numbers. However, when they were broadcast, the ground truth numbers were significantly different from the patient numbers held by the State and local governments and public health authorities.

5. Analysis

During the FSE there was significant uncertainty in the patient numbers. Indeed some of the artificialities discussed in the previous section may have increased the uncertainty. While the artificialities were unrealistic, the chaotic and uncertain environment they produced was realistic.

Decision-makers and those attempting to estimate the exposed population reacted in a variety of ways to the problem of uncertainty in the patient numbers. The methods used by the DuPage County GIS analyst attempted to resolve the fundamental conflict they were facing which was that the patient data were potentially inaccurate but that they needed accurate predictions of the number of infected persons in the county. By knowing the day, time, and place of the release and combining this information with demographic, economic, medical, and law enforcement data, the analyst was able to make a reasonably accurate estimate without knowing the detailed progression of the actual cases of the disease. Participants who chose to use the actual numbers of reported cases could be said to be ignoring the uncertainty inherent in the data. Even if they knew that the data were suspect, they still used them, as there was no other apparent alternative. In these examples, reported caseloads were used in various approaches to develop an estimate of how many patients would need treatment.

Finally, some participants focused on other measures in order to move decisions forward. For example, the Chicago DPH decision-makers lacked confidence in both the data they were receiving and their ability to use the data to predict how to allocate resources. Instead they focused their decision upon the vulnerable population, instead of focusing on the infected or exposed populations.

6. Conclusions

This section provides three sets of observations and conclusions: 1) one relating to uncertainty and how participants dealt with it, 2) the information iceberg problem, and 3) a more general set of observations of how epidemiology played in the various EOC operations.

SUMMARY OF CONCLUSIONS—DECISION-MAKING:

The extent of the affected population will always be uncertain in a bioterrorism incident. Public health officials and decision-makers use epidemiological models, informed by the threat environment, to help determine the scope of the problem.

During the FSE, few attempts were made to understand the affected population. ***The DuPage County GIS analysis was the only documented effort that examined how large the problem might be.***

To alleviate some of the inherent uncertainty, model predictions and patient data should be coordinated among agencies and across jurisdictions. In addition, data collection should be better executed than was observed during the FSE.

By finding data, systems, and methods that allowed them to work around the uncertainty, some officials were able to make more informed decisions.

a. Uncertainty

From the preceding reconstruction, the following was observed:

- Uncertainty in the patient population numbers existed during the FSE. Most of this uncertainty was due to exercise artificialities, but it is not clear that during a real event the magnitude of the uncertainty would be less, even if the causes were different; and
- It is not the fact of uncertainty that affected exercise decision-making but how participants dealt with the uncertainty. By finding data, systems, and methods that allowed them to work around the problems with patient reporting data, some participants were able to deal with the uncertainty and make informed decisions.

b. The information iceberg

There were apparently few attempts to understand the long-range patient load. It is unclear why so few attempts were made. Two possible reasons include:

- Lack of long-term exercise play. Participants may have simply ignored what they did not need to worry about; and
- Lack of confidence in the patient data, and no clear way to model the long-term effects in the face of poor patient data.

The last reason may be the most important for developing a general lesson learned about the iceberg problem. The DuPage County GIS analysis was the only documented effort that examined how large the problem might be. This analysis was not accomplished using patient data but rather relied on an estimate of the number of people who might be exposed in the county.

Finally, decision-makers should be knowledgeable of the information iceberg problem for contagious diseases such as plague and especially in cases of potential bioterrorism. It is important for them to expect it, look for it, and question their advisors when it is not brought to their attention.

c. Other issues

These is a set of observations that arose from the work discussed here, but do not relate to either the problem of uncertainty or the epidemic profile.

Information sharing

Once model predictions and patient data are acquired they should be shared with everyone involved in the operation. In fact, information about some modeling efforts was only shared among all the participants during the AAC. There is no evidence that any of the results of these models were provided to other operations centers during the FSE.

The DuPage County EOC felt it would have benefited from model predictions by using them to predict the requirements for and deployment of ambulances throughout the county. A senior DuPage County EOC watch-stander noted (speaking to a member of the Illinois CAT during the AAC), "Why didn't I know that those predictions were available?"

Data collection.

One way to reduce uncertainty and improve the overall fidelity of the data is to do a better job of collecting it. There are systems available, such as the State of Illinois' Phase I and Phase II disaster reporting system, which could he used to collect patient data as well. This system collects bed counts, ventilators, blood supplies, among other supplies, during a disaster. However, the accurate collection of even the existing data requires considerable numbers of personnel, personnel that may not be available during an emergency.

This page intentionally left blank

H. Balancing the Safety of First Responders and the Rescue of Victims

1. Introduction

Historically, first responder rescue agencies have demonstrated high competency and experiential knowledge in managing traditional rescue situations: natural disasters, fires, and technical rescue challenges. In the hazardous materials (HAZMAT) environment, hazard identification is assisted by placard systems, knowledge of shipping contents, pre-planning at fixed facilities, and field-testing processes to identify common hazardous substances. In such incidents when victim survival is dependent upon timeliness of medical treatment (referred to as the *golden hour*), first responders are typically attempt to initiate rescue and removal of victims as rapidly as possible, while Incident Commanders manage responder safety with an ongoing risk-benefit analysis.

However, when faced with a potential weapons of mass destruction (WMD) emergency, first responders encounter a greater risk of becoming casualties themselves. For example, in Top Officials (TOPOFF) 2000, the first responders to arrive after the explosion in Portsmouth, New Hampshire, were incapacitated by a persistent chemical agent used in the attack. During the 9/11 World Trade Center attack, many New York City police and fire fighters died when the towers collapsed. In addition, first responders may be faced with delayed identification of toxic substances, the potential existence of secondary explosive devices, and other unknowns. Under these conditions of additional danger and uncertainty, consideration of risks and benefits in the development of action plans becomes more challenging. If victims are in immediate need of rescue, the initial action plan may reflect best guess/best practices information, placing responders in a rescue mode. However, as more information becomes available, plans can change and rescue operations may come to a halt. This is the scenario that was observed at the Seattle radiological dispersal device (RDD) site during the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE).

During the FSE, a number of public health officials and data collectors at the incident site, many of whom were subject matter experts (SMEs), expressed concern about the time it took to triage, treat, and transport victims. Commentators on the Virtual News Network (VNN) also raised this concern. Given the uncertainty surrounding the explosion, particularly when many of the responders artificially had the knowledge that it was a radiological incident, the Incident Commander had to take precautions to ensure that the responders were safe. This *Special Topic* focuses on the issues surrounding the balance of responder safety and victim rescue.

2. Background

a. Interagency communication

In large-scale incidents and exercises, communication between agencies is typically the largest command and control challenge. Command decision-making and development of an integrated

incident action plan are enhanced by effective communication links between the various agencies on the ground. The ability of a local Incident Commander to use information (e.g., radiation exposure levels, plume modeling, and toxic agent identification) provided by State and Federal responders depends on rapid and effective communication. With more detailed information, the incident action plan and the related risk-benefit analysis evolves with increasingly greater accuracy.

During the 9/11 terrorist attack on the Pentagon, the Arlington County (Virginia) Fire Chief managed his resources on the scene with a number of local and Federal agencies. He stated, "They [the other agencies] understood their role, which was to help the fire department move the incident through its various phases."[102] Avoiding duplication of effort, the Arlington County Fire Chief put the Federal responders to work assisting the Fire Department. For example, he used Federal resources to set up chain-link fencing and scene security in order to isolate the scene. These types of decisions allowed local and Federal agencies to work together and solve incident problems rapidly. He also stated, "Having a relationship with key officials prior to the incident does make a difference. We worked regularly with our military personnel, our Federal Bureau of Investigation (FBI) and Federal Emergency Management Agency (FEMA) personnel. You have to work on those relationships before the incident, not during the incident."[103]

b. Risk-benefit analysis

The use of risk-benefit analysis is common in first responder incident command systems for routine responses, and is likely even more necessary when responding to a possible terrorism event. With the potential use of WMD and secondary explosive devices, it is imperative to maximize the safety of first responders to avoid having them become victims themselves.

Fire departments typically maintain a definite posture towards life safety and rescue. For example, Montgomery County (Maryland) Fire Rescue (MCFR) has a systematic approach to risk-benefit analysis. Their policy states, "Saving live victims is the rescue mission, while minimizing the risk of harm to the rescuers."[104] This does not mean that fire and rescue operations are suspended until all possible risks are defined in detail; the objective of the first responders remains saving as many lives as possible. In the event of a chemical attack, MCFR policy cautions first responders "not to 'automatically' assume that the incident involves super toxic chemical agents."[105] For the Phoenix Fire Department (PFD), risk-benefit analysis means that when victims are present all first responders are to move forward with standard operating procedures unless a secondary device is present. However, if no apparent victims, life hazards, rescue situations, or threatening fires exist, fire department personnel should not be exposed to risk. PFD policy states that in this situation "first arriving units should secure a perimeter, evaluate the situation, and await the arrival of the Hazardous Materials Technicians."[106]

[102] Elliott, Timonthy. "First Responders, Feds Join Forces." Fire Chief. December 2001. Fire Chief Magazine. July 8, 2003.
[103] Ibid.
[104] Montgomery County. Montgomery County, Maryland Fire and Rescue Service. Managing the Consequences of a Chemical Attack: A Systematic Approach to Rescue Operations. Montgomery County: Maryland, 2001.
[105] Ibid.
[106] City of Phoenix. Phoenix Regional Standard Operating Procedures. Hazardous Materials Weapons of Mass Destruction Chemical, Biological, Radiological. Phoenix: Arizona, 2000.

The first step in conducting a risk-benefit analysis involves assessing the disaster scene and gathering vital information. The early stage of information collection can include field reconnaissance (recon). Initial recon is viewed as a key factor when deciding if the rescue is a "Go" or "No-Go" situation. Ongoing data collection through recon provides the Incident Commander with the information needed to make accurate decisions regarding risk and resources. In a presumed WMD situation, the recon team is not sent to help victims; instead, their mission is to establish how many victims, the type of incident, and the level of risk involved with the incident. This information helps guide commanders in determining how to address the incident, and best save lives. However, it also means that the response time to triage, treat, and transport is necessarily longer than during a non-WMD incident.

c. Personal Protective Equipment

A significant component of an initial action plan is the determination of appropriate Personal Protective Equipment (PPE) for responders. Because time, distance, and shielding are important means for protecting responders from the exposure to gamma radiation, training is also a necessary pre-cursor to the response to incidents involving radiation.

The recon team is the first to move into an operational area. Therefore, it is imperative that they are equipped to handle any level of risk so that they can safely report back to the command post. MCFR policy is that the recon team wears the best available protective clothing with standard firefighting breathing apparatus:

> *For initial on-scene quick rescue of live victims, first responders should wear their turnout gear, self-contained breathing apparatus (SCBA), and butyl gloves. However, later into the incident and where rescue may still be required, first responders should wear Level B Protection or the appropriate chemical suit as indicated by the site safety plan.*[107]

The Boston Fire Department has similar guidelines regarding PPE. When Boston's first responders arrive on the scene of a presumed chemical attack, guidelines require them to don all PPE equipment available before entering the contaminated site.[108]

There has been much controversy on the best way to protect response units, especially when dealing with unknown agents in the opening hours of a response. In 1999, the Soldier and Biological Chemical Command (SBCCOM) issued guidelines for Incident Commanders' usage of PPE. While some departments felt these guidelines were useful, more than half of the fire service survey respondents said they would not sanction SBCCOM guidelines and would have developed their own PPE guidelines.[109] Some departments, including MCFR, have adopted selected SBCCOM techniques into their own guidelines. For example, MCFR instituted the usage of portable fans to help ventilate buildings where chemical agents may be present.[110,111]

---

[107] Montgomery County. Montgomery County, Maryland Fire and Rescue Service. Managing the Consequences of a Chemical Attack: A Systematic Approach to Rescue Operations. Montgomery County: Maryland, 2001.
[108] City of Boston. Standard Operating Procedure No. 61. Operations and Response to Terrorist Incidents. Boston: Massachusetts.
[109] Peterson, David F. "Terrorism and Turnouts: The Controversy." Fire Engineering. March 2002. Fire Engineering Magazine.
[110] SBCCOM test results showed that 50-70% of chemical concentration can be decreased when the portable fans are used.

Specialized protective equipment matched to hazardous substances is ideal but is currently not likely to be available in a timely manner or in quantity enough to accomplish victim rescues in most hazardous environments.

d. Secondary explosive devices

Terrorists can employ a number of tactics to inflict as much damage as possible. One strategy used by terrorists is the use of a delayed secondary explosive device. The purpose of such a device is to injure or kill first responders. Typically, these devices are hidden near the original incident.

Secondary explosive device awareness has become policy and is accounted for during first responder training throughout the world. Most first responder units understand the need to watch out for these devices. A review of several fire rescue policies indicates that even if secondary explosive devices are suspected, rapid intervention and victim removal still remains the ultimate goal. If secondary devices are found, response units are directed to immediately pull back and wait for specialized explosive ordinance disposal assets. For example, the PFD has a simple yet precise procedure addressing awareness of such devices. The first arriving units are expected to establish command and begin sizing up the situation. While responding, they are to:

> *...be aware of secondary devices designed to injure additional victims and/or first responders. Upon sighting a device that appears operable, [personnel are instructed to withdraw] until Police Bomb Squad has inspected/rendered safe any suspicious appearing device.*[112]

MCFR and the Denver Fire Department both have similar response methods.[113,114]

It is also useful to examine the emergency response policies of Northern Ireland and England. Their use of incident command and risk-benefit analysis has proven successful over decades of domestic terrorism response experience. The Northern Ireland Fire Brigade maintains an awareness of potential secondary device placement, avoiding command post locations near dumpsters and parked cars, where such devices may be hidden. Arriving bomb technicians sweep the command post areas first, eliminating the possibility of additional explosives.[115] The *United Kingdom Home Office Strategic National Guidance* also emphasizes the need to sweep command post and support areas for the presence of secondary devices.[116]

3. Reconstruction

The evaluation team did not obtain specific data describing the incident commander's risk-benefit analysis process. However, it did obtain data describing the response, which is the focus of this reconstruction. Figure 27 depicts a timeline of the key events during the rescue phase at

[111] Montgomery County. Montgomery County, Maryland Fire and Rescue Service. Managing the Consequences of a Chemical Attack: A Systematic Approach to Rescue Operations. Montgomery County: Maryland, 2001.
[112] City of Phoenix. Phoenix Regional Standard Operating Procedures. Hazardous Materials Weapons of Mass Destruction Chemical, Biological, Radiological. Phoenix: Arizona, 2000.
[113] Montgomery County. Montgomery County, Maryland Fire and Rescue Service. Managing the Consequences of a Chemical Attack: A Systematic Approach to Rescue Operations. Montgomery County: Maryland, 2001.
[114] City of Denver. City and County of Denver Emergency Operations Plan. Denver: Colorado, 2002.
[115] Langtry, John. Assistant Divisional Officer. Northern Ireland Fire Brigade. Telephone Interview. July 16, 2003.
[116] United Kingdom Home Office. Strategic National Guidance. The Decontamination of People Exposed to Chemical, Biological, Radiological or Nuclear (CBRN) Substauces or Material. United Kingdom. February 2003.

the RDD site. It was constructed using the observations from data collectors at the incident site. All times are noted in Pacific Daylight Time (PDT) unless otherwise specified.

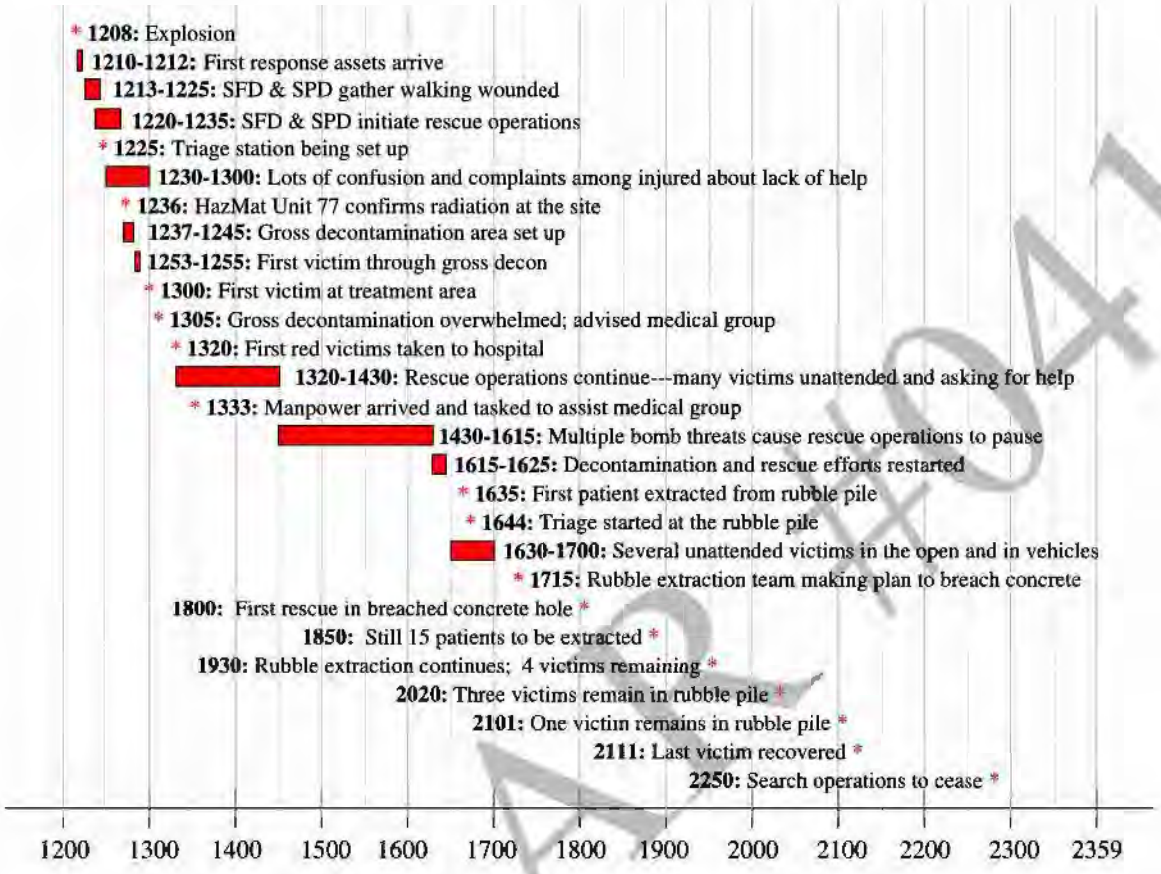


Figure 27. Reconstruction of Rescue Operations at the Radiological Dispersal Devise Site

Incident site observations indicate that within minutes after the simulated RDD explosion on May 12, 2003, police cruisers, fire engines, and ambulances arrived at the scene. The responders, in particular Seattle Police Department (SPD) personnel, first gathered all walking wounded and removed them from the scene. SFD repeatedly made announcements over the loud speaker instructing anyone who could walk to slowly approach Engine #2 and that help was on the way. SPD was observed searching through the rubble and vehicles, administering first aid, and directing victims to Engine #2. SFD was also observed using ladders to get victims out of buildings. All of these events occurred within 14 minutes of the explosion.

Observations of the response took on a different tone after 1222[117] when the first reports of radiation reached the incident site. HAZMAT arrived at 1227 and immediately started to take readings. There was much confusion at the incident site with several accounts of victims crying for help with no response from rescuers.

[117] All times Pacific Daylight Time.

At the same time that HAZMAT was taking initial readings, SFD was also setting up triage, treatment, and decontamination stations. According to logs from data collectors observing the incident site, a triage station was being set up by 1225,[118] a treatment station was set up by 1243, and a decontamination station was set up between 1237 and 1252. The first victim was moved through the decontamination station at 1253, and the first victim was observed at the treatment station at 1300.[119] At 1305, the decontamination station reported that they were overwhelmed with victims. There was no indication that they got any assistance until 1333, when additional personnel arrived and were tasked to assist the medical group.

During a typical mass casualty incident, victims are tagged with colored tape or paper based upon the extent of their injuries. Victims with red tags have life threatening injuries and require immediate care. Victims with yellow tags need treatment but could sustain a short delay. Treatment of victims with green tags can be delayed until the more seriously injured victims have been cared for. Figure 28 shows the times that victims with red, yellow, and green tags were transported from the incident site to a hospital according to data obtained from hospital control. The first two red victims were taken at approximately 1315.[120] From 1315 to 1508, a steady stream of victims was taken to area hospitals. From 1315 to 1424, only the more serious red and yellow victims were transported, and then from 1424 to 1508 mostly green victims were taken to the hospital. This suggests that there was a lull in the response and no seriously injured victims were rescued and taken to the hospital. In fact, rescue operations had periodically been delayed due to reports of sniper sightings and potential secondary explosive devices prior to 1430 and were halted at approximately 1430 because a secondary explosive device was found at the incident site.

Rescue, treatment, and decontamination operations started again between 1615 and 1630, and as shown in figure 28, victim transport was restarted at 1638. Mostly red and yellow victims were taken to area hospitals between 1638 and 1814, at which time hospital control ended operations. The data show that prior to the pullback at 1430, a red or yellow victim was transported every 3.4 minutes; after rescue operations resumed the transport rate increased to one red or yellow victim transported every 1.6 minutes. It is not clear what led to an increase in rate of victims transported.

[118] The evaluation team has no data indicating the level of activity at the triage station at this early stage of the response, and no data indicating when the triage station was operational.
[119] The evaluation team has no data indicating the severity of injuries for the victims moving through the decontamination and treatment stations at this early stage of the response.
[120] Note that the data do not indicate if these patients were the first patients to go through decontamination or if the red patients went through decontamination at all.

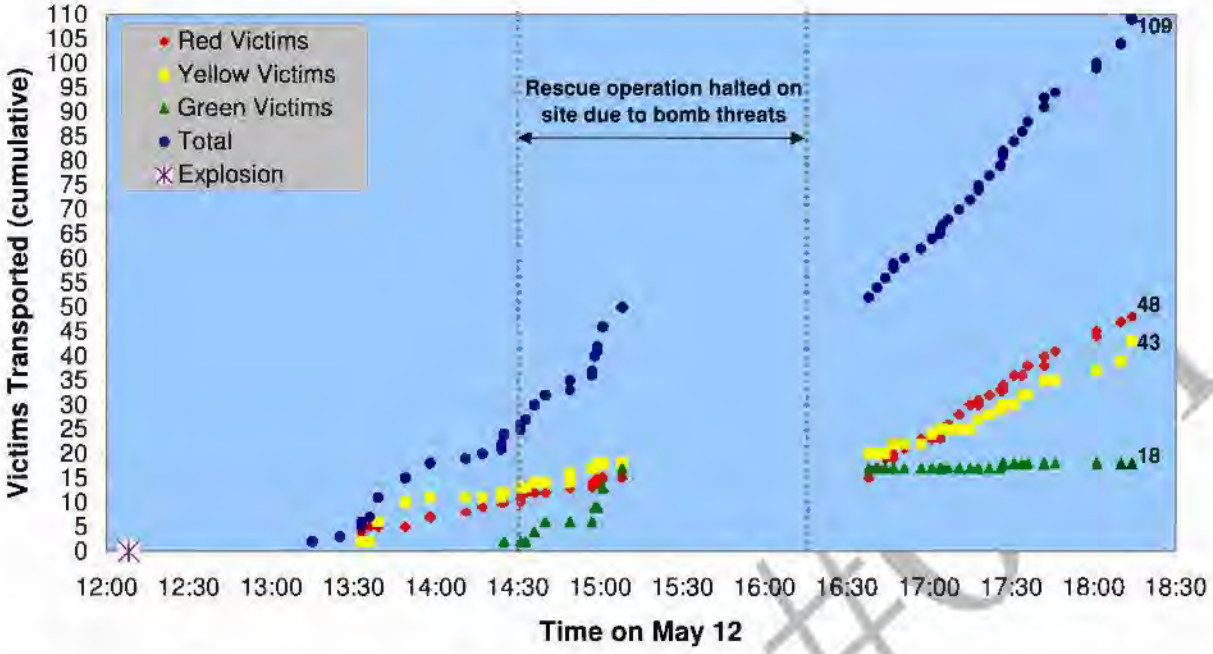


Figure 28. Transport of Victims from Incident Site[121]

According to data obtained from Harborview Hospital, which was hospital control during the exercise:

- A total of 109 victims were transported to area hospitals during the time that hospitals participated in the exercise: 48 red, 43 yellow, and 18 green victims; and
- At the beginning of the exercise, 150 volunteers were placed in the incident site. Therefore, 41 victims remained on the incident site when hospital play ended.

However, the log kept by hospital control differs with the tracking data kept by exercise control. According to exercise control:

- A total of 115 victims were transported to area hospitals: 34 red, 46 yellow, and 35 green;
- Responders rescued an additional 13 victims too late to be processed by the hospitals. These victims were still loaded into ambulances, but taken directly back to Union Station; and
- An additional 22 victims were not rescued until after hospital exercise play ended.

The evaluation team was unable to determine why there was a discrepancy in the two logs. Possible explanations include:

[121] Data from Harborview Medical Center Mass Casualty Incident Patient Tracking Log and Seattle King County Public Health Incident Log.

- Exercise control assigned an injury status to each of the victims at the start of the exercise. Responders may have re-classified victim status during the course of the exercise;
- It is possible that there were additional victims transferred to area hospitals from 1511 to 1608 when hospital control was temporarily transferred to Overlake Hospital; and
- It is possible that the 13 victims recorded by exercise control that were processed and transported to Union Station after hospital control ceased operations were not recorded by hospital control.

4. Artificialities

During the FSE, a number of artificialities affected how players responded to the RDD incident, as well as some players' perceptions of the response and are, therefore, factored into the analysis. The artificialities included:

- Responders were at an advantage because they knew that the scenario involved an RDD explosion. Furthermore, many responders were aware of the concerns that came out of TOPOFF 2000 and other real world or exercise events—that responders went into an incident site so quickly they became casualties themselves. Therefore, during the FSE, many first responders did not rush into the scene when rescue operations began.
- Exercise control expected to have 200 moulaged victims for the exercise. Based upon initial planning for the exercise, hospitals expected ninety percent of all victims to be transported by 1800. This translates to 180 victims transported. However, there were 50 volunteer no-shows on the morning of May 12, 2003, so there were only 150 moulaged victims. Hospital control was not aware of this change. So they were expecting more patients than were available; this may have exacerbated medical and public health concerns about the overall rescue.

5. Analysis

Observations from the incident site from the first hour after the explosion indicate that after radiation was detected, responders were held back while HAZMAT teams conducted an initial assessment of the situation. While hospital control was aware that radiation had been detected at the incident site, there is no indication in the data collector logs that incident command or the medical group at the incident site communicated with hospital control to explain the need to conduct a more detailed risk-benefit analysis before rescue operations could commence.

After the first hour, the response became more typical—victims were pulled out of the incident area, assessed, and transported to the hospital based upon the severity of their injuries. However, rescue and decontamination operations were periodically halted and eventually ceased for almost two hours due to secondary bomb threats.[122] This caused a similar delay in the transport of victims to area hospitals. There is no evidence in the data collector logs that indicated hospital control or the individual hospitals were aware of this delay. Similarly, there are no data from data collectors at the incident site indicating that the medical group or incident command

[122] This delay would likely have been even longer if exercise control had not injected that the secondary explosive device was far enough away that it would not impact rescue operations.

communicated with hospital control about the discovery of a secondary explosive device. After the FSE, a hospital controller confirmed that the hospitals were unaware of the secondary explosive device.

6. Conclusion

Rescue operations at the RDD incident site during the FSE highlight the need for incident command and hospital control to communicate with each other during an emergency, especially one involving WMD. The public health and medical communities should be made aware of the need for incident command to conduct a detailed risk-benefit analysis prior to the start of rescue operations. These communities also need to be aware of the actions rescuers will take if a secondary explosive device is found and the impact that will have on victim rescue and transport. In addition, incident command must communicate with the public health and medical officials so that they understand the situation.

SUMMARY OF CONCLUSIONS—BALANCING THE SAFETY OF FIRST RESPONDERS AND THE RESCUE OF VICTIMS:

- Operations at the RDD incident site highlighted the need for robust communications between hospital control and incident command.
- The medical and public health communities need to be educated concerning the activities that first responders will take when faced with a potential terrorist incident involving WMD.
- Public information personnel from the first responder, medical, and public health communities should also be educated about expected emergency response procedures so that the media and, therefore, the public are given one consistent message during an incident.

While it didn't occur during the FSE, it is extremely likely that in a real-world emergency the media would have become aware of the delay in transporting victims to hospitals. Without a concerted message from the public health and responder communities concerning the need to balance responder safety and victim rescue, a public outcry could have ensued. Therefore, public information personnel from both of these communities need to be educated about expected emergency response procedures during a mass casualty incident, especially one involving WMD. In addition, they also need to be kept informed by their respective leadership to ensure a consistent message is presented to the media and the public.

This page intentionally left blank

VI. ANALYSIS OF THE SIX CORE AREAS

1. Introduction

These six core areas of analysis were identified early in the Top Officials (TOPOFF) 2 (T2) planning phase by reviewing the TOPOFF 2000 After Action Report (AAR), lessons learned from 9/11 and the following anthrax attacks, Federal, State, and local participant objectives for T2, previous weapons of mass destruction (WMD) exercise AARs, and WMD training materials. Although the issues differed somewhat in content and presentation, they displayed considerable underlying similarity, and naturally clustered into six core areas of analysis. While these areas are closely interrelated, they are distinct. Viewing the exercise in light of these areas provides a useful organization of observations and ideas.

These areas of analysis include:

- Emergency public policy and decision-making;
- Emergency public information;
- Communications, coordination, and connectivity;
- Jurisdiction;
- Resource Allocation; and
- Anticipating the Enemy.

Because emergency public information played such a central role in each of the pre-Full-Scale Exercise seminars, as well as the Full-Scale Exercise (FSE), particular emphasis is placed upon this area.

2. Instances of challenges and good practices

In the various building-block seminars and the Large-Scale Game (LSG) leading up the FSE, several issues, or challenges, emerged that are relevant to the six core areas of analysis. In addition, a number of potential good practices were identified by seminar and LSG participants. During and subsequent to the FSE, the evaluation team identified instances of these challenges and good practices that occurred during the exercise. *Instances* are defined as occurrences that played out during the FSE. In several cases, challenges and good practices arose during the FSE that were not anticipated by the seminar and LSG participants. These were identified and catalogued by the analysts as well.

For each core area, a brief introduction and background are provided. This allows for an FSE-based context, such as key events and challenges that occurred within the areas, for discussions of the area. This is followed by a discussion of the key challenges and good practices in which feedback from the seminars and the LSG is examined and compared to the issues that arose during the FSE. Finally, conclusions are drawn and suggestions are made as to how these issues could be tested in future exercises.

This page intentionally left blank

A. Emergency Decision-Making and Public Policy

1. Introduction

Public policy and decision-making during an emergency differs from day-to-day policy and decision-making. The difference is even more significant during an emergency as a result of a terrorism attack. In such emergencies, top officials face especially difficult, political decisions under conditions of uncertainty characterized by unknown, or changing, information-baselines. For example, public health considerations might make quarantine a seemingly obvious choice. But, as was observed regarding Top Officials (TOPOFF) 2000 by Biodefense Quarterly in September 2000:

> *Decisions regarding patient isolation, travel advisories, home curfews, the closure of airports and highways, and attempts to "quarantine" cities and states must be balanced against the practical feasibility of such measures, and their implications for civil liberties.*[123]

This area examines the unique challenges, difficulties, and nuances of decision-making and policy-making in the initial aftermath of a terrorist weapons of mass destruction (WMD) attack.

2. Background

Despite foreknowledge of the scenario by some but not all, top officials and other decision-makers faced numerous challenging decisions throughout the course of the exercise. Some of these decisions are provided in Table 10.[124]

[123] Inglesby, Thomas, Grossman, Rita, and O'Toole, Tara, "A Plague on Your City: Observations from TOPOFF," *Biodefense Quarterly*, Volume 2, Number 2, September 2000.

[124] Decisions shown do not necessarily represent every decision made by top officials in these jurisdictions, but rather a sampling of the primary emergency public policy-related decisions.

Table 10. Examples of Emergency Public Policy Decisions Faced during T2

Washington Venue	Illinois Venue	Federal Agency/Executive
• Determination of shelter-in-place order. • Issuance of mayoral and county proclamations of civil emergency. • Issuance of mayoral and county delegations of authority. • Issuance of governor proclamations of state of emergency. • Governor's request for Presidential Declaration of Major Disaster. • Implementation of exclusionary zone by city officials. • Closure/re-opening of road system by Washington Department of Transportation (WDOT) and city authorities. • Implementation of food control zone by state officials. • Determination of protective actions under condition Red by all affected jurisdictions. • Evacuation from shelter zone by city, county, and state officials. • Controlled re-entry to exclusion zone by emergency workers and members of public. • "Initial return" by state officials to allow people to return home in areas that did not appear to be affected by blast. • Radiological remediation and recovery criteria	• Determination of protective action guidelines (PAG) for containing the plague (shelter-in-place) by state officials. • Issuance of mayoral and county proclamations of civil emergency. • Issuance of mayoral and county delegations of authority. • Issuance of governor proclamations of state of emergency. • Governor's request for Presidential Declaration of Major Disaster. • Closure/re-opening of the road system by Illinois Department of Transportation (IL DOT). • Executive Order #3 - suspended pharmacy practice act to let non-pharmacist to dispense prophylaxis and to do so outside of pharmacies. • Executive Order #4 – authorization to implement quarantine. • Determination of protective actions under condition Red by all affected jurisdictions. • Determine priorities for distribution of the Strategic National Stockpile (SNS) by Illinois State. • Re-opening of roads by IL DOT. • Medical decisions: —where to move critically ill, versus exposed, versus worried-well, versus other patients. —whether to convert specific rooms or an entire building to negative pressure, if the capability exists. —determination of how long patients should stay at hospitals. —determining how patients would get home when discharged under condition Red.	• The elevation of the seven-city alert level to Red by the Department of Homeland Security (DHS) based upon the radiological dispersal device (RDD) attack and intelligence. • The elevation of the national alert level to Red by DHS based upon the RDD and bioterrorism attack. • Presidential Declarations of Major Disaster and Emergency in the states of Washington and Illinois, respectively. • Declaration of a Public Health Emergency by the Secretary of the Department of Health and Human Services. • Closure of airspace by DOT/Federal Aviation Administration (FAA). • Federal restrictions on food distribution by regional Federal Drug Administration. • Re-opening of airspace by FAA.

3. Discussion of challenges/good practices

In the seminars leading up to the Full-Scale Exercise (FSE), Top Officials (TOPOFF) 2 (T2) participants identified numerous challenges and some good practices related to *Emergency Decision-making and Public Policy*. Almost all of the challenges and good practices were observed during the FSE. This is additional evidence that foreknowledge of the scenario in an exercise does not necessarily result in foregone conclusions. While all the core areas of analysis in T2 are interrelated, the area with the greatest impact on emergency decision-making is that of

Communication, Coordination, and Connectivity. The ability of decision-makers to obtain or discern reliable, validated, timely, and understandable information to inform their decision-making emerged as a primary challenge throughout the exercise.

Table 11 depicts the challenges, and good practices relevant to *Emergency Decision-making and Public Policy* that arose in the seminars, as well as the instances that show how these issues played out during the FSE. Instances are occurrences experienced hy participants during the FSE that indicate challenges or good practices associated with particular issues. In the table, a (-) is used to indicate challenge, and a (+) indicates a good practice. A ( ) is used to indicate a neutral observation in the FSE—one that is neither a good practice nor an issue. *Good practices* are those practices that players felt were effective, or which the data indicate worked well;[125] these practices could potentially be explored further or promulgated on a broader scale. *Challenges* are examples of the T2 response that were difficult for the responder community and that had significant impact on decision-makers. Challenges do not imply wrong actions or incorrect responses by any organization or the community at large—this After Action Report (AAR) and the analysis as a whole did not focus on evaluating right and wrong actions. Challenges require the continued attention of the national response community to facilitate smoother responses in the future.

[125] References in the table are based on specific references in the data. Just because something is not specified as a good practice does not mean it did not go well in participants' opinions or did not happen.

Table 11. Emergency Decision-Making and Public Policy Issues during T2

ISSUES	SEMINARS/LSG					FSE INSTANCES GOOD PRACTICES AND CHALLENGES
	Emergency Public Information	*Radiological Dispersal Device*	*Bioterrorism*	*Direction & Control*	*Large-Scale Game Consequences*	
a. Understanding what decisions need to be made and by whom.		✓	✓	✓	✓	See "Jurisdiction" Core Area (+) Washington State Emergency Operations Center (EOC) attempted to use defined decision processes. (+) Seattle EOC representatives cross-fertilized decisions. (-) Some uncertainty in road re-opening authorities. (-) Some uncertainty in airspace re-opening authorities. (-) Some uncertainty in authorities to re-open facilities where plague was released.
b. Making decisions under conditions of uncertainty: accuracy versus timeliness of decisions.		✓	✓		✓	(+) Radiological dispersal device (RDD) site leaders recognized that decisions needed to be made without all information. ( ) The shelter-in-place zone had to be expanded in Washington. ( ) Discussion on size of exclusion zone. ( ) Road openings in Washington would likely have had to be re-closed due to plume. ( ) First responders in Washington held back on victim rescue pending preliminary risk-benefit analysis.
c. Handling international implications of decisions (transportation, security, etc.) and having consistency in decisions across borders.	✓			✓	✓	(+) Numerous instances of Department of Homeland Security (DHS) and other agencies interfacing with international authorities.
d. Making the notable, politically charged decisions (quarantines, Strategic National Stockpile (SNS) distribution, etc.) and how to handle them.				✓	✓	() Officials in Chicago suggested requiring proof of presence at one of the release sites to receive prophylaxis. ( ) Quarantine was considered in Illinois. ( ) Whether other countries could access the stockpile was considered.

ISSUES	*SEMINARS/LSG*					FSE INSTANCES GOOD PRACTICES AND CHALLENGES
	Emergency Public Information	*Radiological Dispersal Device*	*Bioterrorism*	*Direction & Control*	*Large-Scale Game Consequences*	
e. Management of economic impacts of increased security measures.				✓	✓	(+)Information Analysis and Infrastructure Protection Directorate in DHS examined economic impacts of nationwide alerts. (+) Agencies at all levels documented the projected economic impacts of security measures.
f. Understanding the extent to which the Threat Condition Red changes every aspect of decision-making.				✓		(-) Most agencies were uncertain what actions to take in response to an elevation of the Homeland Security Advisory System to Red.
g. Handling/understanding long-term restoration impacts.					✓	NA. Not played.

a. Understanding what decisions need to be made and by whom, and knowing who to have at the table

This issue is inherently related to the core area of *Jurisdiction* (See the "Jurisdiction" *Core Area*), but it has significant implications in the arena of emergency decision-making. Emergency policy decisions in the aftermath of a terrorist WMD attack are challenging enough, but not knowing who has the authority to make what decisions adds tremendously to the challenge. Such uncertainty not only impacts public relations (to the extent it increases the chances of inconsistent messages going out, or messages that may need to be altered later), but it also multiplies the inter-agency coordination burden as agencies feel their way through the process under the pressure of an unfolding disaster.

The *Jurisdiction* core area examines the jurisdictional uncertainties that participants experienced during the exercise, almost all of which arose in the context of decisions. Transportation emerged as a primary area where many were not aware of the various authorities for closing and re-opening elements of the nation's transportation system, including roads, airspace, the rail system, and ports. Other issues where decision-making was unclear included Homeland Security Advisory System (HSAS) threat elevations (see the "Alerts and Alerting" *Special Topic*), and re-opening the facilities in Illinois where plague was released.

Another issue faced by decision-makers is not always having the right people involved in the decision-making process, and sometimes not knowing who the right people are. Both of these factors can make the unique challenges of this core area—making difficult policy decisions under conditions of uncertainty—more challenging. Likewise, improvements in the decision-making process can help reduce the uncertainty in some decisions, and increase the credibility of difficult decisions faced during such times. There were instances of the FSE during which decisions were not coordinated with all relevant parties. Perhaps the most dramatic example of this was when decision-makers at Federal, State, and local (FSL) levels were challenged to make policy decisions based upon the potential radiological contamination in the Seattle area. Setting aside the difficulties they experienced confirming the extent of the contamination (See the "Data Coordination" *Special Topic*), top officials needed experts who could translate detailed technical data into plain-language to aid them in the policy decisions they faced.

Not all agencies had the needed technical expertise on hand. In the words of a King County Emergency Operations Center (EOC) participant, "translating technical data on radiation into meaningful 'so what' terms and coordinating this was difficult. It took us three days to find someone [decision-makers] could understand." The Washington State Department of Health acknowledged in the venue Hotwash:

> *Our biggest policy issue was around data—we were data rich and information poor. We did not have one place where highly technical data were being analyzed in one place. The result was that different policy rooms were making decisions based upon the data they had, which were probably right based upon the data they had, but not consistent with others.*

Federal resources designed to assist decision-makers in translating technical data into meaningful terms were often not effectively utilized during the exercise. For example, the Advisory Team, which provides Protective Action recommendation support for decision-makers under the Federal Radiological Emergency Response Plan (FRERP), was not accessed by local decision-

makers. This struggle to understand the implications of detailed technical data, despite knowledge of the scenario by some, demonstrated that decision-makers were not assisted in this particular area by knowledge of the scenario.

The City of Chicago and the collar counties also noted in their Lessons Learned Reports from T2 the importance of having the right people in decision processes, stating that EOCs must be staffed with decision-makers, not just information gatherers. They also noted the importance of configuring seating arrangements in the EOC to have similar disciplines grouped together. One example of a good practice is that WA State EOC staff appeared to have defined decision processes that they used in their decision-making. Designed by the emergency managers who work there, the WA State EOC facility floor plan and building design promotes collaborative decision-making and information flow with its open floor structure, video teleconference capability, and electronic information sharing systems. In addition, a data collector in the Seattle EOC remarked that the EOC appeared to have substantial representation from various disciplines on hand to cross-fertilize decisions, and there appeared to be processes by which designated staff was empowered for emergency decision-making when the Mayor was absent.

b. Making decisions under conditions of uncertainty: accuracy versus timeliness of decisions.

The spokesperson for the City of Seattle at the venue Hotwash summarized this issue well when he said to the audience, reflecting on his experience from the FSE, "Nothing is static—the plume changes, evacuation zones change, etc. A solved problem is maybe only temporary—a final decision this hour may be a different decision the next hour."

Top officials are routinely challenged in real life to make decisions under conditions of uncertainty. In both the Washington and Illinois, decision-makers were faced with the challenge of making decisions under conditions of imperfect information. In some cases, needed information was forthcoming in time (such as knowledge about whether an outbreak of Pneumonic Plague is naturally-occurring or an act of bioterrorism). In others, the information was unknown or may be based upon imperfect data, still requiring interpretation. In both cases, decision-makers must weigh the relative costs of time—the delay while waiting for the information base to improve—against the costs of less-than-perfect information.

T2 provided opportunities for decision-makers to explore these tradeoffs. The role of the Department of Homeland Security (DHS) is to assess the risk of terrorist attacks (a very imprecise task by definition), and to implement preventative measures designed to prevent or thwart attacks. This is an exceptionally difficult task replete with uncertainty. However, the Secretary of DHS cannot afford to wait for certainty to act—*certainty* for the Secretary of DHS is defined as an attack.

Perhaps the most dramatic decisions that were made during the FSE were those by the DHS Secretary to elevate the national alert system to Red first in seven select cities, and then nationwide (the City of Seattle and King County both elevated their jurisdictions to Red in the wake of the radiological dispersal device (RDD) blast—this is discussed in more detail in the "Alerts and Alerting" *Special Topic*). Of course in the exercise this was notional, and based upon notional intelligence. Likewise, in the exercise the real implications of a nationwide red alert could not be played. But the decision process and decision tradeoffs that the DHS Secretary and the Homeland Security Council (HSC) considered were real. And agencies' responses, if

only to express great concern at the cost of maintaining a condition Red posture given a nonspecific threat, were also real. They challenged leaders to refine the HSAS system so that it achieves the intended goal of preventing future attacks in a way that, if possible, is more specific to localities at greater risk and minimizes unintended consequences.

In Washington, many policy decisions were made under conditions of uncertainty. The shelter-in-place parameters, the size of the exclusion zone, boundaries of the food zones, and road closures all depended on information regarding the size and nature of the radiological contamination. In anticipation that decision-makers would receive limited data in the early hours following the RDD incident, the Washington Department of Health, Public Health Seattle/King County, and the EPA developed default Protective Action Guidelines (PAGs) prior to the FSE. The Seattle Mayor implemented these *default* PAGs during the early hours of the incident, as decision-makers awaited the collection of the data required to effectively model the radiological contamination. During T2, as in reality, information changed over time, and some decisions had to be re-examined. Decision-makers in the WA venue, for example, expanded the shelter-in-place parameters once, and held heated discussions regarding the size of the exclusion zone. They also confronted the political issues of opening and then potentially having to re-close transportation systems based upon the recognition that they did not have all the information needed for these decisions. Operational decisions at the incident site were made in the midst of uncertainty, such as how long to wait for confirmation of radiation readings before rescuing victims, although it was somewhat influenced by artificiality. During T2, there is evidence to suggest responders held back from rescuing victims until a preliminary risk-benefit analysis could be done.

In the bioterrorism attack in Illinois, decision-makers were constantly challenged to make decisions under uncertainty. For reasons both of exercise artificiality as well as coordination challenges between agencies, tracking patient numbers was extremely difficult. Hospitals and the public health community were challenged to anticipate and plan for surge issues that would likely overwhelm the public health system within seven to ten days under the scenario.

And of course, throughout the exercise there was some uncertainty as to whether there would be additional follow-on attacks, though this was not aggressively played by most and was not specifically designed into the exercise.

c. Handling international implications of decisions (transportation, security, etc.) and having consistency in decisions across borders

The international scope of T2 was another ground-breaking element of T2 design. Represented through Canadian play and notional international injects, this expanded the scope of decisions and implications faced by top officials. On the domestic side, there were numerous instances of DHS and other agencies interfacing with international authorities in decisions such as transportation, food and import restrictions, border security, economic impacts of decisions, threat intelligence, and protective action measures. In the *National Direction and Control Seminar*, Canadian representatives stated that they would be interfacing with the Centers for Disease Control and Prevention on epidemiological data and tracking. They did just that during the T2 FSE. In addition, Canadian officials worked with DHS to place liaisons in Washington and Illinois. The DHS Office of International Affairs also coordinated extensively with Canadian counter-parts in all aspects of play to include the elevations of the threat condition to Red and addressing potential international economic implications of security measures and job

furloughs. Interestingly, in the seminar on bioterrorism, participants stated they did not think that cancellation of international flights would be likely once the plague epidemic spread internationally. This is another example of things not happening as expected during the FSE: the first cases of a mysterious illness were being reported from Vancouver as early as May 12, 2003. Within two days international (and domestic) flights were suspended as the U.S. transportation system was temporarily shutdown in Chicago. The Department of State (DOS) and Canadian AARs address international implications of the scenario and the lessons learned from the FSE in detail.

d. Making the difficult, politically charged decisions (quarantines, Strategic National Stockpile distribution, etc.)

During T2, decision-makers at all levels faced difficult decisions. The DHS decision to raise the red alert was surely a difficult one, and was discussed previously. In another example of a key decision, the Governor of Illinois requested a Presidential Declaration of Major Disaster to obtain federal assistance through the Stafford Act for the escalating bioterrorism disaster that had its epicenter in Chicago. This request was first denied, likely because it did not qualify under the language of the Stafford Act[126]. In the end, this request was approved as an emergency declaration—and while purely notional, is nonetheless groundbreaking to the extent it challenged traditional interpretations of the Stafford Act.

Decision-makers in Illinois faced two difficult decisions: The potential need to implement a quarantine and how to distribute the limited initial supplies of the Strategic National Stockpile (SNS) before the arrival of the Vendor-Managed Inventory (VMI).[127] While officials never publicly used the term quarantine and did not notionally enforce it, the decision was made to close down air, sea, and rail transportation and to instruct the public to take a voluntary "snow day." By May 14, 2003, the IL Governor had issued an Executive Order authorizing this and other emergency measures, such as releasing patient information to law enforcement and allowing licensed medical practitioners to operate outside of normal areas. Another Executive Order allowed non-pharmacists to dispense prophylaxis.

An interesting decision in Chicago was one where authorities required physical proof of exposure to one of the three known release sites as a prerequisite for receiving SNS medications, to ensure that only the initial exposed population (and its close contacts) received what were originally limited numbers of medication. This policy appeared to ignore the problem of secondary infections that the city and counties were beginning to deal with at that point, not to mention the possibility that other releases were still underway.

In an example of a good practice, city and state officials proactively acted to implement authorities to enable them to take extraordinary measures such as the ability to implement quarantine and to let non-pharmacists dispense prophylaxis and to do so outside of pharmacies should it be needed. DHS appeared to be researching legal authorities to implement a national quarantine should it be necessary.

[126] The Stafford Act was developed to address natural disasters or those with physical infrastructure damage.

[127] As described in the "SNS" Special Topic, it is an exercise artificiality that the push packages were deployed at all. In a real event, the SNS reaction to requests for SNS would have been to send the Vendor Managed Inventory, since Pneumonic Plague was already identified. Nevertheless, during the FSE top officials in Illinois had to make decisions as if they had a limited supply of prophylaxis.

e. Management of economic impacts of increased secnrity measures.

The FSE did not play out long enough for players to have to manage the economic implications of increased security measures, with the exception of potential impacts relating to the various alert elevations to Red. There are numerous instances in which agencies at all levels actively considered such impacts. The Information Analysis and Infrastructure Protection Directorate within DHS examined economic impacts of the nationwide alerts on May 14, 2003. Concerns related to this were a dominant theme in the *Alerts and Alerting* session at the AAC.

These issues were front and center at the post-FSE tabletop exercise held in the Washington venue on May 15, 2003, and also at the LSG (see LSG AAR) held in December 2002[128]. In the tabletop, participants recommended the involvement of the private sector to lend insights into this critical aspect of recovery and restoration. The Director for Economic Consequence Management at the Homeland Security Council was in attendance and stated that a Working Group would be established to initiate economic analysis using the Department of Commerce to evaluate the magnitude of the incident, and later develop two-week and two-month assessments to better understand the impacts. The Working Group would identify what federal resources might be available, but would work through local and State officials and the private sector to develop a local economic recovery plan and to make recommendations to the White House on needed resources.

During the LSG, participants in the economics group cited the need to conduct micro- and macro- economic disruption analysis; develop a long-term recovery plan; and catalogue available federal support across agencies. The Canadian delegation at the game predicted an increased focus on protecting national critical infrastructure and expectations that the private sector would start spending more on security, rather than waiting for government help. During T2, the private sector was minimally represented. Numerous participants suggested expansion of private sector participation in future TOPOFFs and the continuance of events such as the LSG to examine longer-term issues such as this.

f. Understanding the extent to which condition Red changes every aspect of decision-making

This issue was difficult to assess during T2, partially because many of the broad-reaching increased security measures one might expect under Threat Condition Red were already implemented (or in the process of being implemented) by the two participating venues as direct protective action responses to the specific attacks they were facing. Another reason this is difficult to assess is, as was discussed under the *Special Topic* section on alerts and alerting, there was widespread uncertainty on the part of most agencies as to what actions they should be taking in response to Threat Condition Red. This topic, for this reason alone if nothing else, merits continued attention and refinement by agencies at all levels. Future TOPOFF exercises might consider inviting States or cities that are not directly affected to participate in the FSE to gauge this and other national issues.

g. Handling/understanding long-term restoration impacts

Long-term restoration impacts were not played during T2 due to the duration of the exercise. They were addressed in the LSG where participants from FSL and international agencies, as well

[128] The LSG examined longer-term impacts in the aftermath of terrorist WMD attacks.

as the private and non-profit sectors spent three days actively discussing long-term restoration challenges in the aftermath of terrorist WMD attacks in three post-attack "moves:" Move I, 30 days out; Move II, 30 days through 6 months out; and Move III, 6 months out and beyond.

In Move II of the LSG, the issues centered primarily on the areas of decision-making and public information as participants cited ripple effects of security measures on the economy and international communities, the lack of a tax base to support needed revenue streams, continued issues in maintaining public confidence, managing economic impacts, managing calls for bureaucratic reorganizations, and managing growing accountability/liability issues with government actions. In Move III, participants were very cognizant of the fundamental shift in the national psyche that would have occurred by a campaign of terrorism attacks, and which would affect every sector, particularly the economic sector. They cited the tremendous drain on personnel and budgets in many localities, but specifically those directly affected by the RDD and bioterrorism attacks. They raised the issue of the continued and ever-present threat of future attacks, and how to improve prevention. Finally, they cited the numerous economic measures that would need to be taken by corporations and citizens to supplement the economy. Long-term remediation of a radiological incident site was not fully addressed during T2, not even during the LSG. In reality, it would receive heavy state, local, congressional, and media attention and would he one of the most critical aspects of response. The responsibility under existing plans for carrying out clean up activities is not clear under existing policies and should be examined in future exercises. Further the FSE did not play out long enough to fully exercise the public health implications of a bioterrorism attack. Participants unanimously cited the value of exercises that force them to confront and explore long-term restoration issues and impacts. The building-block structure of the TOPOFF Exercise Series lends itself to examining these issues.

4. Conclusions

Two groundbreaking decisions were addressed during the FSE that have not yet occurred in the real world:

- Elevations to red by City, County and Federal authorities (DHS); and
- Request for and issuance of a Presidential Declaration of Emergency for a bioterrorism disaster.

Decision-makers at all levels struggled with these and other difficult emergency public policy decisions, demonstrating that foreknowledge of the scenario by some participants in no way led to foregone conclusions.

The ability of decision-makers to obtain or discern reliable, validated, timely information, and to translate complex technical data into information that informs policy decisions, emerged as a primary challenge that underpins this entire core area. Quality decision-making does not mean that the decisions do not change or are permanent. Quality decisions are based upon the best information available at the time—information that sound processes help to ensure is valid. As the information-baseline evolves and decisions must be re-examined, there is a solid hasis for the new decisions that emerge. Quality decision-making is marked by a thorough understanding and assessment of the tradeoffs at stake, which is only possible by having the correct expertise and decision authorities at the table.

The international scope of T2 and active participation of the Canadian Government expanded the scope of decisions faced by domestic top officials in the exercise. It represented a significant new element of the TOPOFF exercise design and participants have stated that it should be expanded upon in the future. The international implications of domestic decisions made during T2 are addressed with the T2 AARs produced by DOS and the Canadian Government.

While the economic impacts of terrorist attacks and resulting security measures and long-term restoration and recovery issues were not exercised during the FSE, participants throughout the exercise expressed continued interest in exploring these issues. Future TOPOFFs should expand on the concept of the LSG, which addressed long-term issues such as these in-depth. Finally, public response was not aggressively played during T2 and may be another element worthy of consideration to further challenge decision-makers in through branches and sequels in future exercises.

B. Emergency Public Information

1. Introduction

By definition, the term *emergency public information* reflects an understanding that public information during an emergency might differ from business-as-usual public information. Further, the task of those responsible for public affairs might vary according to the type of emergency—natural disaster or terrorist attack. For these reasons, those responsible for public information may find that despite the fact that they do their job every day, it becomes different, and very possibly more important, during a set of events like those that were simulated during T2.

The 9/11 attacks and the Maryland/Washington D.C./Virginia sniper attacks of 2002 demonstrated another unique aspect of terrorism regardless of scale: The acts may have been local in nature, but they were national in impact. These challenges caused emergency public information to emerge as a top issue in TOPOFF 2000 and in T2. T2 provided a context in which emergency public information strategies could be tested, examined, and refined under the challenge of dealing with two different, simultaneous attacks (with more potentially in motion).

The T2 design did not include an aggressive news-gathering function with multiple reporters calling the offices of top officials; it did not include substantial injects of simulated public responses to information; and it did not involve print or radio media outlets. Also, many of the most likely spokespeople in real emergencies—top officials—were not able to play at a level to truly simulate round-the-clock, real-world public information involvement. Special mention should be made though of those federal officials such as the Secretaries of DHS and HHS, as well as local officials such as the Mayor of the City of Seattle, who played extensively. However, these design elements, while potential considerations for future exercises, are not necessary to explore and exercise emergency public information issues. During T2, public information officers (PIOs) participated; media was simulated in some cases through the use of the Virtual News Network (VNN); and press releases were developed that, had this been a real-world event, would have been broadcast. This area of analysis examines those sources, as well as available broadcasts of real-time interviews by phone or in person through VNN, to understand what messages were (or would have been) delivered to the public, by whom and when.

2. Background

The first emergency public information challenges during the Full-Scale Exercise (FSE) arose in the wake of the unexplained explosion around noon on May 12, 2003, in the South of Downtown district of Seattle. The Mayor of Seattle, the Fire Chief, the Police Chief, and the Public Health Seattle/King County (PHSKC) Director held their first press conference 60 minutes after the explosion. The Mayor confirmed the presence of radiation in the explosion area and the PHSKC Director issued guidance to shelter-in-place in the central business district and other areas in the

vicinity. They instructed the public who may have been exposed to radiation to remove clothes, shower/bathe, lather, and not to consume food or water in the affected area.

Thirty minutes later a Seattle spokesperson announced the activation of the Seattle Emergency Operations Center (EOC). The public was urged to avoid areas within one mile of two cross streets in the affected area. Although it was not broadcast on VNN, Washington State released an announcement in this same timeframe noting the activation of the State EOC, outlining the State's role to monitor the situation, and reminding the public not to call 911 except for life-threatening emergencies.

The Department of Homeland Security (DHS) did not make a public statement about the explosion until nearly eight hours after the attack when DHS Secretary Ridge announced the elevation of the Homeland Security Advisory System Threat Condition to Red for seven cities. This may have been artificiality, but it is noteworthy.

In Illinois, public information challenges arose when the first patients began reporting to area hospitals with mysterious flu-like symptoms. The Mayor of Chicago addressed the city in the aftermath of the radiological dispersal device (RDD) explosion and instructed the city that the government was on higher alert. However, the bioterrorism attack had already occurred with releases in three locations on May 12, 2003. The Governor was the first to address the state and the nation regarding the outbreak of plague on May 13, 2003.

During the T2 building-block activities leading up to the FSE, but particularly in the seminar on emergency public information, participants identified numerous issues regarding public information. Many of these played out during the FSE. Examples include speaking with one voice, the need for more coordination on public health messages at all levels of government, finding the right contact in an organization, and the need for cross-border communications and coordination.

Participants in the building-block activities also cited concerns with public information related to the HSAS threat level. They mentioned the need to better understand what type of threat information to give to the public, the need to provide protective action guidance with threat levels, the need to balance threat fatigue with heightened anxiety, and the need to effectively handle the first hours of an attack before a Joint Information Center (JIC) can be established. Other concerns included managing rumors, the importance of clear and consistent messages from multiple spokespersons, the need to provide credible explanations for restrictive public policy decisions such as quarantines, and the need for accurate information to support decision-makers.

Table 12 depicts the challenges and good practices relevant to *Emergency Public Information* that arose in the seminars, as well as the instances that show how these issues played out during the FSE. Instances are occurrences experienced by participants during the FSE that indicate challenges or good practices associated with particular issues. In the table, a (-) is used to indicate challenge, and a (+) indicates a good practice. A ( ) is used to indicate a neutral observation in the FSE—one that is neither a good practice nor an issue. *Good practices* are those practices that players felt were effective, or that the data indicate worked well;[129] these practices could potentially be explored further or promulgated on a broader scale. *Challenges*

[129] References in the table are based on specific references in the data. Just because something is not specified as a good practice does not mean it did not go well in participants' opinions or did not happen.

are examples of the T2 response that were difficult for the responder community and which had significant impact on decision-makers. Challenges do not imply wrong actions or incorrect responses by any organization or the community at large—this After Action Report (AAR) and the analysis as a whole did not focus on evaluating right and wrong actions. Challenges require the continued attention of the national response community to facilitate smoother responses in the future.

Table 12. Emergency Public Information Issues during T2

ISSUES	SEMINARS/LSG					FSE INSTANCES GOOD PRACTICES AND CHALLENGES
	Emergency Public Information	*Radiological Dispersal Device*	*Bioterrorism*	*Direction & Control*	*Large-Scale Game Consequences*	
a. Managing rumors, conflicts, and misinformation.	✓	✓	✓	✓	✓	(+) State and local agencies in Washington and Illinois contacted the Virtual News Network to dispel rumors. (+) City of Seattle appeared to give hourly press conferences.
b. "Speaking with one voice"—one message/multiple spokespersons.	✓	✓		✓	✓	(+) The Principle Federal Officials in Washington and Illinois emphasized the need for one message, and consistency with State and locals. (+) City/County/State joint press conferences were held in Illinois and Washington. (+) Regional Joint Information Center (JIC) in Washington and "joint" releases in Illinois. (-) Multiple phone numbers given for information in both venues. (-) Conflicting messages given by different officials and agencies. (-) Little coordination between Federal agencies and State/local JICs. (-) Inconsistent messages from City/County on safety of perimeter zone and food/water safety in Washington. (-) City/County and Federal messages had different themes about the radiological dispersal device. (+)Agencies in both Washington and Illinois used information provided by the Centers for Disease Control and Prevention's (CDC) Health Alert Network (HAN) and other CDC sources.
c. Maintaining spokesperson credibility.	✓		✓	✓		Not exercised.

ISSUES	SEMINARS/LSG					FSE INSTANCES GOOD PRACTICES AND CHALLENGES
	Emergency Public Information	*Radiological Dispersal Device*	*Bioterrorism*	*Direction & Control*	*Large-Scale Game Consequences*	
d. Providing consistent Protective Action Guidance (PAG) for threat elevations and explanations of rationale for both PAGs and threat elevations.	✓	✓			✓	(+) Rationale for shelter-in-place messages appeared to make sense, but later inconsistencies may have complicated things. (+) Rationale for "snow day[130]" guidance in Illinois made sense based upon disease transmission information. (+) Consistent messages in Washington regarding the shelter-in-place orders. (+) Chicago Mayor/Office Emergency Management explained protective actions for Red, and why more info could not be shared (security). (-) Very little guidance was given to the public in both national elevations to Red. (-) Little explanation for why entire country was elevated to Red. (-) Radiation guidance to public in WA was to shower, bag clothes, stay inside; but health workers were told to wear masks. (-) Plague guidance to public in Illinois was to stay inside and avoid those with symptoms, bnt health workers were told to wear masks. (-) Inconsistent treatment guidance for plague transmission: Illinois Department of Public Health (IDPH): Surgical masks; the CDC: Masks may not be necessary; the Department of Homeland Security (DHS): N-95 masks, goggles, glasses for healthcare workers. (-) Inconsistent messages on transmissibility of Pneumonic Plague (Ridge: "not contagious person to person"; CDC: "extremely transmissible," CDC and IDPH: six feet; Canada: three feet.
e. Handling early post-attack information when information is limited (pre-JIC). .	✓		✓	✓		(+) Top Officials at all levels appeared forthright about what wasn't known. (-)Some statements were made prematurely and were changed later.

[130] As used during T2, the phrase "snow-day" was to indicate that the public was to stay at home as if they were impacted by a major snow storm.

ISSUES	SEMINARS/LSG					FSE INSTANCES GOOD PRACTICES AND CHALLENGES
	Emergency Public Information	*Radiological Dispersal Device*	*Bioterrorism*	*Direction & Control*	*Large-Scale Game Consequences*	
						(-) Shelter-in-place zone had to be expanded.
f. Having pre-coordinated information packages.	✓			✓	✓	(-) Some agencies (e.g., CDC, City of Seattle) had pre-packaged material to disseminate or upload onto their website, but these packages were not coordinated with other agencies. *Agencies acknowledged in Hotwashes that this would have been helpful.* (+/-) Public Affairs staff in the Illinois State EOC Office of Human Services worked aggressively to anticipate questions the public would ask to coordinate answers. However, this coordination occurred after plague had broken out.
g. Ensuring accuracy.	✓			✓		( ) Attempts were made to ensure accuracy of information but coordination was extremely difficult. (+) Seattle/King County coordinated with City of Chicago for information sharing.
h. Coordinating cross-border messages.	✓			✓		Not played enough to assess.
i. Handling intense media pressure.				✓	✓	NA: Not played.
j. Balancing public information needs with national security needs.		✓				Not sufficiently played to assess.
k. Minimizing unintended consequences: (i.e., the worried-well).		✓				(-) Washington information was not sufficiently clear to avoid potential floods of worried well—especially since radiation is invisible. (+) Clear messages in Illinois on potential infected: At release site or person-to-person contact with symptomatic people. (-) Attempts to require proof of presence at release sites (Chicago/DuPage County).
l. NEW: Unclear language.						(-) Different technical terms used by spokespeople with no explanation. (-) Confirmation of diagnosis of non-specific "plague" by top officials. (-) Unclear distinction between essential/non-essential workers.

a. Managing rumors, conflicts, and misinformation

The artificiality of VNN, coupled with both the standard and large-scale information coordination issues experienced during any crisis, combined to create conditions where participants were able to exercise this challenge during T2 play. Rumors abounded during the FSE as they would in any real life crisis, and determining which rumors were true during the FSE proved no less challenging in many cases. For reasons that can be attributed to both the artificiality of VNN and information coordination issues, VNN carried information that was not always accurate. For example, on May 14, 2003, at 0945 Eastern Standard Time, the Department of Health and Human Services (HHS) was concerned that VNN was running numbers on plague casualties that were inconsistent with those given by their Secretary's Emergency Response Team (SERT). HHS public affairs contacted VNN to correct this. Coordination occurred between the State health department and Interagency JIC, and the City of Chicago held a press conference to attempt to correct this inconsistency. In the end, the explanation for the erroneous numbers was an artificiality: VNN stated that it was instructed to only report numbers that the Master Control Cell (MCC) gave them. But the exercise in rumor control was a valuable one. In Illinois, the Chicago Office of Emergency Management (OEM) contacted VNN to correct the address of one of the distribution sites that had been broadcast incorrectly.

"Top Ten" Rumors in FSE Play*

1. There was a secondary explosion.
2. Air samples detected Strontium in the RDD.
3. **There are staff absences in Chicago hospitals.**
4. The Chicago airport is closed.
5. 18 Chicago hospitals are on virtual closure.
6. T2 exercise temporarily stopped in Chicago area on 5/14.
7. **Prussian blue was delivered to Seattle.**
8. The threat level was elevated for the nation at 1600 hours EDT on May 12.
9. Prussian blue is a protective paint.
10. **The RDD explosion occurred at noon on May 12.**

**Bolded rumors were true and others were false.*

In contrast, another rumor that was broadcast on VNN proved to be due to player actions—the rumor that Prussian Blue was being delivered at the request of the state. In fact, the state did not request Prussian Blue; the origin of this rumor was DHS, the Federal Drug Administration (FDA), and Federal agencies that were arranging for the delivery of this treatment through the Strategic National Stockpile (SNS). Participants at the Interagency JIC and the State EOC acted to dispel this rumor by contacting VNN, as well as Federal agencies in Washington, D.C.

The Washington State EOC called VNN to correct erroneous reporting that hospitals were overwhelmed. Seattle and King County attempted to dispel rumors on VNN regarding Marshal Law being considered (it was not). Finally, some organizations held hourly press conferences that would have been effective in helping to maintain a constant stream of "official" messages to the public. One agency, the Environmental Protection Agency, even had a rumor board to track down and validate rumors.

b. Speaking with one voice—one message/multiple spokespersons

Not surprisingly, speaking with one voice proved to be one of the greatest emergency public information challenges experienced by participants. Table 13 depicts the many public information voices of various organizations over the course of the FSE.[131]

Table 13. Active Voices in Public Information during T2 FSE

ORGANIZATION	5/12/03	5/13/03	5/14/03	5/15/03
Washington Venue				
Washington State Emergency Operations Center (EOC)	■	■		
Seattle EOC	■	■		
Seattle-King County Regional Joint Information Center (JIC)	■	■		
King County JIC	■	■		
Washington Department of Public Health (DPH)	■			
Washington State Ferry	■			
Seattle Police	■			
Harborview Medical Center	■			
Federal Bureau of Investigation (FBI) JIC	■	■		
Federal/Interagency Venue				
Headquarters Department of Homeland Security (DHS)	■	■	■	■
DHS/Federal Emergency Management Agency (FEMA)			■	■
Headquarters Department of Health and Human Services (HHS)		■	■	■
HHS/Centers for Disease Control and Prevention (CDC)				■
HHS/Federal Drug Administration (FDA)		■	■	■

[131] This table presents representative set of organizations that prepared or delivered messages for the public based upon press releases submitted at the close of the FSE and the VNN interview record. It does not necessarily reflect all organizations preparing such messages nor necessarily account for every day the depicted organizations were preparing such messages.

ORGANIZATION	5/12/03	5/13/03	5/14/03	5/15/03
FBI				■
Department of State			■	
FDA		■		
Department of Labor/ Occupational Safety and Health Administration			■	
State of Illinois Venue				
DHS-Chicago			■	■
FBI-Chicago				■
Office of the Governor		■	■	■
Illinois Emergency Management Agency		■		■
Illinois Department of Public Health			■	■
Illinois State Police			■	■
Regional JIC		■	■	■
City of Chicago/Office of Emergency Management	■	■	■	
Chicago Department of Public Health			■	■
Cook County Department of Public Health			■	
Kane County Department of Public Health			■	
DuPage County Department of Public Health	■	■	■	■
Lake County Department of Public Health			■	

While both venues implemented regional JIC concepts, the organizations shown in the table produced at least one independent press release. As many participants pointed out in the seminars, multiple spokespersons are to be expected in an event of the magnitude any weapons of mass destruction (WMD) attack would produce, and that is not necessarily problematic. In an emergency of the scale and psychological impact of a terrorist WMD attack, it is critical that government spokespeople speak with one voice and have a consistent message. But having one government voice is usually easier said than done and is an issue of coordination as much, or more, than one of politics.

During T2 there were instances of good coordination between Federal, State, and local government organizations in both the radiological and bioterrorism public information campaigns. In Washington, leaders were consistent with the public guidance to shelter-in-place following the radiological attack. They were generally consistent with protective action guidance to remove and bag clothes, take a warm shower, lather, and remain indoors. Jurisdictions were consistent with messages regarding transportation closures. In Illinois, leaders were consistent with messages telling people to seek emergency medical care immediately if they believed they were exposed to plague or were symptomatic. The leaders in Illinois were also consistent with transportation closure messages. Leaders at all levels attempted to reassure the public that the communities would get through this difficult and frightening time, and to remain calm.

There are numerous instances of organizations coordinating within and between JICs and reaching out from local to State to Federal levels. In both venues, the Principle Federal Official (PFO) from DHS emphasized and worked for a consistent federal message that was consistent with the State and local messages. In some cases, joint press conferences were held with representatives from the Washington State, the City of Seattle, King County, the JIC, and others.

However, there were a number of occasions where different voices were providing different messages—a fact that likely would have caused confusion. Tables 14 and 15 highlight messages that were conveyed via press releases from various organizations in Washington and Illinois. The messages were in five areas: relative danger, where to obtain information, protective action guidance, guidance regarding the red threat condition, and how to know if you were contaminated.

In Washington, the public was given five different phone numbers and at least two websites at various times for information relating to the RDD attack by organizations including the American Red Cross, the City of Seattle, Federal Emergency Management Agency (FEMA), King County, and Washington State. While each number may have served a distinct purpose, it was difficult to know for sure what number to call for what purpose, and they were not released as a coordinated "joint" set.

Finally, the Regional Disaster Plan signed by numerous agencies in the City of Seattle and King County designates the City of Seattle as the lead agency for a regional JIC. The City established a JIC at its EOC to which King County sent a representative. King County however, also established at least one JIC and proceeded to release messages independent of the City of Seattle that were not always coordinated. This contributed to inconsistent messages to the public.

Table 14. Public Messages in the State of Washington

Message Categories	Regional JIC	City of Seattle	King County IC	WA State	FBI JIC	FEMA	DHS	CDC[132]	FDA	American Red Cross
Relative Danger[133]	Low	Medium	Low	Medium	NA	NA	High	NA	NA	
Where to get information	General Information: 866-4CRISIS	General Information: General Information: 800-555 HELP	General Information: 866-4CRISIS Crisis Clinic: 206-461-3200 King County Employees: 206-205-8600 Road Conditions: 206-296-8100 800-695-ROAD Schools: http://www.schoolreport.org www.govlink.org Sound Transit : 888-889-6368 www.soundtransit.org Water Taxi Information: (206) 553-3000 888-808-7977		877-940-4700 (tips)	www.fema.gov.	NA	NA	NA	866-GET-INFO 206-323-2345 www.redcross.org
Protective Action Guidance	Shelter-in-place Shower Bag clothes Don't consume food/ water	Shelter-in-place Shower Bag clothes Don't consume food/ water	Shelter-in-place Shower Bag clothes Don't consume food/water	Shelter-in-place Shower Bag clothes Don't consume food/ water	NA	NA	NA	Prussian Blue	Prussian Blue	866-GET-INFO www.redcross.org
Guidance on Condition Red							Avoid public gatherings Don't go to school/ church.			866-GET-INFO www.redcross.org
How to know if you might be contaminated	You'd be sheltering.	You'd be sheltering.	You'd be sheltering.	You'd be sheltering.						

[132] The Centers for Disease Control and Prevention (CDC) provided notional support to the states via its Health Alert Network (HAN) and their website. HAN messages do not go directly to the public; rather they are provided to State and local health departments, other government agencies, and medical organizations to support public information by those agencies. The T2 analysts did not have data from CDC's website.

[133] "Relative danger" refers to the relative overall danger of the RDD explosion that was conveyed to the public through various agencies/organizations.

The PHSKC Director stated at 1715 Pacific Daylight Time (PDT) on May 12, 2003, in a press conference that there are "little to no long-term health risks from this type of bomb" and that this was "not a health emergency." Twenty minutes earlier, however, a Washington State Department of Health (DOH) spokesperson stated in a VNN interview that it was "too soon to tell" if there is danger in the downtown area. The type of bomb was not known yet (he had previously stated that officials were still trying to determine exact "radiological isotopes") so the risks were still unknown. In another example, citizens were at first advised that the water was not safe and to only consume water in closed containers. Later that day, the Mayor declared the water system was safe. But more messages followed from the PHSKC, again instructing the public to only drink water in closed containers and to not let pets drink water from outside. Concerns regarding runoff of contaminated water were raised by health and environmental agencies, concerns which were later determined not be an issue.

In addition, Federal agencies such as the FDA appeared to be releasing messages regarding Prussian Blue, a radiation treatment for Cesium exposure, that were not coordinated with the State and locals officials in Washington. At 1800 PDT on May 12, 2003, the DHS Secretary announced on VNN that Department of Energy (DOE) would be delivering unspecified medications from national stockpiles. Federal agencies began coordinating the deployment of Prussian Blue by around 1300 PDT on May 12, 2003. While its deployment may be automatic with DOE as a resource for first responders, neither the local responders nor the State expected to need it or use it for the general public. To that extent, public announcements regarding it were not synchronized with other messages coming in from State and locals regarding the severity of the radiation contamination. The Washington State EOC and the Interagency JIC expressed frustration about DHS "making local announcements."

During the first six hours of the RDD in Seattle, messages from the City, County, State, and Federal spokespeople effectively carried different themes. The city's messages conveyed a disaster of a serious enough scale that a number of emergency public policies had been implemented, yet they conveyed the idea that sheltering-in-place was sufficient protection. The county's messages attempted to reassure the public that there was nothing to worry about and that there were little to no long-term health risks. Finally, DHS Secretary Ridge reported on VNN, six hours into the disaster, that "we're sending the National Stockpile" conveying a potential disaster of a sufficiently large scale that local resources were already overwhelmed.

In Illinois, messages appeared to be closely coordinated between State and local governments. The collar counties and the City of Chicago produced regular joint releases. Independently produced press releases by jurisdictions were rare. Overall, this resulted in consistent messages regarding instructions to the public and key themes: seek immediate treatment if symptomatic, remain calm, and Pneumonic Plague is contagious and serious but highly treatable. They released a set of information numbers for the public to use, with one number for each jurisdiction. However, there were some inconsistencies among jurisdictions regarding which antibiotics would be effective. The City of Chicago stated that Doxycycline was the treatment being used, Illinois mentioned the same medication and Ciprofloxacin, and the Centers for Disease Control and Prevention (CDC) mentioned four other antibiotics but not Ciprofloxacin or Doxycycline. The dominant guidance to the public, however, was to seek emergency treatment immediately if individuals believed they were exposed, so these inconsistencies might not have had dramatic effects.

Table 15. Public Messages in the State of Illinois

Message Categories	City of Chicago	State of IL (IDPH)	"Joint" City/ County	Cook County	DuPage County	Kane County	Lake County	FBI	FEMA	American Red Cross	CDC
Prognosis	Deadly but treatable with antibiotics							NA	NA	NA	Deadly but treatable with antibiotics
Where to get information	312-743-INFO Animal Health: 217-782-4944	www.State.il.us/idph-dr/topoff_2 866-TOPOFF2		888-555-CURE	630-682-7000	800-555-6337	847-377-8130	877-940-4700 (tips)	800-621-FEMA	866-GET-INFO www.redcross.org	
Protective Action Guidance	Antibiotics: *Doxycycline* Cover mouth when cough/sneeze Who should get Antibiotics: (5/14) Only those exposed to release site (proof required) (5/15) Exposed to site or close contact with those directly exposed to site	Antibiotics: Doxycycline /Cipro Who should get Antibiotics: (5/13) Exposed to symptomatic persons. (5/14) Exposed to site or to symptomatic person.	Who should get Antibiotics: (5/14) Only those with symptoms should seek medical treatment, otherwise monitor condition. (5/15) Exposed to site or to symptomatic person	See "Joint."	(5/12) Who should get Anti-biotics: Exposed to site or to sympto-matic person	(5/14) Who should get Anti-biotics: Exposed to site or to sympto-matic person	See "Joint."	NA	NA	NA	Antibiotics: *Streptomycin* *Gentamicin* *Tetracycline* *Fluoro-quinolone* Disposable surgical masks
Guidance on Condition Red	Stay indoors.						NA		NA	NA	866-GET-INFO www.redcross.org
How to know if you might be contaminated	Exposure to one of release sites: (Terminal 3; later 2; later Int'l, which is terminal 5) 6 feet of symptomatic	Exposure to one of release sites (Terminal 3; later 2; later Int'l, which is terminal 5) 6 feet of symptomatic					Exposure to Int'l terminal				Exposure to release site/6 feet of symptomatic

Also, there is some evidence of inconsistent guidance to the public as to who should seek antibiotic treatment, as there were up to four different messages given to the public:

- Only those directly exposed to the release sites or to symptomatic persons should seek antibiotic treatment;
- Only those who are symptomatic should seek antibiotic treatment;
- Only those who were directly exposed to release sites, or in close contact with those who were; and
- Pre-exposed persons considered at high-risk should seek antibiotic treatment (only one organization referenced this).

There was further inconsistency in messages citing the release sites relative to O'Hare International Airport. Some organizations cited the affected Terminal as Terminal 2, later changing it to Terminal 3 and later calling it the International Terminal (which is Terminal 5). At least one organization referred to the International Terminal as Terminal 3. At one point controllers advised at least one organization to use Terminal 2. There was also inconsistency in the guidance as to what information people should bring with them to the SNS dispensing sites. Only the City of Chicago and DuPage County appeared to publish such guidance, advising people to come prepared with personal and family identification, and information on drug allergies, pregnancy status, and use of contraceptive (City of Chicago only), weight and age of children, whether women are breastfeeding (City of Chicago only), and current medications and general health status (DuPage County only). One would expect to see this comprehensive checklist widely and consistently disseminated.

One message that did not appear to come out strongly or consistently was that of the potential need for surgical masks. Medical community communications reflect the critical importance of N-95 masks[134] in reducing the transmission of plague, even specifying that other commercially available masks would not be effective. However, masks were rarely mentioned in the press releases, and the specific N-95 mask was not mentioned at all. Medical communications also reflected concern that there might be a shortage of this type of mask due to the recent Severe Acute Respiratory Syndrome (SARS) outbreak, but this did not appear to be addressed in the media. In DuPage County, the EOC eventually arranged for a large order of N-95 masks for county hospitals.

The PFOs in both venues observed the lack of Federal agency coordination of messages with State and local governments when they arrived, and acted to improve this. The PFO in Washington noted concern about "unilateral messages from D.C." and that no messages had come to the JIC despite critical decisions such as the seven-city elevation to Red, road/airport closures, and the restriction of border crossings from U.S. Customs. The exercise did not play out long enough in either venue to see how the PFO affect this information flow, but the PFO role has the potential to strengthen and streamline the flow of key information between the State and local governments and Federal agencies during a disaster.

[134] N-95 masks are fitted surgical masks that provide protection against particulate inhalation of contagious biological agents.

c. Maintaining spokesperson credibility

Mr. Frank Sesno, former Washington Bureau Chief for CNN, alerted participants during the *Direction and Control Seminar* to be aware that the media will "follow you down your own dead ends" and report it. Fortunately, participants did not have to contend with this reality during FSE play since there was no active mock-media. For this reason, there was not sufficient data for this area to be addressed.

d. Providing consistent Protective Action Guidance and threat elevation guidance

Determining how much information to release regarding the rationale for threat elevations is a particularly challenging for decision-makers. Balancing the public's need to know and understand certain information to ensure the overall protective posture is indeed elevated, can risk compromising national security. At the After Action Conference, participants voiced strong concerns regarding the lack of specific intelligence from official Federal to State and local channels regarding the nature of the threats or the rationale for threat elevations. In many cases specific information may not be known, but sufficient general intelligence exists to merit an increase in the nation's threat posture. In other cases, classification requirements limit information that can be transmitted from the intelligence community to State and local governments. DHS is currently examining this issue.

During T2, little public information was given to explain the rationale for the threat elevations to Red. In fact, public announcements regarding the threat elevations were fairly confusing (See the "Alerts and Alerting" *Special Topic*), often leaving even government officials uncertain about the alert status of their jurisdictions.

The rationale for the regional Seattle-King County elevation to Red was probably self-evident because terrorism was formally suspected by the time of the announcement. In the seven-city elevation, DHS Secretary Ridge explained the decision as an action to take additional preventative action, based upon both the RDD attack and intelligence that suggested the listed cities may be at extreme risk. On May 13, 2003, when the DHS Secretary elevated the nation to Red, it was in response to the mounting cases of plague in Illinois and Canada. The public was advised to avoid public gathering places, such as churches, schools, and work for 48 hours. However, there was no mention as to why people in Topeka, Kansas, were at as great of a risk of attack as those in perceived high-risk areas such as Chicago or New York City.

In examining the Protective Action Guidance (PAG) messages that were prepared for public release, one issue that emerged was that the recommendations provided to the public were not comprehensive. Just after 1300 PDT on May 12, 2003, in a joint news conference held by the City of Seattle and King County, the public was advised that food and water in the area or that "may have been exposed" should not be consumed. No guidance was given at that time as to what food or water sources may have been exposed or how the public could tell. Later it was clarified that food or water in sealed containers, or food that was indoors, was safe to consume. A news release from the City of Seattle at 1330 PDT on May 12, 2003, advised that "most people" will not experience long-term health effects, but it also advised people to "not take in additional radiation." It did not clarify who might be at risk for such effects or what it meant to "take in radiation," which could appear to imply ingestion or inhalation. It advised people to follow the directions of officials who might decide to evacuate people from the immediate area, arrange medical treatment for those injured by the blast, and decontaminate those who were

contaminated, but it did not specify how one would know if they were contaminated. In fact, other messages stated that exposed people (even at the site) would not necessarily feel sick and noted that radiation cannot be seen. This could have led to an increase in the numbers of worried well and undermined the credibility of the spokespeople trying to reassure the public.

The news that evacuations were potentially being considered could have been problematic at a time when people were also being advised to shelter-in-place without the additional clarification that evacuations were intended as a safe and structured means to move those sheltering-in-place. Also, initial messages instructed the public not to call 911 except to report life-threatening emergencies; however, an alternate number was not offered until almost 90 minutes after the blast. Similarly, the public was instructed at first to shelter-in-place, take a warm shower, and bag potentially contaminated clothes. Ninety minutes after the first message, they were instructed to close windows and turn off ventilation systems, and bring pets inside and bathe them.

In Illinois, people were advised that Pneumonic Plague was potentially highly contagious through the inhalation of respiratory droplets. People could contract the illness if they were in close contact, which was defined as within six feet of an infected and symptomatic person. They were advised to stay home if possible, though essential workers were instructed to report to work. But only one jurisdiction specifically advised people to cover mouths when coughing/sneezing, and, during the first day of play, no jurisdictions mentioned wearing masks as an additional protective action measure. When the additional protective measure to wear masks was mentioned the next day, the commercial surgical masks were recommended, though health community e-mails indicated that only the N-95 masks were considered effective.

e. Handling early post-attack information when information is limited (pre-Joint Information Center)

In any disaster, particularly one involving a possible terrorist WMD attack, there is much that is unknown in the early hours after the incident, including:

- Whether the event is indeed a terrorist attack;
- Whether there will be other attacks; and
- The extent of the damage—particularly from radiological weapons or bioterrorism.

In the seminars, participants emphasized the importance of early and visible leadership from top officials. In Washington, the Mayor of Seattle was on the news within 60 minutes of blast. He confirmed radiation early on and issued shelter-in-place guidance to those in potentially contaminated areas. Those outside the defined area were told that they did not need to shelter-in-place. A combination of factors, such as confusion among agencies in determining the range and types of radiation (see the "Data Coordination" *Special Topic*), as well as changing environmental factors, changed the parameters of the contaminated area over time. This caused decision-makers in the Washington venue to enlarge the shelter-in-place and exclusionary zones.

In Illinois, the Mayor of Chicago addressed the city after the threat condition was raised to Red (the address was pre-taped), and the Governor addressed the State the same day that the epidemic of plague became evident. However, some key messages were delivered much later. For example, the news that plague can be transmitted through symptomatic people was given 24 hours after the first announcement. The public was not advised until May 15, 2003, about the

transmissibility of Pneumonic Plague through cats and about prophylaxis options. Also, immediate guidance was given instructing people to seek medical treatment if symptomatic, but specific antibiotic options were not formally mentioned.

f. Having pre-coordinated information packages

The suggestion for pre-coordinated, agent-specific information packages was made numerous times in the various seminars and the game preceding the FSE. While some agencies appeared to have some fact sheets, neither Illinois nor Washington appeared to have a robust set of pre-coordinated, agent-specific, off-the-shelf information packages. The City of Seattle did direct the public to its website (www.seattle.gov), where it later clarified that fact sheets on dirty bombs, radiation, self-care in times of crisis, and disaster planning and personal preparedness were made available; no public official or press release ever referenced these fact sheets or the availability of fact sheets in general. Public Affairs staff in the Illinois State EOC Office of Human Services worked aggressively to anticipate questions the public would ask and to coordinate a set of answers. However, this coordination occurred after the plague had broken out. The City of Chicago did produce a fact sheet on Pneumonic Plague that was sent out. Some Federal agencies, such as the CDC and the FDA, do maintain fact sheets but it was not clear which State or local agencies utilized them.

g. Ensuring accuracy

Ensuring complete accuracy of information in the midst of a crisis is extremely difficult. Decision-makers are constantly challenged to make decisions based upon imperfect information, and information that is changing (See the "Emergency Public Policy and Decision-making" *Core Area*). This is partly due to the rate at which a crisis unfolds, specifically those involving terrorist WMD, and partly due to issues with coordination and communication (See the Communications, Coordination, and Connectivity *Core Area*). However, as participants pointed out in the seminars, the importance of having as accurate an information-baseline as possible in an unfolding event cannot be understated.

During T2 there were challenges in maintaining accuracy of information. An example is the casualty counts at the RDD scene in WA. Casualty counts were mounting; yet a King County Public Information Officer, speaking for the regional JIC repeated twice in a May 12, 2003, press conference at 1600 PDT that there were "no casualties." By this time there were more than sixty casualties and two deaths were reported in the EOCs. In Illinois, this challenge was equally difficult, as the size of the plague epidemic was growing daily. Leaders in Illinois had a very difficult time confirming accurate information regarding patient counts and fatalities (See the "Hospital Play" *Special Topics*).

Confirming patient numbers in the unfolding bioterrorism event in Illinois proved to be a tremendous challenge for a number of reasons, not the least of which was the artificiality of VNN having been instructed to use pre-scripted numbers from the MCC, which conflicted with the numbers being confirmed by players in the Chicago OEM. While this was an artificiality, the resulting challenge for players was probably emblematic of what happens in the real world with the media and its influence on perceptions of reality.

Ensuring accurate information depends upon having structured, well-defined and robust information flow strategies, where information is accepted from pre-defined validated sources. Such strategies exist in numerous policies such as the Interim Federal Response Plan, but

implementation of them remains a challenge. Regional JIC concepts are a critical element of such a strategy. Twenty-first century communications technologies both enable and challenge these strategies as they eliminate limits of time, distance, and hierarchical structures.

h. Coordinating cross-border messages

There was not sufficient data on the U.S. side to analyze this issue.

i. Handling intense media pressnre

Because news-gathering and public reaction were not played during the T2 FSE, this issne could not he analyzed.

j. Balancing public information needs with national security requirements

This issue was not played in enough sufficient detail to be analyzed.

k. Balancing pnblic information needs with national secnrity needs

Because the intelligence process was notionally played during the T2 FSE, this issue could not be analyzed.

l. Minimizing unintended conseqnences

Minimizing unintended consequences is challenging by definition. Thorough coordination and clear, comprehensive, and consistent messages certainly help in this area. Because public reactions were not heavily played during the FSE, this area is difficult to assess based upon empirical data. However, there are some instances worth examining as they could have potentially resulted in unintended consequences.

On May 14, 2003, the Chicago DPH issued a press release announcing its distrihution plan for antibiotics. It stated that proof of presence at one of the three suspected release sites would be required as a condition for receiving prophylaxis to prevent the lines from being too long. This seemed strange under the circumstances where a) theoretically other unknown releases could have occurred or could have still heen occurring at that time—the nation was under Threat Condition Red; b) the majority of the infected victims by then were second generation cases who were in contact with people at the initial release sites. While this message was not formally retracted in the exercise, all jurisdictions in the Illinois venue had agreed by May 15, 2003, that anyone who showed up for treatment would not be turned away.

In both the RDD attack and the hioterrorism attack, managing the worried-well could have been a huge challenge for the public health and medical communities and public information officers. Clear and consistent guidance from credible spokespersons would be key to minimizing issues of the worried-well. Also, in the State of Washington, the exercise ended before officials were able to say with certainty what the potential long-term implications of any, or specific, radiation exposure might have been, thus limiting the ability to analyze this issue. But, little-to-no guidelines were offered to help people who believed they may have been exposed to radiation determine with assurance that they had not been exposed. This could have resulted in a flood of people to medical centers wanting to confirm whether they were contaminated.

m. Unclear language (new)

Language is critical in a time of crisis. Simple messages are especially important when seeking to maintain calm and invoke specific responses from the public. During T2, the use of technical language with little-to-no explanation proved to be a potential challenge for the audience. In Washington, terms such as *multiple alarm response*, *instrumentation to protect citizens*, *habitability check*, *external hazard*, and *not a health emergency* were used by various State and local spokespeople on the first day.

In contrast, the greatest language challenge for officials in the bioterrorism attack was one of being too vague. The IL Governor's initial speech confirmed the diagnosis of the mysterious respiratory illness as plague. The DHS Secretary, in his speech to the nation on VNN on May 13, 2003, opened by confirming that the mysterious illness in Illinois was plague, but did not specify the type of plague. Some Americans might have assumed he was referring to Bubonic Plague—the "Black Death" of the Middle Ages. In fact the participants at the Large-Scale Game assumed just that when the type of plague was not specified.

3. Conclusions

Emergency Public Information was a dominant theme in TOPOFF 2000 and emerged as a dominant issue during T2. It merited its own seminar, and participants raised concerns and identified issues in this area in every other seminar. It is not surprising that it emerged as an issue during the T2 FSE—unlike everyday public information, leaders in the midst of a disaster, especially one involving WMDs, are thrown into an environment of chaos where time and certainty compete, and the public's attention and demand for information are high. Often the public's safety is dependent on the effective communication and receipt of emergency messages. This produces an environment of great pressure on top officials to speak to the public and to release information—this may result in releasing information that could change, that has not necessarily been thoroughly coordinated, and that may not be consistent with other messages being released at the same time. The messages given to the public by officials are competing with a flood of non-official messages as well. Establishing consistent messages across all official spokespersons is key to maintaining credibility of official spokespeople and is one of the most effective ways to retain the public's attention regarding messages that may be critical to their safety.

Participants stated that the VNN element of the TOPOFF exercises was extremely valuable in simulating the realism of the media element. They have also said that they would like to continue to be challenged in the area of emergency public information through elements such as a robust news-gathering function and simulated public reactions. Many assumed that VNN was playing these functions during T2 when in fact it was not contracted to do so. It was intended primarily to lend an environment of realism to T2—not substitute for information sources. Interestingly, however, it is a parallel to the real world in which participants have acknowledged that they often rely on network news for information because formal channels are slow or nonexistent. The reconstruction of T2 illustrates the information validation issues that are multiplied when any media outlet substitutes for official channels of information.

The dominant issue that emerged from this area in the seminars and during the FSE remains one of coordination. Creating mechanisms that can support this coordination, in the midst of the chaos, is imperative. Ensuring accuracy of information is extremely difficult, and the

information will change. A consistent and comprehensive message that is based upon the best information available at the time should be the goal of top officials and their PIO staffs. The message should be consistent both within any jurisdiction or organization, and with all official public messages. The message should be delivered on a consistent and regular basis; this strategy appeared to be effective in the Maryland/Washington D.C./Virginia sniper incident and 9/11, and appeared to be effective in T2. These three elements—consistency, comprehensiveness, and the best information available at the time—are all required, and should be goals of future emergency public information campaigns.

The ability to achieve these goals in emergency public information depends upon having structured, well-defined, and robust information flow strategies, where information is accepted from pre-defined, validated sources. Such strategies do not exist currently in the national response domain, though regional JIC concepts are a critical element of such a strategy. But twenty-first century communications technologies make adhering to this critical strategy difficult as they eliminate limits of time, distance, and hierarchical structures. Ensuring accuracy of information, or at least as best as possible, depends on a comprehensive system whereby only information from identified sources is accepted as valid, regardless of whatever other information is received. A shared electronic information system could help to streamline information flow, and potentially reduce conflicting information. Ideas were raised in the seminars such as a regular news center concept and town hall meetings that may offer value as well.

The TOPOFF Exercise Series provides a unique opportunity for jurisdictions at all levels, to exercise, experiment with, and improve upon these critical strategies. T2 provided an opportunity for participants to showcase the value of concepts, such as regional JICs, that could be expanded for more comprehensive coordination at broader levels and in distributed environments (i.e., when people cannot be physically co-located). Future TOPOFFs should continue to allow participants to experiment in this area and should consider expanding on mock media functions and mock public response to further challenge participants.

This page intentionally left blank

C. Commnnications, Coordination, and Connectivity

1. Introduction

Nobody questions the importance of communications, coordination, and connectivity in a weapons of mass destruction (WMD) emergency response, and few would question that there are challenges that need to be overcome in this important area. These challenges are relevant in the everyday activities of Federal, State, and local (FSL) authorities, but take on critical importance during an emergency, especially one that involves WMD. While there were good practices during the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE), communications, coordination, and connectivity challenges emerged as dominant, if not the most dominant, challenges and pervaded almost every element of the response. For the purposes of this discussion, *communications* is defined as the exchange of information between agencies and jurisdictions, *coordination* is defined as agencies and jurisdictions working together to meet a common goal or to solve a common problem, and *connectivity* is defined as the means by which communication and coordination takes place. If *communication* describes the "what," *connectivity* describes the "how." The special topic areas provide extensive detail about many of the communications, coordination, and connectivity challenges including how they occurred, and, where possible, why they occurred.

2. Discussion of challenges and good practices

Table 16 depicts the challenges, and good practices relevant to communications, coordination, and connectivity that arose in the seminars, as well as the instances that show how these issues played out during the FSE. Instances are occurrences experienced by participants during the FSE that indicate challenges or good practices associated with particular issues. In the table, a (-) is used to indicate challenge, and a (+) indicates a good practice. A ( ) is used to indicate a neutral observation in the FSE—one that is neither a good practice nor an issue. *Good practices* are those practices that players felt were effective, or that the data indicate worked well;[135] these practices could potentially be explored further or promulgated on a broader scale. *Challenges* are examples of the T2 response that were difficult for the responder community and which had significant impact on decision-makers. Challenges do not imply wrong actions or incorrect responses by any organization or the community at large—this After Action Report (AAR) and the analysis as a whole did not focus on evaluating right and wrong actions. Challenges require continued attention of the national response community to facilitate smoother responses in the future.

[135] References in the table are based on specific references in the data. Just because something is not specified as a good practice does not mean it did not go well in participants' opinions or did not happen.

Table 16. Communications, Coordination and Connectivity Issues during T2

ISSUES	SEMINARS/LSG					FSE INSTANCES
	Emergency Public Information	*Radiological Dispersal Device*	*Bioterrorism*	*Direction & Control*	*Large-Scale Game Consequences*	GOOD PRACTICES AND CHALLENGES
a. Communication: • Processes are needed for distribution of critical information between agencies and jurisdictions and for communication of data and lab information to Incident Commander. • Communication of State and local Emergency Operations Centers (EOCs) with hospitals.	✓	✓	✓	✓	✓	(-) Lack of consistent understanding of formal, validated sources for information. (-) In some cases, lack of formal processes/channels (or understanding of them) for official information. (-) Inconsistent use of terms/unclear technical language. (-) Burdensome/redundant reporting processes for hospitals.
b. Coordination: • Integration of agencies to provide unified response is not clear. • Coordination across multiple agency and jurisdiction EOCs. • Lack of integration of private sector and non-profit organizations in response plans. • Cross-border/international coordination needed.		✓		✓	✓	(-) Multiple agencies collecting/disseminating radiological ground data in Washington. (+) The Principle Federal Official in both venues. (+) Video teleconferences (VTC) were an effective means of coordination. (+) In Washington and Illinois, there were several examples of EOCs working together to solve a problem (procedures for re-opening closed roads in Washington, identification of additional security personnel in Illinois). (+) American Red Cross participated in the Federal Joint Operations Center Consequence Management Group in Washington and at the Interagency level. (+) In Washington, preliminary relationships developed between businesses and emergency response community. (+) In Washington, Canada requested to place a liaison in the Region X Regional Operations Center (ROC). (+) The Department of Energy requested help from Canada on health radiation. (+) In Illinois, numerous examples of conference calls between EOCs and regional Federal agencies (typically the Department of Health and Human Services Regional EOC and the Federal Emergency Management Agency ROC).

ISSUES	SEMINARS/LSG					FSE INSTANCES GOOD PRACTICES AND CHALLENGES
	Emergency Public Information	*Radiological Dispersal Device*	*Bioterrorism*	*Direction & Control*	*Large-Scale Game Consequences*	
						(+) In the Interagency, many examples of Federal agencies communicating with each other. (-) Multiple EOCs stretch liaisons thin and can complicate coordination (+) Prior to the FSE, Washington Department of Health (DOH), Public Health Seattle King County (PHSKC), and EPA developed default Protective Action Guidelines for use in an RDD event.
c. **NEW**: Connectivity.						(-) In Washington, Radiation Monitoring and Assessment Center couldn't transmit data electronically; forced to used phone, fax, and courier. (-) In Washington, Federal Radiological Monitoring and Assessment Center used 56k modem to transmit information and courier to deliver maps to Joint Operations Center (JOC). (-) In Illinois, many hospital fax machines were unreliable, and there was no guarantee of successful data transfer. (-) Hospital data were largely paper-based and disparate reporting processes were burdensome. (-) In Washington, inadequate VTC capability at JOC.

a. Communication

To the extent that effective coordination depends on a common information baseline, communication issues are addressed. The volume of information exchanged by players during the T2 FSE was extensive. More than 2,500 e-mails alone were courtesy copied (as requested of participants by the T2 evaluation team for use in subsequent analysis) to the T2@amti.net address, and this is likely a fraction of the total volume of e-mails exchanged. This number does not include information exchanged by fax, phone, radio, video teleconference (VTC), in person, or obtained by participants over Websites. In response to a disaster, agencies produce multiple levels of information of various types: technical data that are assimilated into information from multiple sources, individual logs kept by staff at most Emergency Operations Centers (EOCs), organizational situation reports produced at regular intervals, summary briefings, and press releases to name a few.

Analysis of T2 communications affords a rare opportunity, albeit a limited one due to time constraints, to examine this critical element of national response in an objective and relatively comprehensive manner. Such an examination is only possible through the artificiality of an exercise that permits collection of the information flow that would be impossible to implement in a real disaster. This analysis represents the highest-level assessment of this critical area. Further examination of this area is strongly recommended to help the national response community understand the existing information system upon which their situational awareness depends, including the key information nodes, along with redundancies, gaps, or efficiencies.

During T2, there were two overarching communication issues:

- Lack of formal processes/channels (or understanding of them) for official information and lack of consistent understanding of formal, validated sources for information; and
- Use of inconsistent or technical language.

Lack of formal processes/channels (or understanding of them) for official information

A prevailing issue that emerged during T2 was the lack formal processes or channels for official information. In an environment of instantaneous information access through e-mail, pagers, instant messaging, and cell phones, adhering to a structured process for exchanging information is difficult. Structured processes may be slower than informal processes; however, they are a far more effective way of validating information than numerous informal processes. When validated information is critical, it is equally critical that mechanisms exist for exchanging it.

During T2, this played out in numerous ways. Agencies experienced difficulty in validating the status of the alert level for nearly 12 hours due in part to the absence of a consistently understood process for official notifications in this arena. As described in "Alerts and Alerting" in the *Special Topics* section, many agencies learned about the Department of Homeland Security (DHS) elevations through the Virtual New Network rather than through official channels. This led to substantial efforts to confirm and validate this information.

Some agencies attributed information problems to too many official reporting channels—various agencies having their own, independent procedures and redundantly requesting updates from agencies. Public health authorities in Illinois required updated resource reporting every three hours in the midst of the outbreak. In many cases, different agencies [(e.g., Illinois Department of Public Health [IDPH], Illinois Operations Headquarters and Notifications Office [IOHNO])] requested similar information in various formats from hospitals. These cumbersome reporting processes appeared to divert resources from other priorities.

The Federal Bureau of Investigation (FBI) Strategic Information Operations Center (SIOC) is staffed by liaisons from other Federal agencies. They are there to field questions, receive information from the FBI to pass back to their agency headquarters, and provide information to the FBI from their agency headquarters. However, in many cases during the FSE, agencies directly contacted the FBI information control officer for information rather than their own liaisons. This was particularly true of DHS.

T2 provided an unprecedented opportunity for traditional government response agencies to interact and work with the public health and medical communities. Hospitals reported that they established many positive working relationships with many FSL agencies. However, they

reported that numerous calls from a variety of people from the same Federal agencies caused some confusion.

Agencies spent substantial time validating rumors about transportation closures, patient numbers in both venues, casualty figures from the radiological dispersal device (RDD) scene, and others due in part to a lack of understanding of validated sources. For example, in the Washington venue, on-scene responders were repeatedly asked about the number of fatalities. Partly because of the "fog" and urgency of a disaster, responders attempted to provide what they knew, rather then defer to the Medical Examiner,[136] leading to inconsistent estimates of the number of dead. In other cases there was a lack of understanding by official sources as to the complete list of information consumers. Both contributed in to a "whisper down the line" phenomenon as information was passed from primary recipients through secondary channels to others who passed it along, unintentionally altering the information along the way as in the childhood game "Telephone."

Finally, there is some evidence to suggest that although many agencies, including DHS, initiated regular reporting intervals, not enough agencies did this. Those that requested "on-demand" reports often did not allow staff sufficient time to gather information. For example, a Department of Health and Human Services email notes that:

> *A request was made by the FBI Consequence Management Group Leader to have each agency provide talking points for a report to the Principle Federal Official, who will update the President of the United States. We had about 10 minutes to pull this information together, so I contacted ROC* [Regional Operations Center] *and REOC* [Regional Emergency Operations Center] *for assistance.*

While this individual sought out official sources for information, a ten-minute notice for updates across all major elements of a disaster response is a recipe for potential information issues.

Inconsistent use of terms/unclear technical language

The use of inconsistent language proved to be another communications challenge during the T2 FSE. In the Washington venue, confusion arose with the interchangeable use by many of the term *casualties* to mean both *fatalities* and *injuries*, or both. The "Emergency Public Information" discussion in the *Core Areas* section details some additional issues with the usage of language for public information. Some of these same examples were issues in internal agency communications. Specifically, the general reference in internal agency communications to the plague resulted in at least one instance of a public health person giving advice that applied to Bubonic Plague (preparing information to reduce transmission through rodent population) rather than Pneumonic Plague. Officials remarked about the critical importance of having technical data translated into plain language to support decision-making and risk communications.

b. Coordination

In the Illinois venue, the greatest challenge involved the coordination of actions, information, and data flow requirements among 64 hospitals, five POD hospitals, and three separate but inter-related state-wide organizations (IDPH, IOHNO, Illinois State EOC). In Washington, there were

[136] In Washington, the Medical Examiner is the formal source for confirming deaths.

many agencies collecting radiological ground data to assist in the determination of the extent and type of contamination caused by the RDD explosion. Early on, these agencies transmitted their data on-demand to numerous other agencies—in many cases by-passing the coordination processes and mechanism of the Federal Radiological Monitoring and Assessment Center (FRMAC). In some cases, these agencies were measuring slightly different things, though such differences were not necessarily understood by the recipients of this information, many of whom were not technical specialists. This proved to be problematic later on when these data were used by several different agencies to create inconsistent plume and deposition models.[137]

At the RDD site in Washington, there were some issues with the apparent lack of a unified command structure during the early stage of the response. Although, there were a number of briefings attended by the Seattle Police Department (SPD) Incident Commander, the Seattle Fire Department (SFD) Incident Commander, the FBI, and the Federal Emergency Management Agency (FEMA), there was no mention of a unified command to facilitate coordination efforts until 0915 on May 13, 2003.[138] However, even that briefing did not include representatives from health or emergency medical services, leaving full coordination nearly impossible.[139] A data collector commented after the exercise:

> *While all disciplines were present, there was no indication that they were truly working together. In fact, except for the briefings, the only interdisciplinary coordination occurred by "chance meetings..."*

An additional coordination problem arose with the DHS National Operations Center and the Washington State EOC regarding deployment of the DHS Prepositioned Equipment Package (PEP). On the second day of the FSE, the Incident Commander requested deployment of the PEP. Per the guidelines in the DHS/ODP PEP Briefing Book, a request for deployment of PEP from the Washington Governor, was processed through the Washington State EOC. The data show that attempts were made to follow established PEP guidelines; however, the guidelines were vague and did not provide sufficient detail. For example, the request for deployment must come from the Washington Governor, but it was not specified if a verbal request is sufficient or if the request should be in writing. The request was eventually routed through the FEMA liaison in the Washington State EOC. However, once the request reached the DHS National Operations Center, it was not processed because the responsible individual(s) or PEP Program staff could not be located. Additionally, the staff in the DHS Homeland Security Operations Center (HSOC) appeared not to be familiar with the PEP program or process. Thus, a major delay in deployment of the PEP was encountered, while the National Operations Center tried to locate someone who knew about this program. More detailed procedures employing the HSOC as the request point of entry and training from DHS for requesting deployment of the PEP could help to ameliorate this in the future.

[137] For more information, see "Data Collection and Coordination" in the *Special Topics* section.
[138] It is possible that a unified command was established before this time, but the evaluation team does not have any such data.
[139] It is also likely that this briefing or any other at this level did not include representatives from the technical agencies collecting radiological data since they were working for the Hazardous Materials Chief, not the Incident Commander. For more information, see the *Special Topic* on data coordination.

The presence of the Principle Federal Official (PFO) in both venues, but particularly in the Washington venue, proved to be an effective conduit for improving coordination among the multiple agencies and multiple governmental levels of response. Other good practices in coordination during the FSE included the following:

- There were several examples of agencies and jurisdictions coordinating to solve problems. For example, in Washington, the Seattle EOC worked with the Washington Department of Transportation and the Washington State Patrol to develop and implement a plan to decontaminate and re-open highways. In Illinois, the EOC structure proved valuable when the State EOC activated Illinois law enforcement mutual aid to provide Chicago additional security personnel in anticipation of a shortage of city workers;
- There are numerous examples in both Washington and Illinois of State, county, and local EOCs conducting conference calls and VTCs. In many cases, these conferences included regional representation of Federal agencies, including the regional FEMA Regional Operations Center (ROC). In both venues, the PFO also initiated regular conference calls with State and local top officials.[140] In the Interagency venue, both the SIOC and the DHS collected information from and distributed information to other Federal agencies. Federal agencies and departments also participated in conference calls and VTCs involving many different departments and agencies and communicated between agency headquarters in Washington, D.C., and their regional counterparts;
- During the FSE, there were several good practices of standardized information sharing. All FSL agencies with permission to access the Department of Energy (DOE) National Atmospheric Release Advisory Capabilities secure Internet site could download predictions of the radiological plume. Also in Washington, the Seattle and State EOCs shared information through an Internet-based system. However, neither the King County EOC nor Federal agencies had access to the system, which limited its value. In Illinois, DuPage County utilized the Pro-Net surveillance system to track hospital calls and admissions and to provide early alerts to possible disease outbreaks; and
- The FSE provided unusual opportunities for the inclusion of some organizations not typically included in response organizations. In Washington, the American Red Cross staffed the Seattle, King County, and Washington State EOCs, which is not unusual; however, they also staffed the Federal Joint Operations Center (JOC) which was unprecedented. Their national headquarters was also involved at the interagency level. Also in Washington, the Bank of America co-located an EOC with the Federal Reserve. Finally, the months of planning allowed Seattle businesses to develop or broaden relationships with the emergency response community. They are now in the process of establishing the Business Emergency Network (BEN) to increase the business community's awareness and involvement in emergency response.
- The need for advance coordination among agencies, such as the CDC and FDA, on the availability of medical countermeasures for humans and animals for other potential threat agents is critically important. The TOPOFF Exercise Series offered numerous opportunities to do this.

[140] For more information, see the *Special Topic* on the Principle Federal Official.

Exercise activities that took place in Canada are beyond the scope of this AAR, but there were several examples of U.S. communications and coordination with Canadian authorities. The International Office within DHS communicated regularly with Canadian government officials as well as government officials from other nations. In addition, after the RDD explosion, DOE Headquarters requested radiological assistance from Canada. As a result, Canadian officials asked to place a liaison in the Region X ROC.

c. Connectivity

A variety of means were used to communicate during the FSE. While there was an increasing use of Internet-based transmissions, there continued to be heavy reliance on faxes particularly in the case of the Illinois hospitals. Table 16 provides examples of some of the typical connectivity issues that arose during the exercise. An issue of concern at the federal level not indicated in the table was the difficulty some agencies had receiving and passing classified information.

One issue that was not identified during the seminars or the Large-Scale Game was the potential for technical challenges. During the FSE several such challenges arose. In Washington, the Department of Health Radiation Monitoring and Assessment Center had poor connectivity and was forced to distribute data primarily via phone, fax, and with a courier. The DOE FRMAC in Washington communicated with and transferred information to their servers in Nevada through a 56K modem, which they reported as much too slow and unreliable. The Advisory Team[141] also had technical limitations—they had one phone line, which was also their Internet connection.[142] In addition, the Federal JOC in Washington had inadequate VTC capabilities. All of these connectivity challenges had an impact on the ability of technical experts, agencies, and jurisdictions to communicate effectively.[143]

In Illinois, the lack of a robust emergency communications infrastructure was manifest by a reliance on telephones and faxes for patient data transmission. Often, however, the fax machines were unreliable and there was no certainty that the transfer was successful, or there was inadequate staff to monitor them. In addition, if the phone lines were compromised, then the distribution of data would be severely compromised.[144] While in some cases, these connectivity issues may have been due to the fiscal and physical constraints of the exercise, this was not always the case. Many organizations referenced the critical need for better, more robust connectivity (i.e., internet access) in their Lessons Learned reports.

3. Conclusion

As described in detail in the *Special Topics* section, the communications, coordination, and connectivity challenges had an impact on the information available to top officials, which in turn affected their ability to make decisions. In all three venues, top officials made decisions based

[141] The Advisory Team consists of representatives from Federal agencies and provides the lead Federal agency with advice on environmental, food, health, and safety issues that arise during and from a radiological emergency.
[142] The Federal Radiological Monitoring and Assessment Center and Advisory Team informed the evaluation team that these technical limitations are real-world—not exercise artificialities, as they set up wherever they find appropriate space. They reported working toward a mobile, high-speed system, but they have to be sure that it meets their technical and security needs.
[143] Because of a lack of coordination observed during the FSE, the connectivity challenges discussed above are the not the primary cause of the communication challenges observed during the FSE. For more information, see "Data Collection and Coordination", "Hospital Play", and Decisions Under Uncertainty" in the *Special Topics* section.
[144] For more information, see the *Special Topics* section on hospital play.

upon inconsistent and often incomplete information. Such inconsistencies also made it to the public (see the *Core Area* on public information), which has the potential to compromise the credibility of top officials. While better coordination and communications may not lead to better decisions, top officials should be confident that they are basing their decisions upon the most up-to-date and valid information available. Although it is doubtful that communications, coordination, and connectivity will ever be perfect, exercises, including the TOPOFF Exercise Series, can serve to identify areas where communications, coordination, and connectivity can be improved.

Although there were significant communications, coordination, and connectivity challenges during the FSE, players and planners reported that the building-block process allowed them to develop new or stronger relationships with their colleagues. Many have developed and implemented processes based upon their T2 experiences to improve their communications, coordination, and connectivity capabilities.

This page intentionally left blank

D. Jurisdiction

1. Introduction

Metropolitan-area providers of emergency services typically have interlocking mutual-aid agreements or emergency assistance compacts that clarify jurisdictional issues. But terrorist attacks using weapons of mass destruction (WMD) bring into play entities and considerations not normally encountered and not necessarily provided for in these agreements. Authorities that seem clear on paper are not always as clear in practice as real-world experiences and exercises repeatedly demonstrate. Previous exercises, such as Top Officials (TOPOFF) 2000, and real-world events, such as 9/11 and the anthrax attacks in 2001, highlighted such challenges. In this section, we examine the issues, conflicts, or gaps in jurisdictional authorities and the assumptions that arose when policies and agreements were put into practice under the uniquely challenging conditions of simulated terrorist WMD attacks.

2. Discussion of challenges and good practices

Participants raised and examined jurisdictional issues throughout the cycle of T2 including the FSE. Table 17 depicts the challenges, and good practices relevant to *Jurisdiction* that arose in the seminars, as well as the instances that show how these issues played out during the Full-Scale Exercise (FSE). Instances are occurrences experienced by participants during the FSE that indicate challenges or good practices associated with particular issues. In the table, a (-) is used to indicate challenge, and a (+) indicates a good practice. A ( ) is used to indicate a neutral observation in the FSE—one that is neither a good practice nor an issue. *Good practices* are those practices that players felt were effective, or that the data indicate worked well;[145] these practices could potentially be explored further or promulgated on a broader scale. *Challenges* are examples of the T2 response that were difficult for the responder community and which had significant impact on decision-makers. Challenges do not imply wrong actions or incorrect responses by any organization or the community at large—this After Action Report (AAR) and the analysis as a whole did not focus on evaluating right and wrong actions. Challenges require continued attention of the national response community to facilitate smoother responses in the future.

During the T2 FSE, there were many successes in the jurisdictional arena; however, the issues that were experienced emerged in two overarching areas:

- Confusion over who has authority for what actions/decisions; and
- Authority for the control and dissemination of information.

[145] References in the table are based on specific references in the data. Just because something is not specified as a good practice does not mean it did not go well in participants' opinions or did not happen.

Table 17. Jurisdiction Issues during T2

ISSUES	SEMINARS/LSG					FSE INSTANCES
	Emergency Public Information	*Radiological Dispersal Device*	*Bioterrorism*	*Direction & Control*	*Large-Scale Game Consequences*	GOOD PRACTICES AND CHALLENGES
a. Confusion over roles and authorities. Some agencies seem to have duplicative roles under certain circumstances. Plans are sometimes duplicative, or in conflict. Some authorities are unclear in bioterrorism response.	✓	✓	✓	✓		( ) Issues during the Full-Scale Exercise were less about disputes over who's in charge, but rather *who is in charge of what.* (-) Questions arose concerning the department of Homeland Security and its relationship with other agencies. (-) Some questions with implications of bioterrorism and the declaration of a public health emergency. (-) Some uncertainty regarding transportation authorities.
b. Authorities to release information.	✓	✓		✓		(+) Regional Joint Information Center concepts implemented. (-) Frustration at Federal agencies releasing "local" messages. (-) Control of information can have an impact on other activities. *See "Emergency Public Information" core area.*

a. Confusion over roles and authorities

The primary question relating to jurisdiction during the T2 series of activities evolved throughout the exercise cycle from *who is in charge* to *who is in charge of what.* Participants increasingly clarified that the issue in emergencies is often not turf battles, but rather uncertainty among the various entities involved in response to multiple, sometimes overlapping, authorities that are driving the numerous actions being simultaneously and urgently addressed. From a jurisdictional perspective, many things went more smoothly during T2 than participants expected. For example, during the post-FSE tabletop held in Seattle, the spokesperson from the City of Seattle stated: "During T2, I expected to see a chaos of power that would hamper the response effort—these expectations were profoundly unmet as all levels of government and agencies came together to respond to this crisis." This was exemplified by the transfer of control

of the RDD site in Washington, first to the Federal Bureau of Investigation (FBI) once Seattle Fire Department completed rescue and recovery operations, and then through the Federal Emergency Management Agency (FEMA) back to the local authorities when the FBI completed the crime scene investigation.

However, beyond the RDD incident site there were instances of agencies not knowing who had what authority to make certain decisions (see the "Emergency Decision-making and Public Policy" *Core Area*). For example, in Illinois there were multiple discussions regarding who was in charge of the decontamination process, who had the authority to re-open the facilities where plague was released (the United Center, O'Hare International Airport, and Union Station) and who had the authority to define the requirements that must be met to re-open the contaminated sites. This last point is particularly troublesome since it involves both an assessment of when it is scientifically "clean" versus be perceived as safe by the public. This issue was also relevant in Washington as long-term remediation and restoration of areas with radiological contamination is a significant public health and environmental protection challenge. These, and other long-term issues, were discussed among Federal, State, and local (FSL) agencies and departments in WA at the post-FSE tabletop on May 15, 2003.

Jurisdictional authorities related to transportation were also unclear during the FSE. During T2 some confusion arose among participants as to who had what authorities to close and re-open airspace, rail systems, and road systems. In the case of airspace, there was some confusion as to whether authority to close and re-open airspace and temporary flight restrictions lay with the newly-created Transportation Security Administration (TSA) or the Federal Aviation Administration (FAA). TSA and Veterans Administration logs indicate that TSA implemented a shutdown of airspace in the Seattle area, restricted flights, and closed airspace within 30 miles of the three area airports. Other logs from FEMA, Department of Transportation (DOT) Crisis Management Center, and FAA indicate that only FAA had this authority. There was also confusion regarding the authority to close airports. Some participants, including those from FEMA, believed that only DHS had this authority. In fact, the local airport authority has jurisdiction over the status of their local airports.

Discussions occurred within DOT about the legal authority of TSA to close rail systems (currently only private rail operators have this authority for freight, while DOT has some influence over Amtrak). In addition, FEMA reported to DHS that the U.S. Coast Guard (USCG) had closed down the Port of Chicago, and a DHS Crisis Action Team (CAT) log noted that the Customs and Border Patrol had closed the Port of Seattle—when actually, only the Captain of the Port has this authority (a USCG log notes this). The USCG clarified the authorities of the Captain of the Port at the Washington venue Hotwash noting that "knowledge of these authorities would be very helpful to emergency responders." These USCG authorities—to close the port, stop all work at all waterfront facilities, control all vessel movement including freezing them in place, to order vessels to leave, and require significant increases in security at private waterfront properties—take on potentially national and international significance within the context of a terrorist WMD attack.

There were also some issues about who could re-open road systems. In Washington, the City of Seattle's Mayor was anxious to restore the city to normalcy as soon after the attack as possible, and publicly announced that the roads would be opened at a specified time. However, this announcement had not been coordinated with the WA DOT, which has the statutory authority for these decisions. Based upon the guidance of the WA State Department of Health (DOH), WA

DOT did not agree with the Mayor's decision. The issue was coordinated and resolved in the end but led to hours of confusion by many agencies as to the status of major highways in the area.

The FSE provided a valuable opportunity to identify and explore potential jurisdictional questions relating to DHS' the newly merged federal assets. For example, in Illinois, some issues arose with the declaration of a public health emergency by the Department of Health and Human Services (HHS). Such a declaration gives HHS the authority to deploy resources on its own initiative and at its own cost. This led to some confusion among agencies concerning the status of the Strategic National Stockpile (SNS). The decision to deploy the SNS is made by DHS in coordination with HHS. During T2, the HHS headquarters and DHS officials both gave directives regarding the SNS; SNS deployed based on DHS directives. There was no apparent coordination between DHS and HHS headquarters regarding activation and deployment of the SNS; rather, coordination occurred between senior CDC and FEMA officials. This level of coordination limits the ability of both departments to effectively manage the full scope of assets available for the response effort.

DHS now maintains many of the medical response assets formerly maintained and managed by HHS such as the SNS and the NDMS. HHS is the lead technical agency for public health and medical emergencies, yet retained few operational assets to respond to such emergencies following the creation of DHS. Furthermore, the medical expertise required for effective management of these assets is split between the two departments. It is not clear from the FSE whether this would impact HHS' ability to manage a response following a declaration of a Public Health Emergency in the absence of a presidential disaster declaration—given that it doesn't retain operational control of response assets. Further, the FSE did not stress the federal system enough to analyze how difficult decisions regarding allocation of health and medical assets would be made.

FEMA Headquarters was challenged to refine their relationship with their new parent Department, DHS, during the FSE. One email suggested that the FEMA Emergency Support Team (EST) was not included in a teleconference with the DHS CAT and therefore was kept out of the loop regarding the response. In addition, the EST felt that DHS was deploying assets without going through the proper notification channels. Furthermore, the roles and responsibilities of the new DHS Principle federal Official (PFO) are not well-defined relative to the FEMA Regional Directors and the Federal Coordinating Officer (see the "PFO" *Special Topic*). The Environmental Protection Agency (EPA) also noted in the Washington venue Hotwash the need to work through and define EPA and DHS authorities and to define who has jurisdictional responsibility to take leadership of developing and maintaining health and safety plans for all of the different entities involved. EPA also noted that the process and jurisdictional roles in tasking partners for support was unclear at times. EPA can respond to a local fire department under the National Oil and Hazardous Substances Pollution Contingency Plan, but during the FSE, the regional EPA office felt pulled by the national command structure to coordinate their response with the Federal response

Finally, while these were not played out during the FSE, some agencies did highlight potential jurisdictional issues that may have been faced in the longer-term recovery phase. EPA raised concerns at the Washington venue Hotwash in regards to balancing crisis and consequence management, especially in the context of ensuring worker safety at the site, and the potential safety of citizens on/near site. In the aforementioned tabletop exercise in Washington on May

15, 2003, agencies noted uncertainty as to who makes "large, expensive" decisions regarding restoration of infrastructure such as waste-water system and roadways that cross jurisdictional boundaries. In another example, local police acknowledged during the Washington venue Hotwash that while jurisdiction went well overall, there were some questions relative to FEMA in the recovery stage, such as "would FEMA be in charge [of] the field?"

b. Authority to Release Information

The authority to release information and the "authoritativeness" of that information was a dominant issue during T2. Leading up to the FSE, participants had focused largely on this issue with respect to public information, noting concern in numerous seminars about jurisdictions "speaking" beyond their jurisdictional boundaries. This is especially problematic when a disaster crosses jurisdictional boundaries, as was the case in both the RDD and bioterrorism attacks. As DuPage County pointed out in its Lessons Learned report, "political problems existed with multi-jurisdictional release of information, especially with varying levels of government." DuPage County noted that these issues were amplified when Washington State issues came into play. As participants at the After Action Conference noted, the public will not know which source to believe when government officials release conflicting information.

Regional Joint Information Center concepts can help to mitigate these issues, as was seen in the Illinois venue and as was implemented on a more limited scale in the Washington venue. Broader joint information systems concepts offer the potential to strengthen this public information coordination to proactively include geographically disparate partners. During T2, there were some instances of Federal agencies appearing to release messages without coordinating fully with State or local officials. These issues are discussed in more detail in the *Emergency Public Information* core area.

An additional issue not discussed in the seminars or Large-Scale Game (LSG) arose during the FSE and concerned the "authoritativeness" of information. This issue refers to the reality of multiple agencies collecting and exchanging numerous types of information in any response effort, and the critical ability of agencies to understand who the authoritative sources are for what information.

In the Washington venue, there was confusion with the coordination of radiological data by multiple agencies—all of whom had some authority for the data they were collecting, but the result was confusion among the many agencies that received these data and were uncertain which information was correct or "authoritative." Similar confusion was experienced by agencies sending and receiving the various plume models and projections that were developed during the FSE; some of which was caused by a lack of understanding as to who was the authority for this information. Interestingly, numerous data collector logs suggest that those agencies that generated their own models knew that the DOE was the lead technical agency in Washington. But, when asked whose model everyone should be using, most agencies answered simply that theirs was the valid one.[146]

In another instance, agencies experienced frustration obtaining ground truth on numbers of injuries and fatalities at the scene of the RDD blast. Multiple organizations were requesting updates on this information from public health authorities and incident command, which were in

[146] For a more detailed explanation of the multiple plume models, see the data coordination story in the *Special Topics* section of this After Action Report.

turn receiving updates from on-scene responders. But these various sources all had conflicting information. Public Health Seattle/King County (PHSKC) noted at the venue Hotwash the importance of defining key, credible sources of information that they can rely on since people look to PHSKC for answers. It noted that it is only Medical Examiners who can officially declare deaths, but official certification may not come for days in the event of an RDD explosion. PHSKC highlighted the need to find an appropriate way to provide messages about death counts that are yet to be confirmed by the medical examiner.[147]

3. Conclusions

The FSE demonstrated that jurisdictional policies and the extent to which they are understood by various entities drive and influence every element of response. They define what actions agencies believe they are supposed to take. T2 demonstrated the critical importance of clearly defining and understanding informational authorities as well.

Participants at all levels of government continue to state that exercises such as TOPOFF remain one of the most effective means to convey these understandings and to clarify authorities that may appear clear on paper but which are not as clear when implemented under the complex conditions of crisis. The WA State Adjutant General summarized jurisdictional challenges and solutions at the post-FSE tabletop held in Seattle, when he stated, "our issues are multi-dimensional, and not confined to any single jurisdiction—our recovery architecture must recognize non-traditional partners."

Reiterating the critical importance of continuing to refine the collective understanding of jurisdictional authorities, the WA State Adjutant General encouraged all jurisdictions to "do serious introspection on TOPOFF, use it as stage, and pull together multi-jurisdictional functional areas to talk about what worked well throughout that pulsing system and take a hard look at the gaps at the seams."

[147] Mass fatality management and casualty tracking was a real world problem during the response to the Oklahoma City bombing and the 9/11 attacks. The Department of Homeland Security, Office for Domestic Preparedness, produced a document that discusses these issues.

E. Resource Allocation

1. Introduction

Resource Allocation challenges require decision-makers to weigh conflicting needs and determine how best to apportion limited resources. The conflicting needs can challenge decision-makers within a single agency, or can force decision-makers from different agencies and departments to work together to decide how best to manage critical resources that are in short supply relative to the demand. Often the solution is unconventional.

A weapons of mass destruction (WMD) event producing mass casualties could put enormous demands on scarce medical and public health resources. Resource issues would likely have become a concern in the Washington venue as part of the long-term recovery, post-Full-Scale Exercise time period.

2. Discnssion of challenges and good practices

Table 18 depicts the issues, challenges, and good practices relevant to *Resource Allocation* that arose in the seminars, as well as the instances that show how these issues played out during the Full-Scale Exercise (FSE). Instances are occurrences experienced by participants during the FSE that indicate challenges or good practices associated with particular issues. In the table, a (-) is used to indicate challenge, and a (+) indicates a good practice. A ( ) is used to indicate a neutral observation in the FSE—one that is neither a good practice nor an issue. *Good practices* are those practices that players felt were effective, or that the data indicate worked well;[148] these practices could potentially be explored further or promulgated on a broader scale. *Challenges* are examples of the T2 response that were difficult for the responder community and which had significant impact on decision-makers. Challenges do not imply wrong actions or incorrect responses by any organization or the community at large—this After Action Report (AAR) and the analysis as a whole did not focus on evaluating right and wrong actions. Challenges require continued attention of the national response community to facilitate smoother responses in the future.

[148] References in the table are based on specific references in the data. Just because something is not specified as a good practice does not mean it did not go well in participants' opinions or did not happen.

Table 18. Resource Allocation Issues during T2

ISSUES	*SEMINARS/LSG*					FSE INSTANCES
	Emergency Public Information	*Radiological Dispersal Device*	*Bioterrorism*	*Direction & Control*	*Large-Scale Game Consequences*	GOOD PRACTICES AND CHALLENGES
a. Lack of consistent understanding among Federal, State, and local (FSL) agencies of what federal resources are available, how to request those resources, and how much is available.			✓			(-) Confusion over official channels to acquire the Department of Health and Human Services (HHS) assets now at the Department of Homeland Security (DHS). (-) Local agencies did not always know which capabilities were available for request. (+) Officials elicited actual requirements through teleconferences. (-) Confusion over the process for declarations and in some cases the federal assistance they trigger through the Stafford Act. (+) Coordination of resources in the State of Illinois to secure sufficient security personnel via Emergency Operations Centers.
b. Planning for effective use of resources in emergencies.			✓			(+) Pre-planning the Strategic National Stockpile distribution sites. (+) Supplementing medical personnel with school nurses. (+) Preplanning stockpiles of antibiotics. (-) Multiple agencies reserved a key distribution site.
c. Handling shortages of limited resources.						(+) Illinois Governor's emergency orders opened up sources of volunteers. (+) The American Red Cross tapped supplemental sources to offset shortages. (-) In the Washington venue, FSL resources would have been stressed during the recovery phase, but weren't played out during the exercise. (+) DHS concerned with the long-term impact of nationwide red alert on resources. (+) HHS concerned with the long-term and widespread impact of pneumonic plague.

a. Lack of consistent understanding among Federal, State, and local (FSL) agencies of what federal resources are available, how to request those resonrces, and how much is available

During the Full-Scale Exercise (FSE), confusion was observed at local and state levels about federal assets and the processes for obtaining them. A few examples are highlighted here; more details on this particular issue are explored in the "Proclamations and Declarations" and the "Strategic National Stockpile (SNS)" *Special Topics* sections in this AAR.

There currently is no single source to help state and local emergency managers or responders to determine which federal resources would best meet their needs during an emergency, and there are many methods by which State and local governments can request federal resources. During the T2 FSE, States often requested specific assets—sometimes requesting inappropriate or unnecessary assets in error. For example, in Illinois a request was made for Disaster Medical Assistance Teams (DMATs), although assistance from mortuary services and epidemiologists was desired. On a positive note, this disconnect was identified and corrected during a conference call among the city, state, and regional Federal operations centers.

In the State of Washington, the evaluation team did not identify any examples of such confusion. There are a number of possible reasons for this. One possibility is that Washington has its own radiological emergency experts, as well as experience with radiological emergencies and exercises involving nuclear power plants. Thus, Washington State emergency responders are able to draw upon existing knowledge, experience, and relationships.

In both the States of Washington and Illinois, there was evidence that State and local agencies made requests to the Federal Government based upon *what* and *who* they knew, and, that State and local governments do not know all of the federal resources that are available. These informal methods are not the most efficient way to obtain the necessary resources, and in some cases did not result in the most appropriate resources for the task.

There are many methods by which federal assets can be requested. Requests can go directly to agencies , or federal departments including the Department of Homeland Security (DHS) once they are involved.[149] Because resources are requested and deployed from different sources, it can be difficult for the Federal Government to track and coordinate the many federal assets in the field. This can make it challenging, if not impossible, for decision-makers to weigh all of the available information about resources as they become depleted because the decision-makers might not have complete information on what remains available.

This is not to suggest that the many processes for requesting assistance be replaced with a centralized system. In fact, these multiple avenues for requesting assistance are critical for a number of reasons, including situations for which disasters are not declared, and for ensuring that assets arrive at disaster scenes before official Presidential Declarations are signed—the latter of which occurred during T2 (e.g., Seattle Fire Department requested assistance from EPA not long after the explosion, and Washington State made a direct request to DOE to deploy the Federal Radiological Monitoring and Assessment Center (FRMAC)). FEMA currently tracks and reports the use of federal assets in a disaster through its Mission Assignments and Situation Reports, but

[149] It is currently unclear, or possibly undetermined, whether such requests should go through Federal Emergency Management Agency and the Federal Coordinating Officer, or through the designated Principle Federal Official (PFO) or delegate. See the *Special Topics* section on the PFO for more information.

distribution of these reports is fairly inefficient—usually transmitted through e-mail or fax. There does not appear to be a "one-stop shop" where FSL agencies can obtain information regarding the range of assets that are available, how to obtain those assets, or the status of assets once deployed. A web-based, searchable database of all available federal resources (potentially expanded to include state and local resources at some point), including their names, acronyms, capabilities, and request processes—a distributed yet coordinated knowledge base—may be helpful and may also minimize personnel requests based solely upon "what and who" an individual knows.

b. Planning for effective nse of resources in emergencies

Planning prior to the FSE[150] appeared to facilitate some of the FSE activities. In Illinois, planning for receipt and distribution of SNS medications resulted in a fairly smooth-running process. In contrast, shipment and distribution of the Strategic National Stockpile[151] did not go as smoothly in the TOPOFF 2000 exercise. This reflects in part the tremendous investment in planning and preparedness that has occurred in state and local public health departments since the fall of 2001. In particular, bioterrorism preparedness grants awarded by HHS to state public health departments in 2002 spurred the development of SNS distribution plans among many other activities. The success of the SNS distribution during T2 provides one of many examples of how potential improvements in the nation's emergency response system can be examined in the TOPOFF Exercise Series.

c. Handling sbortages of limited resources

A shortage of prophylaxis for first responders coupled with a concern for unusually high absentee rates led Chicago area officials to predict a shortage of personnel available for security. When the City of Chicago requested security support from the Illinois National Guard, they learned that this resource was unavailable—the troops were deployed in Iraq. Fortunately, the city was able to obtain the needed security personnel from neighboring jurisdictions through existing mutual aid agreements. While this met Chicago's short-term needs, it is not known whether this solution would be sustainable over a greater time period, as the outbreak spread and as neighboring jurisdictions recognized their own needs for security. T2 did not evolve to this level of play to allow greater insight.

Responders obtained via mutual aid agreements also supported Seattle's response. For example, the State Fire Services Mobilization Plan was mobilized to support local firefighters. In addition, Seattle had 14 engines, four ladders, and 21 police cars that were contaminated and impounded. This equipment was expected to be replaced by neighboring jurisdictions using mutual aid agreements. The mutual aid partners, however, were concerned about the length of time that Seattle would need the loaner equipment. This concern was especially relevant because unions told Seattle (notionally) that they would suggest their members not use previously contaminated equipment. They were concerned that "clean" wouldn't really be clean.[152]

[150] The evaluation team is not privy to whether this planning was specific for the T2 exercise, or whether it is consistent with real-world planning for emergencies.

[151] The National Pharmaceutical Stockpile was renamed the SNS when it became part of DHS.

[152] Note that the definition of clean/decontaminated was brought up in seminars, the LSG, and in the Washington venue tabletop exercise. In these discussions, players were not convinced that the public would be comfortable with places and equipment deemed "safe" after decontamination.

In some cases, it is possible to circumvent potentially limited resources by expanding the resource pool. During T2, this circumvention was done in two ways: 1) by relying on unconventional sources of support, and 2) by intervening with executive orders that exempt individuals from repercussions (often legal battles) that would otherwise prevent these individuals from providing services. For example, the American Red Cross requested mental health counselors from the Chicago Public School system to fill in for its predicted 20 percent absentee rate. Also in Illinois, the Governor signed several emergency executive orders that restricted liability and provided immunity to people supporting the response. One was particularly valuable for SNS distribution: it allowed non-pharmacists to dispense prophylaxis.

One of the many challenges in managing limited resources is working to maintain enough resources to handle other yet-to-occur situations—predictable or otherwise. To meet this challenge, those who make allocation decisions need to decide what, if anything, they should hold back from immediate requests to ensure there are resources to support other needs, should they arise. Such planning requires a risk assessment, and, in the case of bioterrorism, expertise on how and how quickly the disease can spread. Such planning requires difficult choices, as it could lead to unfortunate illness and even death. However, it can also avert nation or worldwide spread of epidemics. There is evidence of such planning during T2. In one example, the DHS Emergency Preparedness and Response Directorate was working on a plan to distribute drugs from the SNS to other states that requested the stockpile, recognizing the inevitable spread of cases outside Illinois. In addition, public health officials in Illinois anticipated potential hospital surge requirements that the growing epidemic would require (see "Decision Making Under Conditions of Uncertainty" in *Special Topics*). The Severe Acute Respiratory Syndrome (SARS) outbreak has caused public health authorities to think about how to provide surge capacity. Of course, in the event of bioterrorism, an outbreak could be much more severe. In Washington, the National Guard Civil Support Team was released from the incident site and placed on standby in case they were needed to respond to another incident. Thus, officials at all FSL levels were developing plans to handle the unpredictable.

3. Conclusions

For a variety of fiscal and operational reasons, play in Washington was limited and did not fully stress the system. For example, field play ended after two days, and exercise play ended after a command post exercise on the third day (D+2). The result was that many resources that are often exhausted early in the response either did not need replacing or were not exhausted. In addition, prior to the FSE, the Washington venue chose not to play the plague scenario—which meant that the two incidents did not interact, except in terms of the criminal investigation.[153] In fact, during the exercise HHS sent at least one inject via fax to Public Health Seattle/King County (PHSKC) Department regarding plague patients. PHSKC responded that it was not playing the plague scenario because of real-world resource limitations on public health workers stemming from SARS and the smallpox vaccinations.[154] Players in the Washington State Emergency Operations Center commented that they would have been very challenged if they had played the plague scenario. Furthermore, levels of radiation were designed to be relatively low to impose relatively

[153] Note that early incarnations of the scenario had plague coming to Washington State, but the radiation from Seattle was never conceived of as being transferred to Illinois.

[154] Near the end of the exercise, participants at the King County and WA State EOCs took actions related to the plague outbreak.

minimal impact upon the community. Nonetheless, Washington resources were stressed and requests were made for assistance from mutual aid partners and federal resources. Furthermore, some federal assets, such as the FRMAC, reported that they were having difficulty meeting all requests.

In Illinois, issues of limited resources were anticipated, discussed, and planned for, often with creative and unusual solutions. Federal resource managers also predicted and planned for resource depletion through decision-making that would likely be unpopular. This type of planning suggests that the Federal Government was prepared to make difficult decisions that might be needed following terrorist events.

F. Anticipating the Enemy

1. Introduction

The existence of an enemy makes the response to terrorism attacks qualitatively different from the response to any natural or conventional disaster. For example, the desire to keep terrorists in the dark regarding response plans can work against the desire to keep the public informed. Nature is morally neutral and indifferent to its own effects. Terrorists, however, can exploit government and public reaction to an attack, and this consideration must be taken into account. Media reports, some of them quite detailed, describing adjustments being made by the Government in the wake of 9/11, were criticized for making too much information available to the terrorists. While an active Red Team during the Top Officials (TOPOFF) 2 (T2) Full-Scale Exercise (FSE) was limited in scope, the actions of responders and top officials can still demonstrate awareness of potential follow-on attacks. This area of analysis focuses on those actions discussed in the seminars and observed during the FSE that related to the need to anticipate the enemy.

2. Discussion of issues: challenges and good practices

Table 19 depicts the issues, challenges, and good practices relevant to *Anticipating the Enemy* that arose in the seminars, as well as the instances that show how these issues played out during the FSE. Instances are occurrences experienced by participants during the FSE that indicate challenges or good practices associated with particular issues. In the table, a (-) is used to indicate challenge, and a (+) indicates a good practice. A ( ) is used to indicate a neutral observation in the FSE—one that is neither a good practice nor an issue. *Good practices* are those practices that players felt were effective, or that the data indicate worked well;[154] these practices could potentially be explored further or promulgated on a broader scale. *Challenges* are examples of the T2 response that were difficult for the responder community and which had significant impact on decision-makers. Challenges do not imply wrong actions or incorrect responses by any organization or the community at large—this After Action Report (AAR) and the analysis as a whole did not focus on evaluating right and wrong actions. Challenges require continued attention of the national response community to facilitate smoother responses in the future.

[154] References in the table are based on specific references in the data. Just because something is not specified as a good practice does not mean it did not go well in participants' opinions or did not happen.

Table 19. Anticipating the Enemy Issues during T2

ISSUE	SEMINARS/LSG					FSE
	Emergency Public Information	*Radiological Dispersal Device*	*Bioterrorism*	*Direction & Control*	*Large-Scale Game Consequences*	GOOD PRACTICES AND CHALLENGES
a. Balance public information with security needs.	✓	✓				( ) No evidence to support or refute.
b. **NEW:** Recognition by decision-makers that an active malevolent enemy may seek to exploit response strategies.						(+) Showing caution in responding to an event that might have a terrorist origin. (+) Proactively raising defenses over a widespread area after one area has had a confirmed or strongly suspect terrorist attack. (+) Development of plans to manage limited resources in the event of another attack. (-) Several agencies suggested that anticipating the enemy is not their concern or that it is the responsibility of the Federal Bureau of Investigation.

a. Balancing public information with security needs

Top officials have to weigh competing factors when deciding to release information that could be used by terrorists. These include:

- The need to anticipate the enemy's use of available information, and sometimes limiting the content of information about the response or other emergency-related activities (e.g., shelter locations) that is released to the public; and
- The need to retain the public's confidence or even to enlist their cooperation, and sometimes make statements indicative of what is known about the enemy, including their potential whereabouts, plans, etc.

b. Recognition by decision-makers that an active malevolent enemy may seek to exploit response strategies

During the FSE, there were a number of responder and top official activities that demonstrated a keen awareness of potential follow-on attacks in other U.S. locations and in the already targeted locations. Some examples include:

- Soon after the explosion in Seattle, the Seattle Federal Bureau of Investigation (FBI) field office and FBI Headquarters counter-terrorism division initiated an initial threat assessment, examining the possibility of other explosive devices in the Seattle area;

- The City of Chicago and surrounding counties increased surveillance, and decreased parking and deliveries, at pre-selected, likely terrorist targets after the RDD attack in Seattle incident; and
- Nationwide, there were various closures, and increased guards at facilities, such as nuclear power plants.

In Seattle, the National Guard Weapons of Mass Destruction Civil Support Team was released from the RDD explosion site at 1230 Pacific Daylight Time on May 13, 2003, in part so that they would be available to re-deploy in the event of another terrorist attack, at another place, and at another time. Similarly, considerable thought was given to this by the Department of Health and Human Services, the Department of Homeland Security, the Centers for Disease Control and Prevention, and others to the need to deploy the Strategic National Stockpile and other resources, with explicit mention that the Chicago metropolitan area might not be the only area attacked with Pneumonic Plague.

Finally, the increases of the Homeland Security Advisory System Threat Condition from Yellow to Orange, and then to Red, whether nationwide or only in particular cities coast-to-coast, represented the ultimate in proactively raising defenses over a widespread area.

However, many agencies and jurisdictions acknowledged that they either were not playing against an enemy or that it was the responsibility of others (e.g., the FBI and the Joint Operations Center) to consider the enemy. The former likely represents an exercise artificiality. Further Red Team play was limited to tactical support to the Seattle Police Department Special Weapons and Tactics (SWAT) team, the U.S. Coast Guard, and FBI SWAT activities in the state of Washington, as well as to the Illinois State Police and FBI Hostage Rescue Team activities in the state of Illinois. These events did not impact the broader T2 FSE, and therefore Red Team activities did not directly impact any decisions made by top officials. Yet, agencies and jurisdictions must be aware that their responders will be at risk by nature of being part of the response. The loss of responders in additional attacks could seriously impair an agency's or jurisdiction's response capability, not to mention how such a loss would impact the morale of other responders and the public at large.

3. Conclusions

Despite the fact that the exercise contained limited Red Team play, many participants did consider the possibility of further terrorist attacks. Examples of their doing so exceed the few cited here.

The question of how to respond to an event that seems to have been an act of terrorism, but is lacking conclusive proof, is problematic. This was faced on 9/11 and in the wake of the anthrax attacks in 2001. Officials need to strike a delicate balance among all the competing demands of protecting the public in both response and prevention.

This page intentionally left blank

VII. A COMPARISON TO TOPOFF 2000

This section compares Top Officials (TOPOFF) 2 (T2) to the earlier TOPOFF 2000 Exercise. TOPOFF 2000 resulted in a substantial and valuable Exercise Observation Report, which should be consulted for further details on TOPOFF 2000 findings.

A. Design

The Full-Scale Exercises (FSE) in both TOPOFF 2000 and T2 featured:

- Top official participation;
- A city with a pneumonic plague event;
- Another city with an explosion/hazardous materials (HAZMAT) event: in TOPOFF 2000 a homb was detonated releasing a persistent chemical agent in Portsmouth; in T2 a radiological dispersal device (RDD) was detonated in Seattle; and
- Interagency play at the command post level in Washington, D.C.

Despite the similarities of design between the two TOPOFF exercises, there were major differences. T2 added an international element, not present in TOPOFF 2000, by including some international elements in the scenario and through Canadian government participation.

The designers of T2 responded to some of the TOPOFF 2000 participant feedback, most notably by:

- Facilitating the increased involvement of top officials;
- Eliminating TOPOFF 2000's "no-notice" character in favor of an open exercise in which participants were introduced to the exercise scenario through a cycle of exercise activities of increasing complexity that included seminars and a large-scale game (LSG);
- Introduction of a limited opposing force, or Red Team, to develop the concept and rules of play so that a more robust Red Team could be employed in future exercises; and
- Giving increased attention (via the LSG) to long-term recovery issues.

Exercise planners in the venues actively participated in the design of the scenario. The full-notice, "open-book" nature of the T2 FSE also helped to allay participants' concerns that they or their performance would be evaluated. However, these changes brought about some post-exercise criticism in the media that the "open book" nature of T2, including extensive exposure of the participants to the scenario in the seminars, minimized free-play decision-making. In fact, the designers deliberately chose to maximize continuous learning rather than sequestering the scenario.

This early involvement in design paralleled another path of continuous pre-FSE participation, namely that of the seminars and the LSG. These used the same scenario as the FSE (more precisely, each seminar used the FSE scenario as it stood at the time of the seminar), and had the

effect of making the participants and the designers more aware of the details of each topic treated in the seminars.

B. Participants

Despite its designation as a top officials' exercise, ("TOPOFF," based upon the term *Top Officials)*, TOPOFF 2000 was assessed to have suffered from insufficient top official participation. Likely reasons include the conflict between the no-notice nature of TOPOFF 2000 and the heavily pre-scheduled commitments of top officials. In T2, top officials at all levels of government participated actively during the FSE.

The participating T2 organizations in the Washington and Illinois venues—including local, state, and regional federal entities, as well as private organizations such as the American Red Cross—are too numerous to list here, but special mention must be made of the remarkable level of participation by Chicago area hospitals. Far in excess of the number hoped for, hospitals in the metropolitan Chicago area volunteered to participate in the demanding T2 exercise, and did so while maintaining their caseload of real patients, who required real care at the same time. For this reason, T2 represented an unparalleled opportunity to examine the operation of the public health and medical communities in the face of a bioterrorism attack. This was in significant contrast to the limited medical play which occurred during TOPOFF 2000.

C. Evaluation, and the Data to Make It Possible

T2 employed a significantly different approach to exercise evaluation in TOPOFF 2000. The TOPOFF 2000 Exercise Observation Report is a compilation of the after-action reports of the individual participating entities, and the results of an after-action conference held some months after the exercise where perspectives on the exercise were obtained and exchanged. Such reports and conferences are extremely valuable, and T2 has benefited from having received such reports and having had a similar post-exercise conference one month after the FSE (held on June 17 and 18, 2003); but such information and perspectives, while valuable, are not data.

During the T2 Full-Scale Exercise (FSE), data collectors worked side-by-side with participants to document a time-based record of player actions and decisions. These, and other logs kept by exercise controllers as well as those created in the course of play by participants including emails whose work (and therefore whose FSE play), were combined and sorted by time. Entries were tagged for relevance to the six core areas of analysis and to several of the special topics whose importance emerged only as the FSE unfolded. From these records, analysts working on any particular area of analysis or topic could quickly find all relevant occurrences and compile a comprehensive look at the events sorted according to time. This allowed analysts to view the interconnections that no single participant or observer would have been able to perceive. Importantly, this process traces T2 findings back to the events that actually took place during the exercise. As such, T2 effectively represents the baseline exercise from which all future exercises can be systematically compared.

D. Findings

The following sections present a brief comparison of the results from T2 to the findings of TOPOFF 2000. In the interest of brevity, the latter are taken entirely from the TOPOFF 2000

report's 14 major areas of observation[155] and re-arranged to conform to T2's six core areas of analysis.

1. Emergency public information (EPI)

TOPOFF 2000 resulted in the following observations regarding public information:

- "Confusion on EPI roles, responsibilities, and appropriate public messages"; and
- "Confusion was evident in the chemical venue regarding the role of Joint Information Center (JIC) and Joint Operations Center (JOC) responsibilities."

Confusion as to EPI roles and responsibilities for messages emerged as well in T2. For example, in Seattle a Public Information Officer (PIO) speaking for the King County Regional JIC said in a press conference that there are "no casualties" from the Seattle RDD blast when in fact the King County Emergency Operations Center had a casualty count that was over sixty, and included two fatalities. Other examples included inconsistent themes in public messages from top officials in the Washington venue regarding the relative danger from radiation; varying guidance from agencies regarding antibiotics in Illinois; and at least one press release from the City of Chicago requiring proof of presence at the suspected exposure sites as a condition for receiving prophylaxis.

The confusion of JIC and JOC roles does not seem to have been repeated.

2. Emergency public policy and decision-making

In TOPOFF 2000:

- "Authorities and guidance for population control and movement restrictions (e.g., quarantine) for a large-scale public health emergency are uncertain and not widely understood";
- "TOPOFF 2000 highlighted the need for improved public health sentinel surveillance capabilities";
- "The capacity to gauge the scope and consequences of a catastrophic WMD incident and convey that information to senior officials must be improved to facilitate timely and appropriate decision-making";
- "Lack of, or limited use of, detection equipment was a significant impediment to early recognition of chemical, biological, and radiological…WMD attacks"; and
- "Updates on mitigation efforts must be widely transmitted to both responder communities and the public."

The contrast between TOPOFF 2000 and T2 in this regard is interesting and deserves considerable attention.

[155] Note that TOPOFF 2000's usage of the term "observation" does not necessarily conform to the definition applied to that word in this T2 After Action Report.

As a result of substantially increased public health funding in the wake of the anthrax attacks, planning efforts directed towards a possible intentional smallpox release by terrorists, and actions taken to prepare for a potential Severe Acute Respiratory Syndrome (SARS) outbreak in the United States, considerable thought has been given to the issues of population control and movement restrictions. Despite these activities, implementing them in the event of a real-world requirement would most likely be a difficult problem. T2 did not exercise this aspect of the public health response to a disease outbreak, although policies such as *shelter-in-place* and *snow days*[156] were implemented to protect the population and legal authorities to restrict movement were invoked.

T2 did not fully provide an opportunity to test the efficacy of sentinel surveillance of disease and radiological detection systems. Given the large number of initially exposed individuals, the onset of the plague in Illinois was sufficiently dramatic that it prevented such a test.[157] At one point there had been discussion of having a more subtle disease onset in the Illinois venue to test surveillance systems, but other objectives could only be served by having a large number of patients, and those objectives were deemed more important. There were a number of attempts to estimate the scope of the plague outbreak in Illinois but this was not fully played out during the FSE. Had the exercise continued for one or two more days, the scale of the outbreak would have become a significant issue. Even so, at the federal level in the Department of Health and Human Services, efforts were underway as the week went along to determine the scope of the disease outbreak in order to assist resource planning.

In TOPOFF 2000, the responders entered the blast site and became contaminated by the chemical agent; in T2, by way of contrast, responder safety was clearly balanced against the need to rescue victims. However, officials may have been challenged if the public complained about seeing responders "hanging back" from the incident site.

The TOPOFF 2000 report cites national plans (e.g., the Federal Response Plan (FRP), and the Federal Radiological Emergency Response Plan) as needing reconciliation with Presidential Decision Directive (PDD)-39, the *Domestic Guidelines*. T2 took place in the transition to Homeland Security Presidential Directive (HSPD)-5 from the existing FRP and concept of operations. The creation of DHS and the attendant development of a National Response Plan (NRP) and National Incident Management System (NIMS) mean that the next TOPOFF exercise will be conducted under different doctrine and policies. As such, further analysis of the exercise data can provide additional valuable insight into communications, coordination, and connectivity issues that will be important in the development of the NRP and the NIMS.

Finally, since there is no real-world precedent in which the Stafford Act has been applied to a biological disaster—or one involving non-explosive radiological, chemical, or biological weapons—it is noteworthy that in both TOPOFF 2000 and T2, the widespread impacts of the biological attacks did not qualify as a "disaster," under The Stafford Act. In T2, this led to a declaration of "emergency" in Illinois, when a declaration of disaster was requested by officials. The distinctions between the assistance that can be obtained through these two types of declarations were not always understood by participants. Future exercises should continue to

[156] During the T2 Full-Scale Exercise, the phrase *snow days* indicated to participants that they were to stay at home as if they had been impacted by a major snow storm.

[157] Although as noted in the special topic on hospital play, the initial indicator of the plague outbreak appeared to have come from DuPage County's Pro-Net surveillance system.

refine the applicability of the Stafford Act to bioterrorism and other non-explosive disasters not explicitly defined in the Act, in order to increase Federal, State, and local (FSL) agency familiarity with its application to, and implications for, such disasters.

3. Resource allocation in TOPOFF 2000

The TOPOFF 2000 report cited shortages of medical and other supplies, and the ensuing competition over these supplies on the part of multiple jurisdictions.

The T2 scenario was designed not to stress resources to the breaking point, so shortage concerns did not generally arise. However, there was a potential prophylaxis shortage in the Illinois venue that was quickly averted by the introduction of Vendor Managed Inventory. The RDD incident was not large enough to exhaust the region's resources at least in the near term. Similarly, the exercise ended in the Illinois venue before the most challenging resource demands impacted the medical system in terms of resources such as beds, ventilators, and staff.

4. Communications, coordination, connectivity in TOPOFF 2000

The TOPOFF 2000 report recorded the following observations regarding communications, coordination, and connectivity:

- "Improved interaction is required among U.S. Departments and agencies and international organizations … regarding alerts, notifications, and warnings";
- "Roles and responsibilities in notification (e.g., the National Response Center) were not clear"; and
- "There was no ability to broadcast collective warnings."

These issues remain among the most dominant challenges faced by the national response community. The creation of DHS and the development of the Homeland Security Advisory System have helped to provide communication frameworks, but numerous challenges remain. In T2 these challenges manifested themselves in numerous instances such as the elevation of the HSAS to red for the first time in an exercise or the real world, tracking patient numbers and casualties both in the Washington and Illinois venues, and coordination of public information messages in both venues. Issues remain in the areas of information access, formal and informal communications channels across multiple EOCs and with substantial use of internet-based communications, insufficient electronic communications infrastructures in some domains such as the medical community, and common language, to name a few.

5. Jurisdiction in TOPOFF 2000

In TOPOFF 2000, it was observed that:

- "Roles and responsibilities for operational direction and control…were blurred by the proliferation of response teams."

Despite the creation of DHS, this observation might resonate with some T2 participants. In particular, the role of the PFO in regard to the previously existing response structure needs to be clarified. The proliferation of federal response teams remains an issue—there appear to have been more teams in T2 than there were in TOPOFF 2000. Coordinating and effectively using these federal assets is an area requiring attention.

Plume modeling and deposition analysis problems in T2, and associated data collection and coordination issues, can also be viewed as jurisdictional issues. Furthermore, there were jurisdictional uncertainties over who had the authority to shut down and re-open the transportation infrastructure (e.g., highway, rail, and air systems).

VIII. EXERCISE DESIGN AND CONDUCT LESSONS LEARNED

The Top Officials (TOPOFF) 2 (T2) After Action Conference (AAC) attendees and exercise participants identified several lessons learned relative to exercise design and conduct. After assembly and review, comments were compiled into the following eleven subject areas:

- Planning, Participation, and Coordination Considerations;
- Intelligence Development and Management Processes;
- Exercise Document Guidelines;
- Exercise Time Standards;
- Exercise Artificiality Considerations;
- Consideration of a Functional Web-based Control Capability;
- Additional Exercise Event Considerations;
- Scenario Scripting Considerations;
- Virtual News Network Considerations;
- Exercise Security Considerations; and
- Coordination and Venue Design Team Empowerment.

A. Exercise Design and Conduct Comments

This section addresses exercise design and conduct comments as they pertain to each subject area.

1. Exercise planning, coordination, and participation considerations

The Secretary of Homeland Security should continue to solicit participation in the TOPOFF Exercise Series by formal invitation, encouraging the direct involvement of top officials at every level of Federal, State, and local response, including appropriate non-government organizations.

T2 AAC participants commented that invited senior officials should commit themselves and their organizational resources as early as possible. While T2 gained substantial top official involvement, future events would hugely benefit from even greater support from senior leaders. Their early and significant commitment immediately increases process relevance and the potential for exercise success. The Secretary of the Department of Homeland Security (DHS) direction in establisbing a national exercise program to be administered by the DHS Office for Domestic Preparedness (ODP) will aid participants in scheduling and scoping participation in TOPOFF and other national-level exercises.

The T2 seminars included many senior officials. Comments suggested the complex process for forwarding invitations and coordinating participation requires improvement. Invitations were often forwarded within an organization's executive channels and bypassed the primary exercise planner. This process should commence well in advance of suspense dates to ensure that

exercise planners are aware and informed. Primary exercise planners play key roles in preparing senior officials for meaningful event participation.

Many T2 participants were concerned about the relatively late identification and commitment of participating organizations. Commitments to scope of participation and statements of support requirements must take place earlier in the planning process. T2 planners developed a Memorandum of Understanding (MOU) to codify and identify participating organizations, their commitment levels, and their administrative and logistical support needs. The T2 MOU was completed too late in the planning process to be fully effective. Future TOPOFF Exercise event planners should formalize this document as a binding Memorandum of Agreement completed prior to significant exercise planning and staffing expenditures, preferably by the Mid-term Planning Conference.

Participant comments suggested that T2 data collector and controller roles and requirements were not clearly defined. Qualification guidelines and more specific information regarding their duties would enable more appropriate personnel selection and application. Recruitment needs to occur early enough to permit sufficient opportunity for their training.

Several individuals and organizations suggested including past TOPOFF venue participants in future TOPOFF Exercise planning processes. Individuals with first-hand venue experience in past TOPOFF events could contribute an important depth of corporate memory and insight to future events planning.

T2 included substantial international play, primarily with Canada, reflecting the international scope of potential weapons of mass destruction (WMD) events. It was recognized that future TOPOFFF exercises should emphasize more international involvement. Consideration should be given to inviting key international bodies such as the World Health Organization, in addition to other governments.

2. Intelligence development and management processes

T2 intelligence play was purposefully designed to provide background support to drive the exercise scenario. For simplicity, T2 did not provide an opportunity for analytical review and intelligence development. Several comments suggested including enough depth and complexity of notional intelligence processes to allow for analysis in real time. Such intelligence play should enable and promote the intelligence buildup at exercise commencement and continue as a robust element of play throughout the event. The intelligence community should provide answers to requests for information, including the production of "tear-lines" so that DHS can produce press releases based upon them. This would support the concept of prevention, an important aspect of homeland security.

Further comments suggested that all exercise intelligence data should he handled within actual controlled channels, as it would in the real event.

3. Exercise documents guidelines

Many participants were unclear about T2 scenario control with respect to injects. There was confusion as to which were official, and how official requests for information or injects would or should be received and processed. Most agreed that participants should use preexisting organizational document formats during exercise play just as they would in reality. These documents must include appropriate exercise caveat markings that clearly identify them as

notional so they are not confused with actual document traffic. The exercise control group should use standardized exercise document formats, recognized by all participants as exercise control documents. Establishment of the National Exercise Program and collaborative management processes will improve available tools and templates.

4. Exercise time standards

Confusion sometimes existed as to time references, particularly as the Master Control Cell was in Washington, DC (Eastern Daylight Time), and the venues were in the states of Illinois (Central Daylight Time) and Washington (Pacific Daylight Time). Comments suggest eliminating such confusion with the mandatory use of Coordinate Universal Time, or Universal Time, previously known as Greenwich Mean Time, for all exercise transmissions.

5. Exercise artificiality considerations

Exercise artificialities occur simply because many aspects of a real situation cannot he effectively simulated. The scope of exercise play is limited by funding, logistical and geographical constraints; therefore, some artificialities are beyond planner control and others are choices specifically made to enable specific exercise goals and objectives. Each artificiality should be the product of a conscious choice and provide the means to demonstrable ends. Exercise planners should clearly identify and consider each artificiality for its necessity in achieving exercise objectives.

Overall, planners must weigh real exercise factors against versus notional ones. A robust firewall between artificial scenario information and real world information must be established and maintained at all costs. Realistic deployment timelines and parameters must be maintained in cases where assets are positioned administratively to simplify logistics and costs.

Comments suggested notionalizing additional elements of future events by including first responder casualties, more aggressive exercise press coverage and media pressure, Web-based news formats, extension of play to include more long-term consequences and recovery considerations, and challenges to Continuity of Operations and Continuity of Government plans and processes.

6. Consideration of a functional Web-based control capability

A serious shortcoming cited in T2 was the failure of planned controlled access communication channels and the use of a Web-based Master Scenario Events List (MSEL) tracking tool. In short, the Extranet Secure Portal and the on-line MSEL tools did not achieve performance expectations. Such on-line exercise control tools must be fully functional and all controllers must have ready access and confidence in the tools' reliability.

7. Additional exercise event considerations

While the T2 Full-Scale Exercise (FSE) ended as planned on May 16, 2003, there may have been significant utility in a post-FSE event focusing on remediation and long-term recovery aspects leveraged from the FSE scenario and play. To exploit similar future opportunities, planners should consider the potential of post-FSE events to produce a more comprehensive learning experience. Other smaller spin-off precursor or successor events could emphasize prevention

and protection aspects of a WMD terrorist incident as well as response, and engage all potential players during a notional intelligence buildup.

8. Scenario scripting considerations

Future exercises must closely balance scenario scripting against free play. It is important that all controllers clearly understand the definition and function of the MSEL and Procedural Flow (PROFLOW) processes. To avoid the premature disclosure of MSEL information that occasionally occurred during T2, future events should re-emphasize limited access and distribution of MSEL/PROFLOW information, and establish voluntary yet firm non-disclosure policies. An organizational exercise planner is a "trusted agent" with regard to the MSEL/PROFLOW and as such must protect the data as privileged information, guarding against its disclosure to organization members, or players, actually responding to the exercise challenge.

9. Virtual News Network considerations

Virtual News Network (VNN) accomplished many successes during T2. Future exercises could benefit from some changes and augmentation of VNN operations. The T2 design process can improve to ensure VNN announcements and interviews faithfully correlate with exercise play. Another consideration is the cost of VNN play. Though many recommended that VNN operations continue around the clock, planners must weigh the value of extended VNN play against cost. To add further realness to a simulation, VNN could record and play back its broadcasts during off hours, or provide a 24-hour Web-based news source such as *www.VNN.com*. Future VNN efforts should be targeted at aggressive news gathering that actively seeks sources for stories.

10. Exercise secnrity considerations

Awareness of exercise participant safety and security concerns need to permeate exercise planning and operation. The possibility that sensitive information or closely-held responder procedures might fall into the wrong hands needs to be minimized. Enhanced physical, as well as electronic, security in the venues and the master control sites should be priorities in future events.

11. Exercise coordination and venue design team empowerment

Exercise venue design teams could be empowered to make recommendations regarding equipment and training preparedness needs, based upon their subject matter expertise and insight into existing domestic preparedness programs. The smaller, building-block events leading up to the FSE can be used as tools to enable or increase FSE success. These challenges also present continuous opportunities to identify State and local training, procedural, equipment, and preparedness shortcomings prior to the FSE. Closer linkage to statewide, multi-year Homeland Security strategies under DHS/ODP grant programs will improve the ability to identify needs.

IX. CONCLUSIONS

Following on the success of TOPOFF 2000, TOPOFF 2 (T2) was truly a groundbreaking exercise. It was particularly noteworthy as the first national exercise conducted since the Department of Homeland Security (DHS) was established. As a result, it provided a tremendous learning experience both for DHS and for the Federal agencies that will now be working with DHS during the response to domestic incidents. In addition, the experience in Washington and Illinois provided important lessons regarding Federal, State, and local (FSL) integration. These lessons are valuable to other states and localities as they work to train, exercise, and improve their own response capabilities.

A. T2 involved the play of new agencies and entities within DHS (e.g., the Transportation Security Agency, the Principle Federal Official, and the Crisis Action Team)

- The Principle Federal Official (PFO) concept was tested in both exercise venues. While this position has the potential to assist greatly with the coordination of federal activities across the spectrum of the response, T2 results also indicated that the roles and responsibilities of the PFO need to be clarified with respect to those of the Federal Bureau of Investigation Special Agent in Charge, the Federal Emergency Management Agency (FEMA) Regional Director, and the Federal Coordinating Officer, and potentially others. In addition, the PFO requires an emergency support team with the flexibility and expertise to provide support across the full range of homeland security operations. Other areas requiring clarification include transportation and medical assets now administered through DHS.

B. T2 represented the first time (real or exercise) in which the Homeland Security Advisory System Threat Condition was raised to Red

- This was a beneficial experiment in that the Secretary of DHS both raised selected areas of the country and then the whole country to Red. In addition, local jurisdictions raised their own threat conditions to Red;
- T2 revealed considerable confusion about the notification process and notification channels from the Federal Government to state and local governments. Local efforts to raise their own threat conditions produced confusion elsewhere in the country as to whether the statuses of the local conditions were DHS-driven actions. There was also confusion at all levels of government about what actions should be taken at Red, particularly in the case of selected locations; and
- Finally, although it was not fully explored during the exercise, concern was raised about the costs of being at Threat Condition Red—particularly in the absence of specific threat information.

C. T2 involved an extraordinary sequence of two Stafford Act Declarations wrapped around a Public Health Emergency Declaration by the Secretary of Health and Human Services

- The Presidential declarations were for a major disaster in the Washington venue and an emergency in the Illinois venue. These two declarations illustrated some of the subtleties of the Stafford Act that may not have been fully appreciated before the exercise; for instance, a bioterrorism attack does not clearly fit the existing definition of *disaster* as defined by the Act. ; and
- The Secretary of Department of Health and Human Services (HHS), acting on authorities through the Public Health Service Act and in consultation with the region, declared a Public Health Emergency. This permitted HHS to authorize the use of federal assets (with costs covered by HHS). It appeared to lead to some confusion about where authority to deploy certain assets really lay, with HHS or DHS.

D. Planning and development of the National Incident Management System should take advantage of the T2 experience

- This comment from the TOPOFF 2000 report bears repeating: "Multiple direction and control nodes, numerous liaisons, and an increasing number of response teams complicated coordination, communications, and unity of effort." If anything, T2 may have been characterized by even more teams and communication nodes;
- Communication and coordination issues drove the course and outcome of critical public policy decisions from the elevation of the Threat Condition, to the various disaster/emergency declarations, the determination of exclusion zones, and the re-opening of transportation systems. To the extent that there were problems in these areas, communication issues were likely the primary cause; and
- T2 showed that how people believe communications and coordination are supposed to work is often not how they work in practice. What may appear to be clearly defined processes—such as requesting the Strategic National Stockpile—in practice become much more difficult. The National Incident Management System process needs to leverage the T2 experience.

E. T2 represented one of the largest hospital mass casualty exercises ever conducted, as 64 hospitals in the greater Chicago area participated in response to the bioterrorism attacks, and 123 hospitals either received faxed patieuts or participated in the communications of the exercise

- As such, T2 represented a significant experiment in communications and coordination for the public health and medical communities. In particular, the massive amounts of communication required to track resource status (e.g., beds, specialized spaces, medical equipment) taxed hospital staffs;
- T2 did not last long enough to fully explore the impacts of mass casualties due to bioterrorism on the medical system. Much less than half of the infected population was visible to the medical system at the conclusion of the exercise. This remains an area to explore in future exercises; and
- While there were a number of attempts to estimate the potential scope of the outbreak, the focus of most activities appeared to be on the cases that were presented to the health care

system. It should be noted that HHS was working actively as the week went on to identify the resources that would be required to deal with the infected population.

F. In the Illinois venue, T2 play involved an extensive Strategic National Stockpile request and distribntion component

- Although the actual distribution process appeared to go quite well, there was some confusion over the procedures and processes for requesting and receiving the stockpile. The SNS Operations Center coordinated the stockpile deployment with the Centers for Disease Control and Prevention (CDC) and the FEMA EP&R Director; however, there is no data to indicate that senior-level consultation occurred between DHS and HHS. In addition different jurisdictions in Illinois took different routes (for example, through DHS FEMA and the CDC) to request the SNS; and
- The jurisdictions in the Illinois venue were forced to confront important decisions about how the stockpile (and local assets) would be divided and which population groups would be the first to receive prophylaxis. The discussions and decision-making involved, as well as the challenges of coordinating public information, provide valuable lessons to any metropolitan area.

G. The Department of Homeland Security should consider integrating the existing response policies and plans into the National Response Plan

- States are familiar with and have built their response plans to interact with federal assets using similar agency and department structures and language;
- Federal agencies are satisfied with the language, authorities, and relationships outlined in existing plans such as the Federal Radiological Emergency Response Plan and the National Oil and Hazardous Substances Pollution Contingency Plan; and
- As the National Response Plan continues to be developed, the surrounding issues merit consideration—particularly where existing plans are considered effective for emergency response.

H. T2 involved more intense and sustained top official play than occnrred during TOPOFF 2000

- Of particular note was the play of DHS (which had been in existence for only a little more than ten weeks prior to the exercise), including the Secretary and other senior civilians; and
- HHS operated the Secretary's Command Center, non-stop, throughout the exercise with extensive play at the Assistant Secretary and Operating Division Director level. The Secretary was actively involved in T2 play, and since the Illinois venue involved substantial public health and medical play, the active participation of HHS was critical to the success of the exercise.
- In both the Washington and Illinois venues, the offices of the mayors, county executives, and governors were well represented throughout the exercise by either the elected officials themselves or high-level policy-makers in respective administrations. In particular, the Mayor of Seattle participated substantially in the FSE, providing local top

leadership that greatly contributed to the realism of play and to a greater appreciation of the local challenges and perspectives in a national WMD attack.

I. T2 represents a foundational experience to guide the future development of the TOPOFF exercise series

- Because of the intense data collection process and the effort to make T2 findings traceable through a detailed reconstruction of the exercise events, T2 now represents a baseline upon which subsequent TOPOFF exercises can build and to which they can be rigorously compared. In addition, continued analyses of T2 data can he employed to help guide the design of the National Exercise Program.
- T2 demonstrated the value of the international, private sector, and non-profit perspectives and roles in any response to WMD terrorism. Future exercises will, no doubt, expand on these elements by broadening the participation of these sectors.
- The use of an opposing force (OPFOR), or red team, during T2 provided ground rules for the involvement of a simulated active enemy threat in future exercises. This play should also be expanded in future exercises, as it represents one of the fundamentally different challenges responders face in a terrorist WMD disaster relative to any natural or conventional disaster; and
- The success of the VNN, and widespread participant feedback regarding the desire for additional challenges in the area of public information, suggest that future exercises should include a more aggressive mock-media element, with a more aggressive news gathering function.

X. GLOSSARY OF ABBREVIATIONS AND ACRONYMS

A

AAC	After Action Conference
AAR	After Action Report
ADLE	Advanced Distance Learning Exercise
ALS	Advanced Life Support
AMS	Aerial Measuring System
AMTRAK	National Railroad Passenger Corporation
ARAC	Atmospheric Release Advisory Capability
ARC	American Red Cross
ASPHEP	Assistant Secretary Public Health Emergency Preparedness (HHS)
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives

B

BEN	Business Emergency Network
BDC	Bomb Data Center (FBI)
BLS	Basic Life support
BTS	Border and Transportation Security (DHS)

C

CA	California
CAN	Canada
CAT	Crisis Action Team
CBP	Customs and Border Protection (DHS)
CBR	Chemical, Biological, Radiological
CBRN	Chemical, Biological, Radiological, Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CCU	Hospital Critical Care Unit
CDC	Centers for Disease Control and Prevention
CDC EIS	CDC Epidemic Intelligence Service
CDPH	Chicago Department of Public Health
CDT	Central Daylight Time

CEO	Chief Executive Officer
CFR	Code of Federal Regulation
CIRG	Critical Incident Response Group (FBI)
CMC	Crisis Management Center
CMG	Consequence Management Group
CMT	Crisis Management Team (Kane County, IL)
CO	Colorado
COG	Continuity of Government
CONPLAN	United States Government Interagency Domestic Terrorism Concept of Operations Plan
COOP	Continuity of Operations Plans
CPX	Command Post Exercise
CST	Civil Support Team (National Guard WMD – CST)
CT/NP-ESG	Counter-Terrorism and National Preparedness Exercise Sub-Group
CYBEREX	Cyber Exercise

D

DC	District of Columbia
D-Day	D-Day (-/+) (T2 Full Scale Exercise Start Date)
DEST	Domestic Emergency Support Team
DFO	Disaster Field Office (FEMA)
DHS	Department of Homeland Security
DHS CAT	DHS Crisis Action Team
DHS CBP	DHS Bureau of Customs and Border Protection
DHS EP&R	DHS Emergency Preparedness and Response
DHS ICE	DHS Immigration and Customs Enforcement
DHS/ODP	DHS Office for Domestic Preparedness
DHS/OER	DHS Office of Emergency Response
DHS/TSA	DHS Transportation Security Agency
DMAT	Disaster Medical Assistance Team
DMORT	Disaster Mortuary Operational Response Team
DOD	Department of Defense
DOE	Department of Energy
DOE RAP	DOE Radiological Assistance Program

DOE AMS	DOE Aerial Measuring System
DOE ARAC	DOE Atmospheric Release Advisory Capability
DOE NNSA	DOE National Nuclear Security Administration
DOH	Department of Health
DOH/DRP	"Washington State Department of Health, Division of Radiation Protection Plan and Procedures for Responding to a Radiological Attack"
DOI	Department of Interior
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOS S/CT	DOS Office of the Coordinator for Counterterrorism
DOT	Department of Transportation
DOT CMC	DOT Crisis Management Center
DPH	Department of Public Health
DSHL	Deputy State Health Liaison (Washington State)
DTRA	Defense Threat Reduction Agency
DTRA HPAC	DTRA Hazard Prediction and Assessment Capability

E

ED	Emergency Department
EDT	Eastern Daylight Time
EIS	CDC Epidemic Intelligence Service
EMnet	Emergency Management Network
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EPA	Environmental Protection Agency
EPA RRC	EPA Regional Response Center
EPA RERT	EPA Radiological Emergency Response Team
EPI	Emergency Public Information
EP&R	Emergency Preparedness and Response (DHS)
EPR	Emergency Preparedness and Response (DHS)
ER	Hospital Emergency Room
ERT	Emergency Response Team

ERT	Evidence Response Team (FBI)
ESF	Emergency Support Function
ESMARN	Emergency Services Mutual Aid Radio Network
ESP	Extranet Secure Portals
EST	FEMA Emergency Support Team
EXPLAN	Exercise Plan

F

FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FBI BDC	FBI Bomb Data Center
FBI CIRG	FBI Critical Incident Response Group
FBI ERT	FBI Evidence Response Team
FBI HMRU	FBI Hazardous Materials Response Unit
FBI HRT	FBI Hostage Rescue Team
FBI SAC	FBI Special-Agent in Charge
FCO	Federal Coordinating Officer
FDA	Food and Drug Administration
FE	Functional Exercise
FEMA	Federal Emergency Management Agency
FEMA EST	FEMA Emergency Support Team
FEMA NIEOC	FEMA National Interagency Emergency Operations Center
~~FOUO~~	For Official Use Only
FPS	Federal Protective Service
FRA	Federal Railroad Administration
FRERP	Federal Radiological Emergency Response Plan
FRMAC	Federal Radiological Monitoring and Assessment Center
FRP	Federal Response Plan
FSE	Full Scale Exercise
FSL	Federal, State, & Local

G

GIS	Geographic Information System
GLODO	Group for the Liberation of Orangeland & the Destruction of Others

GMT	Greenwich Mean Time
GSA	General Services Administration

H

HAN	Health Alert Network
HAM	Amateur Radio Operator
HAZMAT	Hazardous Material
HDER	DOE/DOJ Homeland Defense Equipment Reuse program
HHS	Health and Human Services
HHS ASPHEP	HHS Assistant Secretary Public Health Emergency Preparedness HHS
HHS SERT	HHS Secretary's Emergency Response Team
HHS SCC	HHS Secretary's Command Center
HIPAA	The Health Insurance Portability and Accountability Act
HMRU	Hazardous Materials Response Unit (FBI)
HPAC	Hazardous Predicting Assessment Capabilities
HQ	Headquarters
HRT	Hostage Rescue Team (FBI)
HSAS	Homeland Security Advisory System
HSC	Homeland Security Council
HSCenter	Homeland Security Center (DHS)
HSPD-3	Homeland Security Presidential Directive-3, *"Homeland Security Advisory System"*
HSPD-5	Homeland Security Presidential Directive-5, *"Management of Domestic Incidents"*
HUD	Department of Housing and Urban Development

I

I-5/I-90	Interstate Highway 5/ Interstate Highway 90
IA	Interagency
IAIP	Information Analysis and Infrastructure Protection (DHS)
IC	Incident Commander
ICE	Immigration and Customs Enforcement (DHS)
ICS	Incident Command System
ICU	Hospital Intensive Care Unit

IDPH	Illinois Department of Public Health
IEMA	Illinois Emergency Management Agency
IL	Illinois
ILCS	Illinois Compiled Statutes
IL DOT	Illinois Department of Transportation
IMERT	Illinois Mobile Emergency Response Team
ING	Illinois National Guard
IOHNO	Illinois Operational Headquarters and Notification Office
IPS	Illinois Pharmaceutical Stockpile
ISO	Incident Safety Officer
IST	Incident Support Team
IUSAR	Illinois Urban Search and Rescue Team
IV	Intravenous

J

JIC	Joint Information Center
JOC	Joint Operations Center
JTF	Joint Task Force (DOS)
JTTF	Joint Terrorism Task Force

K

KC	King County, (Washington)
KCC	King County Charter, (Washington)
KCOEM	King County Office of Emergency Management
KLERN	Kane Local Emergency Radio Network (Kane County, IL)

L

LFA	Lead Federal Agency
LINC	Local Integration to access NARAC with Cities program
LNO	Liaison Officer
LSG	Large Scale Game

M

MALS	Mobil Analytical Laboratory System

MCC	T2 Exercise Master Control Cell
MCFR	Montgomery County (Maryland) Fire Rescue
MCHC	Metropolitan Chicago Healthcare Council
MD	Medical Doctor
MERRT	Medical Emergency Radiological Response Team (Veterans Affairs)
MERS	Mobile Emergency Response System (National Guard)
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSEL	Master Scenario Events List

N

NARAC	National Atmospheric Release Advisory Capability
NASA	National Aeronautics and Space Administration
NCP	National Oil & Hazardous Substances Pollution Contingency Plan
NCR	National Capital Region
NCR FE	National Capital Region, Functional Exercise
NDMS	National Disaster Medical System
NIEOC	National Interagency Emergency Operations Center
NIMS	National Incident Management System
NNSA	National Nuclear Security Administration
NOAA	National Oceanic and Atmospheric Administration
NRC	Nuclear Regulatory Commission
NRP	National Response Plan
NSC	National Security Council
NSC PCC	National Security Council, Policy Coordinating Committee
NSC PCC (CT/NP-ESG)	National Security Council, Policy Coordinating Committee, Counter Terrorism and National Preparedness Exercise Sub-Group
NWS	National Weather service
NY	New York

O

ODP	Office for Domestic Preparedness
OEM	Office of Emergency Management
OER	Office of Emergency Response (DHS)

ONCRC	Office of National Capital Region Coordination
OPFOR	Opposing Force – Opposition Force
OSHA	Occupational Safety and Health Administration

P

PA	Public Address system
PAG	Protective Action Guidelines
PCC	Policy Coordinating Committee
PCR	Polymerase Chain Reaction
PDD-39	Presidential Decision Directive–39 *"U.S. Policy on Combating Terrorism"*
PDT	Pacific Daylight Time
PFD	Phoenix Fire Department
PFO	Principle Federal Official
PHSKC	Public Health Seattle/King County
PIO	Public Information Officer
POC	Point-of-Contact
POD Hospital	Illinois Disaster POD Hospital. Term used by the IDPH disaster plan for hospitals designated to consolidate and coordinate regional bospital medical information for further transmission to IOHNO.
PPE	Personal Protective Equipment
PROFLOW	Procedural Flow Synopsis
PRO-NET	Professional Reporting Network (DuPage County)

Q

R

RAP	Radiological Assistance Program
RCW	Revised Code of Washington
RD	Region Director (FEMA)
RDD	Radiological Dispersion Device
REOC	Regional Emergency Operations Center
RERT	Radiological Emergency Response Team (EPA)
RN	Registered Nurse
ROC	Regional Operations Center (FEMA)

RMAC	Radiation Monitoring and Assessment Center (Washington State)
RRC	Regional Response Center (EPA)

S

SAC	Special-Agent in Charge (FBI)
SAMHSA	The Substance Abuse and Mental Health Services Administration
SARS	Severe Acute Respiratory Syndrome
SCC	Secretary's Command Center (HHS)
SDS	Same Day Surgery
SeaTac	Seattle-Tacoma International Airport
SEO	Senior Energy Official
SEOC	State of Illinois Emergency Operations Center
SERT	Secretary's Emergency Response Team (HHS)
SFD	Seattle Fire Department
SHL	State Health Liaison (Washington State)
SIOC	Strategic Information and Operations Center
SIRT	The State Interagency Response Team (Illinois)
SME	Subject Matter Expert
SNS	Strategic National Stockpile
SNSOC	Strategic National Stockpile Operations Center
SODO	South of Downtown district of Seattle
SPD	Seattle Police Department
S&T	Science & Technology (DHS)
STB	Surface Transportation Board

T

TOPOFF	TOP OFFICIALS EXERCISE SERIES
"TOPS"	TOPOFF Pulmonary Syndrome
T2	TOPOFF 2
T2 FSE	TOPOFF 2 Full Scale Exercise
T2 LSG	TOPOFF 2 Large Scale Game
TFR	Temporary Flight Restrictions
TOPS syndrome	TOPOFF Pulmonary Syndrome
TSA	Transportation Security Agency

TTX	Table Top Exercise
TV	Television
TX	Texas

U

US	United States
USAR	Urban Search and Rescue
USCG	United States Coast Guard
USDA	United States Department of Agriculture
USGS	United States Geological Survey
UT	Universal Time
UTC	Coordinated Universal Time

V

VA	Department of Veterans Affairs
VA MERRT	VA Medical Emergency Radiological Response Team
VCC	T2 Exercise Venue Control Cell
VMI	Vendor Managed Inventory
VNN	Virtual News Network
VTC	Video Teleconference

W

WA	Washington
WA DOH	Washington State Department of Health
WA DOT	Washington Department of Transportation
WDOT	Washington Department of Transportation
WHO	World Health Organization
WMD	Weapons of Mass Destruction

X-Y-Z

TOP OFFICIALS (TOPOFF) EXERCISE SERIES:

TOPOFF 2 (T2) After Action Report ANNEX A

September 30, 2003

This page intentionally left blank

TOPOFF 2 Electronic Reconstruction Product

NOTE TO USERS:

Background: This file provides an electronic, searchable reference of significant domestic (United States) events and decisions that occurred in the TOPOFF 2 (T2) Full Scale Exercise (FSE) between May 12-May16, 2003. The events in this reconstruction took place in 3 venues: the State of Washington (WA), State of Illinois (IL), and Washington DC (referred to as the "Interagency," and abbreviated as "IA"). It was developed through the reconstruction process detailed in the T2 After Action Report (AAR) and distilled from more than 20,000 lines of raw data entered directly from data collector logs, controller records, participant and agency logs, situation reports, and emails. This file is NOT data. It reflects analysis and follow-up work by analysts to deconflict data within and between venues. Its purpose is as a reference to participating and non-participating entities to provide them a sense of the significant events, activities, and decisions that were faced by the national response community in response to the events in the T2 FSE scenario- a perspective no single agency could have on its own. This does not provide a detailed account of any particular agency's actions.

Additional Notes:

Note that all times reflect Eastern Daylight Time (EDT), which was the official exercise time. Original times have been converted in order to provide an integrated and time-synchronized perspective.

Note that the "Source" Column refers to the organization or organizations which submitted data to support the event/activity/decision listed. There may have been additional organizations that documented any given event/activity/decision.

An Acronym list is provided for the entire Reconstruction as well as for references specific to each venue.

All events/activities/decisions are associated with the venue of their occurrence in the "Venue" column.

The Reconstruction ends with the last event/activity of significance in the FSE at 204 hours on 15 May.

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IA	12-May-03	14:00	INJECT: The DEST departs Andrews Air Force Base in response to a credible threat against the Columbia Generating Station in Richland, WA. (MSEL # 3042)	Event was notional so time is notional		DOT CMC
IA	12-May-03	14:58	At 11:58 Virtual News Network (VNN) begins coverage of an explosion in the South of Downtown (SODO) District in Seattle, WA.	Time ranges from 11:58 to 12:03 PDT (14:58 to 15:03 EDT). Time choosen was from WA VCC Official time and MSEL Team log.	MSEL; TopOff Log;Data Collector Logs; Data Collector Log; Analyst Log; Data Collector Logs; Data Collector Log	WA State EOC; KC EOC; RDD site; VNN; FEMA Region X ROC; KC RJIC
IL	12-May-03	15:00	IL SEOC reports that there has been a reported explosion in Seattle. At this point, it is not certain what the cause of the explosion was. Agency liaisons to be contacted to report to the IL SEOC. Advised to notify IEMA Director.		SEOC Event Log	IL State EOC
WA	12-May-03	15:00	Upon watching the initial VNN report, FEMA Region X Regional Operations Center (ROC) Director notified Emergency Support Function (ESF) lead agencies and requested they send liaisions to staff the ROC (corresponds to MSEL # 2052).	Time taken was from data collector at the IOF, other timeswere recorded at 14:02 and 13:10 PDT (17:02 and 16:10 EDT) by the MSEL team from unknown sources. Action initiated from VNN report In fact many ESF representatives actually came to the EOC that morning, before STARTEX.	Data Collector Log	FEMA IOF
IA	12-May-03	15:00	SNS Operations Center activated		CAT team operations report	DHS CAT
IL	12-May-03	15:03	Chicago OEMC elevates local alert level from Yellow to Orange		Data Collector Log	Chicago EOC
WA	12-May-03	15:03	Upon watching the initial VNN report, Seattle EOC notifies the King County EOC of an explosion in the SODO District of the city (corresponds to MSEL # 2023).	Time was taken from first report to KC EOC by Seattle EOC at 12:03 PST (15:03 PDT). Other times are 12:04 PDT (15:04 EDT) from the MSEL spreadsheet, 12:10 PDT (15:10 EDT) from the same data collector reporting 12:03 PDT (15:03 EDT), and 12:28 PDT (15:28 EDT) from the MSEL spreadsheet.	MSEL; Data Collector Logs	Seattle EOC; KC EOC; WA State EOC
WA	12-May-03	15:04	Based on VNN report, Seattle FBI Field Office Operations Coordinator notifies SIOC (corresponds to MSEL # 2017)	Time was chosen from data collector log at WA State EOC. SIOC OPS Coordinator Log records notification at the same time	Data Collector Log	WA State EOC
IL	12-May-03	15:05	IL SEOC activated		Data Collector Log	IL State EOC
WA	12-May-03	15:05	After watching the initial VNN report, the Seattle EOC notifies Washington State Ferry (WSF) EOC of the explosion in the SODO District of the city. They acknowledge that they are aware of the problem and have activated their EOC (corresponds to MSEL # 2015).	Time used was obtained from WSF Lead Controller at WSF EOC, Other times were 12:06 PDT (15:06 EDT) from a Seattle EOC DC and 12:10 PDT (15:10 EDT) from the MSEL Team (unknown source).	MSEL Team	
WA	12-May-03	15:08	STARTEX: At 12:08 an explosion occurs at the intersection of 6th Ave S and South Hanford Street (MSEL # 2005).	STARTEX was delayed by VCC Director for 10 minutes due to placement of victims. Time taken was from WA VCC Official time, analyst on site at RDD and MSEL Team log. Other reported times ranged from 12:08 to 12:10 PDT (15:08 to 15:10 EDT).	MSEL Team; Analyst Log	RDD site
WA	12-May-03	15:09	INJECT: Seattle Police and Fire dispatch simulate getting 911 calls. Seattle Police notifies nearby units to respond and investigate. Based on the simulated call volume and call descriptions, Seattle Fire sends an appropriate response (MSEL # 2006).	Police and Fire dispatch were part of the exercise SIMCELL. The initial dispatches that were sent out were done as injects not as reactions to 911 calls. There were no simulated 911 calls.	MSEL	MSEL
WA	12-May-03	15:10	Seattle EOC Director begins the EOC's notification chains (corresponds to MSEL # 2014).	Time taken from Seattle EOC DC log.	Data Collector Log	Seattle EOC
WA	12-May-03	15:10	First responding units arrive on scene, including SFD Engine #2, ambulance and 9 SPD patrol cars. All of these units initially still alarmed or on-viewed (self-dispatched) based on hearng the explosion (corresponds to MSEL # 2010).	Information taken from several DC log entries that occur between 12:08 and 12:13 PDT (15:08 and 15:13 EDT).	Data Collector Logs	RDD site; KC EOC; Harborview EOC
WA	12-May-03	15:10	Public Health-Seattle&King County (PHSKC) EOC activates in response to the notification by the Seattle EOC of the explosion (corresponds to MSEL # 2018).	No data points suggest that PHSKC EOC was notified by Hospial Control as was called for in the MSEL. At 12:10 PDT (15:10 EDT) Seattle EOC notified PHSKC EOC. At 12:25 PDT (15:25 EDT) the incident commander notified PHSKC EOC as well.	Data Collector Log	Seattle EOC
WA	12-May-03	15:10	WA SEOC notified of the explosion and activated to Phase III (corresponds to MSEL # 2025)	Time notes when WA SEOC was notified, not by whom (MSEL called for the WA SEOC to be notified by the Seattle EOC). Time as taken from data collector at WA SEOC. Other times collected by the MSEL team were 12:11 and 12:30 PDT (15:11 and 15:30 EDT).	Data Collector Log; MSEL Team	WA State EOC
WA	12-May-03	15:10	FEMA Region X informed that the WA SEOC is activated (corresponds to MSEL # 2039)	Time taken was from DC in WA SEOC. WA SEOC made call based on VNN report, not actual detonation. Other times reported were 12:36 by the MSEL team and 12:00 by the FEMA VCC Rep.	EOC Supervisor Log; MSEL Team	WA State EOC
IA	12-May-03	15:11	Message sent by HHS Secretary's Command Center (SCC) to COOP Notification, through Roam Secure Alert Network: A large explosion in the SODO District of Seattle, WA, unknown source of explosion, unknown injuries.		Agency Log	DHS/HS Center
WA	12-May-03	15:12	SFD announced that victims who can walk should slowly approach Engine #2; those who need help are instructed to stay where they are	Announcement started at 12:12 PDT (15:12 EDT) and was continuous to at least 12:18 PDT (15:18 EDT).	Data Collector Log	RDD site
WA	12-May-03	15:12	Seattle EOC activated to Phase III operations		Seattle EOC Log	Seattle EOC
WA	12-May-03	15:12	Washington State Emergency Management Division (WA EMD) Director calls the WA SEOC and orders a Phase III (Full Operations) activation.		Data Collector Log	WA State EOC
IA	12-May-03	15:12	EPA Region 10 On Scene Coordinator deployed to incident site		Data Collector Log	EPS Aux. Ops Ctr

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	12-May-03	15:14	CPD notified the following departments and agencies about the explosion in Seattle:		Data Collector Log	Chicago EOC
IL	12-May-03	15:15	Chicago EOC Activated		Data Collector Log	Springfield IL EOC
IA	12-May-03	15:15	Report to SIOC that the FBI SAC has been notified, the ERT and SWAT recalled, and an on-scene commander dispatched		OPS Coordinator Component Log	SIOC
IA	12-May-03	15:20	FEMA EOC receives call from FEMA Region X ROC reporting a bomb blast in Seattle		OPS Coordinator Component Log	FEMA EOC
WA	12-May-03	15:21	Based on the report from the City of Seattle Emergency Operation Center regarding a large explosion in the vicinity of 2700 Airport Way, the King County Emergency Operation Center (EOC) has been activated at Level III. The cause of explosion is unknown; no other details are available at this time.		Press Release	KC IC
WA	12-May-03	15:22	INJECT: Seattle Fire Department Unit 77 (HAZMAT) simulated responding from Station 2 (SFD HQ). This would have brought them through the plume, so as they were responding controllers informed players that there radiation pagers alarmed (MSEL # 2013).	Time came from Fire Alarm Center's call log. Unit 77 (HAZMAT) immediately called in when there radiation pager alarmed. Data Collector logs had the time at 12:29 PDT (15:29 EDT) from the KC EOC, 12:22 PDT (15:22) EDT from radio traffic overheard at the RDD Site, and 12:21 PDT (15:21 EDT) from the SFD FAC.	Data Collector Logs	KC EOC; RDD Site; SFD FAC
WA	12-May-03	15:25	A traige station is being set up near Ladder 7 and multi casualty units, 150 yrds south of bomb site	Time taken was from RDD Site Technical Decon Controller. Only clear data point about Triage.	Data Collector Log	RDD site
IA	12-May-03	15:25	SIOC receives report from DHS that radiation was detected in Seattle		Data Collector Log	FBI SIOC
IA	12-May-03	15:25	VNN update: unconfirmed report of detection of radiation		Data Collector Log	CDC EOC Atlanta
WA	12-May-03	15:29	At 1230 the city of Seattle lead PIO authorizes a press release acknowledging the activation of the EOC and response of the city's first responders to an explosion. Text: FOR IMMEDIATE RELEASE 1230, 12 May 2003 SUBJECT: FOR MORE INFORMATION CONTACT: Seattle EOC Activated City of Seattle EOC Media Line: (206) 233-5072 http://www.seattle.gov City of Seattle Activates Emergency Operations Center to respond to emergency south of downtown Seattle The Seattle Police Chief activated the City of Seattle's emergency operations center just past noon today in response to an explosion south of downtown Seattle. Police and Fire personnel are on scene to determine the nature of the blast. Citizens are urged to avoid the area within a mile of Airport Way S. and S. Hinds Street. The Seattle Mayor is being briefed and will address the public as soon as possible.		Press Release	Seattle EOC
WA	12-May-03	15:30	Washington State Top Officials in the WA SEOC Policy Room alert the Washington State National Guard WMD Civil Support Team to go on standby and prepare to deploy in support of the City of Seattle.		EOC Supervisor Log	WA State EOC
WA	12-May-03	15:30	FBI SAC notified that radiation was detected at the incident site. The SAC requested the DEST and HMRU and requested that the SIOC be notified (corresponds to MSEL # 3045).	Time taken was from FBI SAC Log, but where the notification came from is not noted (MSEL called for notification to come from the Seattle EOC). Other time 12:35 PDT (15:35 EDT) from MSEL Team - source unknown.	SAC Log Data; MSEL Team	FBI WA Field Office
WA	12-May-03	15:32	The Washington State Ferry EOC locked down all ferried and shut down service (corresponds to MSEL # 2026).	Time was taken from WA SEOC data collector observing WSP. Earliest time reported that Ferries were shut down. This entry was recorded later, but specifically mentions 12:32 PDT (15:32 EDT) as shut down time. Other entries merely not time call was received or are time update was given, not time ferries were shut down. Other reported times - 13:25 PDT (16:25 EDT) from a DC at the KC EOC, MSEL team times 12:34 PDT (15:34 EDT) reported to the MSEL team from an unknown source, and 12:40 PDT (15:40 EDT) reported to the MSEL team from the WSF Lead Controller.	Data Collector Log; MSEL Team	KC EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	12-May-03	15:32	INJECT: The detection of cesium was injected to the Incident Commander. The MSEL item represented was the time that the FBI thought they would detect it. The IC controller saw the time come and pass and injected this information without permission from the VCC. Other times recorded for this occuring were 13:30 and 14:15, captured by MSEL team, source unknown (MSEL # 2031).	The detection of cesium was injected to the Incident Commander. The MSEL item represented was the time that the FBI thought they would detect it. The IC controller saw the time come and pass and injected this information without permission from the VCC. Other times recorded for this occuring were 13:30 and 14:15 PDT (16:30 and 17:15 EDT), captured by MSEL team, source unknown.	MSEL Team	WA VCC
IL	12-May-03	15:33	DuPage County EOC notified IL SEOC of explosion in Seattle; moving to initiate EMNet (satellite based point-to-point secure communications network of all EOC's)		Data collector Log	DuPage Co. EOC
IL	12-May-03	15:35	IEMA notified CCSEMA about an explosion in Seattle with possible detection of radiation. Also notified that IEMA has opened its EOC		Message & Event Log	CCSEMA
IA	12-May-03	15:35	INJECT: HHS SCC notifies HHS SERT of the incident in Seattle (MSEL # 3106)		Data Collector Log	FDA EOC
IL	12-May-03	15:36	Chicago EOC holds Radioactive Dispersal Devices (RDDs) consequence briefing		Data Collector Log	Chicago EOC
WA	12-May-03	15:36	This is the time in the MSEL that SFD HazMat and/or SPD Arson/Bomb Squad was to receive radiation alerts on their monitoring devices. There are no clear observations from data collectors. Many report HAZMAT or ABS showing up on scene and some of their activities, but there are no clear descriptions of them confirming the radiation readings (corresponds to MSEL # 2024).		MSEL Team	WA VCC
IA	12-May-03	15:37	Message sent by HHS SCC to COOP Notification, through Roam Secure Alert Network: Radiation has been detected in the explosion in the SODO District of Seattle. Unknown radiological type and level.		Agency Log	DHS/HS Center
WA	12-May-03	15:38	WA EMD Director approves the first press relase acknowledging an event in the City of Seattle and describing WA State's current response to the situaton. Press Release: CAMP MURRAY, WA- The State Emergency Operations Center (EOC) at Camp Murray was activated at 12:10 p.m. today in response to an explosion in the south. The WA Governor has been informed of the incident. Representatives from the state departments of Military (Emergency Management); Health; Transportation: Ecology; Agriculture; and the State Patrol as well as the American Red Cross are reporting to the State EOC.	Press release was from DC notes. may not be exact wording.	Data Collector Log	WA State EOC
WA	12-May-03	15:40	Decontamination area being established at incident site		Data Collector Log	RDD site
WA	12-May-03	15:40	WA Governor has been informed of the incident.		Press Release	WA State EOC
IA	12-May-03	15:40	CDC EOC Emergency Response Coordinator prepares message to notify CDC's centers, institutes & offices of the radiological incident in Seattle		Data Collector Log	CDC EOC Atlanta
IA	12-May-03	15:40	FDA receives phone call from HHS SCC confirming radiation of unknown source in Seattle		Data Collector Log	FDA, EOC Rockville, MD
WA	12-May-03	15:41	King County EOC posts notification that security level is RED		Data Collector Log	KC EOC
IL	12-May-03	15:42	Chicago EOC notified BOMA, Sears, Aon Center, Hancock Buildings regarding potential terrorist threat		Data Collector Log	Chicago EOC
IA	12-May-03	15:42	FDA EOC activated		Data Collector Log	FDA, EOC Rockville, MD
IA	12-May-03	15:42	TSA desk at DOT CMC receives phone call from TSA representative at DHS confirming radiation in Seattle		Data Collector Log	DOT CMC
IA	12-May-03	15:44	VACO receives confirmation from DHS that radiation has been detected in Seattle		Data Collector Log	VA Central Office
IL	12-May-03	15:45	Chicago DPH reports HAN is looking for unusual disease clusters		Data Collector Log	Chicago DPH
IL	12-May-03	15:45	CPD feels that an attack by terrorist group "GLODO" is imminent; looking at nuclear targets. Chicago is at a "heightened alert" status, increasing awareness and vigilance at possible targets		SEOC Event Log	IL State EOC
IA	12-May-03	15:50	Reports coming in to HHS SCC from DHS about Pu 229, Ce 137, and Americium	While this did occur in the exercise, there is no way that the three radioactive components could have been identified this early in the exercise. HHS liaisons in WA discounted this information and it did not impact play.	Data Collector Log	HHS
WA	12-May-03	15:51	No chemical agents detected at the incident site	Actual time was between 12:51 and 12:59 PDT (15:51 and 15:59 EDT)	Data Collector Log	RDD site
IA	12-May-03	15:57	HHS sending SERT to Region X REOC		Data Collector Log	HHS
IA	12-May-03	15:57	Region X REOC officially activated		Data Collector Log	HHS
IA	12-May-03	15:57	HHS receives request from DHS to identify HHS assets that are available to deploy - need for brief to DHS Secretary		Data Collector Log	HHS

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	12-May-03	15:59	Hospital Control contacting all western WA hospitals with exception of Monroe County		Data Collector Log	Harborview EOC
WA	12-May-03	16:00	SFD advises SPD to set up a command post next to SFD command post for communication purposes. SPD Incident Commander directs arriving SPD personnel to set up perimeter		Data Collector Log	RDD site
WA	12-May-03	16:00	At 13:00 FEMA ROC Region X received notification that the Consequence Mangenemt Group at the JOC was stood up.		Data Collector Log	FEMA Region X ROC
IA	12-May-03	16:00	INJECT: DOS task force stands up in response to the explosion in Seattle (MSEL #4040)		Data Collector Log	HHS
IA	12-May-03	16:00	HHS SCC requests that CDC assemble team of SMEs that can potentially deploy to Seattle (corresponds to MSEL # 3111)		Data Collector Log	CDC EOC Atlanta
IL	12-May-03	16:01	Chicago EOC receives information from Chicago DPH that the HSAS has been elevated to RED. Chicago EOC holds at ORANGE until the information can be confirmed.		SEOC Event Log	IL State EOC
WA	12-May-03	16:02	FEMA Liaison reports that DHS Secretary dispatched a Forward Coordinating Team to assist the IC with determining resource needs.		Agency Log	WA State EOC
IA	12-May-03	16:02	DHS CAT Situation Report contains update that Greater Seattle is Threat Level RED		Situation Report	DHS-CAT
WA	12-May-03	16:03	SFD receives plume prediction from NARAC showing cloud moving N x NW (corresponds to MSEL # 2038)		MSEL	MSEL
WA	12-May-03	16:04	Law Team preparing Mayoral Proclamation of Civil Emergency Order Delegation of Authority. This was done in consultation with Mayor's general counsel		Agency Log	WA State EOC/Seattle EOC
IL	12-May-03	16:05	Chicago EOC contacted METRA, RTA, and CTA and briefed them on the situation; 'self-evacuation' locomotives back in town; decide to have CTA start "Rush Hour" earlier		Data Collector Log	Chicago EOC
WA	12-May-03	16:05	WA SEOC policy group asked staff to start on Governor's proclamation		EOC Supervisor Log	WA State EOC
WA	12-May-03	16:05	Air Space closure had been requested by IC and the WA SEOC, 5 mile radius and up to 1000 feet.		Agency Log	WA State EOC/Seattle EOC
IA	12-May-03	16:05	INJECT: FBI SIOC to Issue warning order to Crisis Medical Response Asset (corresponds to MSEL # 3673)		Data Collector Log	FBI SIOC
WA	12-May-03	16:06	Discussion at IC ensues about the NARAC model which leads to a recommendation to set up a 10 mile area where citizens should remain in doors. They can recommend this but there is not enough manpower to enforce it.		Data Collector Log	RDD site
WA	12-May-03	16:07	WA SEOC policy group asked staff to start on request for a presidential disaster declaration.		Data Collector Log	WA State EOC
IA	12-May-03	16:08	FAA reports to DOT Chief of Staff: Temporary Flight Restriction (TFR) has been issued for 30 mile radius around SEATAC airport air traffic control tower up to 20,000ft. All in bound traffic has been re-directed.		Data Collector Log	DOT CMC
WA	12-May-03	16:09	King County Executive instructs EOC staff to notify King County employees working in Seattle - tell them to shelter in place, but prepare for them to move		Data Collector Log	KC EOC
IL	12-May-03	16:10	Chicago EOC displaying Shelter-In-Place activities in Seattle; enacted vehicle parking prohibition near target areas in and around Chicago		Data Collector Log	Chicago EOC
IA	12-May-03	16:10	ICE Situation Room and ICE HQ Reporting Center activated.		Situation Report	DHS-CAT
IA	12-May-03	16:10	CDC NCEH convenes the Preliminary Assessment Team (PAT) to discuss the radiological event. The PAT agrees to activate the EOC - meaning response operations and associated support will center in the EOC. Additionally, the PAT discussed the potential radiological elements being reported--Plutonium 238/239, Cesium 137 and Americium. Most of the discussion focuses on the [exercise] "validity" of the elements reported to have been detected, given the detectors available on-scene at this time. CDC's lead for radiation indicated the only detection devices of a portable nature detect gamma emissions and therefore would not be able to detect these elements. CDC staff also alerted to be prepared to deploy to Seattle to support FRMAC		Data Collector Log	CDC EOC Atlanta
WA	12-May-03	16:14	Seattle EOC PIOs issue press releases in multi-languages		Agency Log	Seattle EOC
IA	12-May-03	16:15	EPA Auxiliary Operations Center receives report that radioactive materials have been detected in field at Seattle.		Data Collector Log	EPS Aux. Ops Ctr
IL	12-May-03	16:17	IDPH advises Chicago OEMC of change in alert status from Orange to Red; but not confirmed.		Data Collector Log	Chicago EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	12-May-03	16:17	Seattle DOT informed SPD of their recommendation to halt all traffic coming into downtown. They are developing a traffic plan.		Seattle EOC Log	Seattle EOC
IL	12-May-03	16:20	ARC of Greater Chicago received message that radiological activity detected in Seattle		Data Collector Log	ARC of Greater Chicago HQ
IA	12-May-03	16:20	FEMA EST receives request for 3 WMD task forces from ESF-9		Data Collector Log	FEMA EST
IA	12-May-03	16:20	NAWAS carried a message that the NCR had gone to RED.	The NCR had not gone to RED at this time	Data Collector Log	HHS
IA	12-May-03	16:26	HHS EOC inquiring as to source of Seattle weather data (e.g., wind direction). CDC radiation division is working on short / long term effects of the radiation release and will get information to hospitals on the isotopes.		Data Collector Log	HHS
IA	12-May-03	16:28	DHS HS Center received call from OSLGC Homeland Operations Center saying that the Federal Protection Services reported that the City of Seattle raised threat level to Red.		HSC OSLGC Incident Log	DHS/HS Center
WA	12-May-03	16:29	Update on WA DOT Road Closures: I-5 at I-405 north bound (Tukwilla) at I-5 at I-405 soundbound (Lynnwood), thus I-5 is closed down. I-90 and SR 520 are closed west bound into the City of Seattle, and the west bound lanes have been opened to Emergency routes east bound from the city of Seattle. Washington State Ferry EOC has shut down all routes and Ferry operations		IAP Section Activity Log	WA State EOC
WA	12-May-03	16:34	SPD SWAT and SPD EOD agree to link up together before either go into target area		Data Collector Log	RDD site
IA	12-May-03	16:34	FBI SIOC and DHS are considering redeployment of DEST		Data Collector Log	FBI SIOC
IL	12-May-03	16:35	ARC of Greater Chicago received notification from Chicago OEMC that alert status raised to Red		Data Collector Log	ARC of Greater Chicago HQ
IL	12-May-03	16:35	Director of Chicago OEMC advises that change to Red is unconfirmed; hold at Orange until HSAS notification		Data Collector Log	Chicago EOC
WA	12-May-03	16:35	FBI ASAC: DEST assets redeployed; Ce137 identified; TSA closed airports and airspace; upcoming press conference-not releasing anything of substance/no video		Analyst log	FBI Command Group Mtg
IA	12-May-03	16:35	INJECT: At the request of the Seattle SAC the SIOC requests DHS redirect the DEST to Seattle from the Columbia Generating Station in Hanford, WA.		TSA Daily Watch Log	DHS/CAT
WA	12-May-03	16:35	DOE Region 8 RAP Team receives call requesting assistance from WA DOH (corresponds to MSEL # 2037)	Time taken is from DOE RAP review comments. Other times recorded are from a WA SEOC data collector at 13:56 PDT (16:56 EDT); other times reported to the MSEL team are 13:00 and 13:57 PDT (16:00 and 16:57 EDT) from unknown sources.	AAR Review Comments	DOE RAP
IA	12-May-03	16:36	DOT CMC update: Washington State Ferry system shut down, FHWA reports I-5 is closed, I-90 is closed westbound / open eastbound near blast site.		Data Collector Log	DOT CMC
IA	12-May-03	16:37	DHS has activated NDMS		Data Collector Log	HHS
IA	12-May-03	16:37	DHS moving assets forward. On alert: 4 DMATs, NMRT-C, Region 10 DMORT, DPMU team, MST, DMORT WMD, IMSURT.		Data Collector Log	HHS
IA	12-May-03	16:37	HHS SCC noted that as yet there had been no Federal declaration--hence, OER advised against activation of ESF 8.		Data Collector Log	HHS
WA	12-May-03	16:39	SPD mobile command van now colocated with SFD mobile command van and SFD ICP		Data Collector Log	RDD site
IA	12-May-03	16:40	SIOC received report: Estimated 25 dead in Seattle blast area; blast zone is "hot"		Data Collector Log	FBI SIOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	12-May-03	16:42	Decision between SFD plans and SPD to combine both agencies planning processes together into a unified system		Data Collector Log	RDD site
IA	12-May-03	16:45	INJECT: DEST diverted to Seattle, WA. (MSEL # 3048)		ONCRC/USSS/DHS Activity Log	DHS/CAT
IA	12-May-03	16:45	INJECT: CDC & HHS ASPA craft an appropriate public health announcement in consultation with FBI JIC (MSEL # 3110)		Data Collector Log	HHS
IA	12-May-03	16:45	NNSA/HQ calls the NNSA/NV EOC to notify the CMRT Phase I and Phase II and the AMS (fixed-wing only) (corresponds to MSEL # 3132)		Data Collector Log	HHS
WA	12-May-03	16:45	At 13:45, the CST received notification from the WA SEOC to deploy to the incident site	The time used was from a post-exercise conversation with the CST Commanding Officer. The National Guard Component Log in the WA State EOC recorded this at 14:00 PDT (17:00 EDT)	Analyst Notes	CST Commanding Officer
WA	12-May-03	16:51	King County issued disaster declaration		Data Collector Log	FEMA Region X ROC
WA	12-May-03	16:54	FBI ASAC (Assistant Special Agent in Charge) and SPD IC have a discussion: There is no armed threat; SWAT and Bomb squads conducted secondary sweep. SFD cleared to go into hot zone for aid and rescue		Data Collector Log	RDD site
IA	12-May-03	16:58	Discussion in HHS SCC about declaring a Public Health Emergency	A Public Health Emergency was ultimately NOT declared for Washington	Data Collector Log	HHS
IL	12-May-03	17:00	Chicago EOC notifies Chicago DOT, Streets & Sanitation Dept., BOMA, Aon Center, Transunion building, IL Hotel & Lodging Assoc., North Michigan Avenue, Sears Building, Hancock Building, Merchandise Mart to suspend deliveries into buildings.		Data Collector Log	Chicago EOC
IA	12-May-03	17:00	INJECT: Consequence Management Agencies are notified to report to the SIOC (MSEL # 3401)		Data Collector Log	FBI SIOC
IL	12-May-03	17:02	IL SEOC confirms alert status still at Orange		Data Collector Log	ARC - Chicago HQ
WA	12-May-03	17:02	City employees are advised to stay at work and shelter in place until Seattle EOC receives further direction from the SFD		Agency Log	WA State EOC/Seattle EOC
IA	12-May-03	17:03	DOT CMC receives call from the Captain of the Port of Seattle: passenger ferry closed down as of 1515 EDT		Data Collector Log	USDOT HQ
IA	12-May-03	17:05	CDC Office of Communications begins coordination with HHS, inter-agency JIC, and local/State public affairs offices to craft health communication messages.		Data Collector Log	CDC EOC Atlanta
IA	12-May-03	17:05	Hundreds of doses of Prussian Blue are en route to Seattle from DOE. They will arrive at 2100. Discussions at HHS SCC pointed out the facts that 1) this amount would only treat 250 people for one week, and that therefore ought to be limited to exposed responders, and 2) Prussian Blue only counters the radiation coming from the Cesium.		Data Collector Log	HHS
IA	12-May-03	17:05	DOE deliberating sending DTPA to Seattle. DTPA is only useful in the first 6 hours after exposure. So DTPA in Oakridge Stockpile wont get there in time.		Data Collector Log	HHS
WA	12-May-03	17:06	Press conference on VNN with Seattle Mayor: estimate 50-60 injured; tells citizens to "shelter in place" if they are located south of Royal Brougham - west of Rainier Street - north of S. Alaska - east of Duwamish Waterway including Harbor Island		Data Collector Log	Washington State EOC
WA	12-May-03	17:08	Seattle Mayor declares State of Emergency		Agency Log	WA State EOC/Seattle EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IA	12-May-03	17:10	EPA OSC report to EPA HQ: EPA responders to start perimeter monitoring; also suggests monitoring and tracking of 1st responders.		Data Collector Log	EPA EOC HQ D.C.
IA	12-May-03	17:10	NCEH is notified that FEMA Region X ROC had become operational as of 1100 EDT.		Data Collector Log	CDC EOC Atlanta
IL	12-May-03	17:11	Chicago EOC distributes information that HSAS level is still ORANGE		Data Collector Log	ARC - Chicago HQ
IA	12-May-03	17:17	FBI SIOC reports radioactive plume moving toward or near SeaTac Airport from downtown Seattle.		Data Collector Log	FBI SIOC
IA	12-May-03	17:19	FBI update: 4 male suspects - one suspect in custody by Seattle Police Department; 3 at large		Data Collector Log	FBI SIOC
IA	12-May-03	17:20	DHS Secretary receives letter from WA Governor requesting release of pre-positioned equipment package (PEP) in Seattle; letter is forwarded to CAT.		Agency Log	DHS/HS Center
IA	12-May-03	17:21	HHS sends blood donation coordinator to talk to VNN and rectify the story on need for blood		Data Collector Log	HHS
WA	12-May-03	17:25	AMS (Aerial Monitoring System) deployment order issued		Data Collector Log	WA State EOC
WA	12-May-03	17:32	Washington State Governor declares a State of Emergency in Western Washignton in response to the explosion in Seattle (corresponds to MSEL # 2074). Text: I, Gary Locke, Governor of the state of Washington, as a result of the aforementioned situation and under Chapters 38.08, 38.52, and 43.06 RCW, do hereby proclaim that a State of Emergency exists in the Western Washington, and direct the supporting plans and procedures to the Washington State Comprehensive Emergency Management Plan be implemented. I also hereby order into active state service the Washington National Guard. I do hereby authorize the Washington Emergency Management Division to establish Food Control Areas around the areas that may be contaminated above protective action guidelines. The Washington State Departments of Health and Agriculture are authorized to issue food embargoes for the Food Control Area to redue the possibility of adulturated food form leaving the Food Control Area. Law enforcement agencies are authorized to stop and inspect vehicles departing an identified Food Control Area and to direct the vehicle operators to return food produced or grown to its point of origin within the Food Contro	Time taken was from WA State EOC Log. Additional times include 14:22 PDT (17:22 EDT) from State EOC's EMACS Section log, 14:40 and 15:00 PDT (17:40 and 18:00 EDT) from MSEL Team logs	Proclamation	WA State EOC
WA	12-May-03	17:34	DOH Representative at WA SEOC making request direct to FEMA for FRMAC team		Data Collector Log	WA State EOC
IA	12-May-03	17:35	DHS-CAT situation update report: FPS deployed to ROC, JOC, and all major federal locations in Seattle. FPS San Francisco is ready to send additional police officers to Seattle. Police officers were deploying with radiation detection devices to facilities northwest of the blast site and tracking prevailing winds.		Situation Report	DHS-CAT
IL	12-May-03	17:36	Kane County EOC reports that the Chicago EOC is up and running due to a possible attack in Chicago.		Data collector Log	Kane County EOC
IA	12-May-03	17:36	VNN report: Red Cross activates blood donor system.		Data Collector Log	HHS
IL	12-May-03	17:46	Kane Co. received EMNet Emergency Message that Lake Co. EOC has been partially activated because of Seattle bombing.		Data collector Log	Kane County EOC
WA	12-May-03	17:46	WA Governor's Proclamation of a State of Emergency forwarded to JOC		Washington National Guard Log	WA State EOC
IL	12-May-03	18:03	IEMA notified CCSEMA that the IL SEOC made a decision to shut down as of 17:00, lacking any definitive information or credible threat		Message & Event Log	CCSEMA

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	12-May-03	18:08	Seattle EOC requests DHS pre-positioned equipment package (PEP) located at Boeing Field		Data Collector Log	Seattle EOC
IA	12-May-03	18:10	Report to SIOC that Federal Hazmat teams, including first Federal radiation detection team, have arrived on-site in Seattle.		Data Collector Log	FBI SIOC
WA	12-May-03	18:11	Hospital control transferred to Overlake Hospital Medical Center from Harborview Medical Center due to broken water main at Harborview	Time chosen is when Overlake confirmed transfer of hospital control	Data Collector Log	Harborview EOC
IL	12-May-03	18:15	VNN reports that IL Governor has ordered increased security at nuclear power plants		SEOC Event Log	IL State EOC
WA	12-May-03	18:15	FRMAC authorized to deploy; estimated time of arrival in Seattle at 18:00.		FRMAC Log	FRMAC
WA	12-May-03	18:18	FBI Seattle ERT arriving at incident site		Data Collector Log	RDD site
WA	12-May-03	18:18	FBI California/San Francisco HMRT arriving on site		Data Collector Log	RDD site
IA	12-May-03	18:20	VNN report: Seattle hospitals receiving an overwhelming number of patients.		Data Collector Log	HHS
IL	12-May-03	18:29	Pro-Net alerts DuPage County Health Department to an increase in admissions of patients with respitory complaints to Edward Hospitals		Detailed Incident Report	DuPage County EOC
WA	12-May-03	18:40	FBI HMRU arriving on site		Data Collector Log	RDD site
IA	12-May-03	18:45	SCC receives Seattle casualty update: 2 fatalities and 92 hospitalized.		Data Collector Log	HHS
IL	12-May-03	18:46	Chicago DPH decides to send out dirty bomb information to the public, but will wait to send out information on the alert status		Data Collector Log	Chicago DPH
IL	12-May-03	18:49	Blast fax sent to 34 hospitals on information about radiological dispersion devices and for hospitals to increase surveillance; took 49 minutes to transmit		Data Collector Log	Chicago EOC
WA	12-May-03	18:55	Hospital control transferred back to Harborview Medical Center		Incident Log	Harborview EOC
IA	12-May-03	19:02	HHS SCC set up the CDC Emergency Comms System, and modified its website to highlight radiation information.		Data Collector Log	HHS
WA	12-May-03	19:20	WA Governor signed the request for Presidential Disaster Declaration		Operations Section Activity Log	WA State EOC
IA	12-May-03	19:23	In the FBI SIOC, presentation of DHS's list of seven threatened cities (Seattle, Chicago, New York, Los Angeles, San Francisco, Houston, and the District of Columbia) resulted in a discussion of whether these cities were close to nuclear power sites. If so, FBI would recommend transition to Red.		Data Collector Log	FBI SIOC
IA	12-May-03	19:35	DHS Secretary declared HSAS RED in Seattle.		TSA Daily Watch Log	DHS/CAT
WA	12-May-03	19:36	HHS Secretary and DHS Secretary discuss the deployment of additional health physicists to WA		Data Collector Log	REOC
IL	12-May-03	19:40	Chicago OEMC sends message to RTA, CTA, METRA to bring trains down and start rush hour early. Contacted BOMA, Transunion building, Sears, Aon Center, Hancock Towers, Streets and Sanitation: no parking, etc.		Data Collector Log	Chicago EOC
WA	12-May-03	19:45	King County employees whose job site is located inside the effected zone are to shelter in place until otherwise advised. King County employees who live inside the zone cannot return to their homes. Employees are encouraged to follow the transit plan set out by King County Metro Transit.		Press Release	KC IC
WA	12-May-03	19:45	Global message to King County employees - King County employees are allowed to leave anytime but are encouraged to check the Employee Hotline, at 206-205-8600, the King County Web site, and watch the local news tomorrow morning for updates and information about reporting to work.		Press Release	KC IC
IL	12-May-03	19:47	Edward Hospital reports admission of family of four suspected of SARS, but with unusual coughing up of blood. DuPage County Health Dept. called IDPH and other five hospitals to alert them.		Detailed Incident Report	DuPage County EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	12-May-03	19:50	SPD requesting FBI assistance at scene of explosion.	Briefing occurred at 17:30 PDT (20:30 EDT). Action took place sometime between 16:50 and 17:30 PDT (19:50 and 20:30 EDT), when the briefing took place.	Intelligence Summary Report (ISR) Seattle Division	WA State EOC
IA	12-May-03	20:00	HHS SCC orders two SNS sites nearest Chicago to be readied for loading onto the airplanes.		Data Collector Log	HHS
WA	12-May-03	20:20	DHS Secretary, in consultation with Seattle Mayor, has declared HSAS Red for the Seattle/King County area	Also recorded by a data collector at the FEMA IOF	FEMA activity Log	WA State EOC
IL	12-May-03	20:21	Director of Chicago OEMC reports that a telephone call from Chicago Dept. of Health & Human Services has raised the alert status from Orange to Red. While awaiting confirmation by Fax; all Chicago OEMC personnel/agencies will implement Red Alert.	This actually reflects change in Chicago Health and Human Services alert status	Data Collector Log	Chicago EOC
IA	12-May-03	20:27	DHS-CAT reports that DHS has advised that effective at 2130 EDT, the alert level will be raised to RED for the following cities: Seattle, San Francisco, Los Angeles, Houston, Chicago, New York, Washington, D.C.		Situation Report	DHS-CAT
IL	12-May-03	20:32	Chicago area EOCs notified of elevation of HSAS to RED for seven high-risk cities.		Detailed Incident Report	DuPage County EOC
WA	12-May-03	20:40	FBI announced that incident is a terrorist event		Component Log	RDD Site
IA	12-May-03	20:46	HHS SCC gets word of the seven-city Red; will notify CDC to load the planes.		Data Collector Log	HHS
WA	12-May-03	20:50	SFD requested the release of DHS pre-positioned equipment package (PEP) located at Boeing field. Request passed to FEMA		Operations Log	WA State EOC
IL	12-May-03	20:56	Chicago Fire Dept informed by FBI Chicago that Chicago is listed as a "probable" target. Increase security for senior elected officials – Governor and Mayor. Specific threats have been identified.		Data Collector Log	Chicago EOC
IL	12-May-03	20:57	CPD recommend cancellation of White Sox baseball game and McCormick Place convention; Emergency Management Coordinator concurs. 12 hour shifts for sworn personnel; all in uniforms. Contact special details at O'Hare and Midway for Code Red protocols. Increased security for city target buildings.		Data Collector Log	Chicago EOC
WA	12-May-03	21:00	WA Hospital Control ceases operations		Incident Log	Harborview Hospital
IA	12-May-03	21:00	CDC operations center receives message from HHS SCC that 7 cities are now at threat level red. EOC staff notifies associated CDC staff members		Data Collector Log	CDC EOC Atlanta
IA	12-May-03	21:02	HHS, conferring with Chicago health officials, wants to pre-deploy the SERT now; it will be there by morning. In another matter, HHS will work with with RHA to pre-position SNS stockpile near Chicago, based on information from British Columbia.		Data Collector Log	HHS
WA	12-May-03	21:10	SPD IC meet with Mayor and Chiefs at police command post; SPD IC advised that this was a terrorist event		Data Collector Log	RDD site
IA	12-May-03	21:10	FBI SIOC learns that 7 cities will go to Red at 2130.		Data Collector Log	FBI SIOC
IA	12-May-03	21:30	USSS Director's Crisis Center activated		Federal Response Briefing (Info Cut-Off Time: 0600 13 May 03)	DHS-CAT
IA	12-May-03	21:41	CDC putting out health alert to Chicago area doctors and hospitals. Plague is to be added to watch list, based on intelligence. But CDC is not suggesting an outbreak of this disease; the alert says to look for flu, or similar respiratory illness.		Data Collector Log	HHS
WA	12-May-03	21:44	Seattle Shelter-in-place press release approved		Press Release	Seattle EOC
IA	12-May-03	21:45	HHS SCC received notification from OER that NDMS teams were activated (notionally) in response to HSAS elevation to RED for the seven cities.		Data Collector Log	HHS
WA	12-May-03	22:00	US Coast Guard Seattle is at MARSEC 3 (highest level of security) - this means certain parts of the Port of Seattle are closed and port traffic is being directed to other locations		Situation Report 2	WA State EOC
WA	12-May-03	22:00	DEST arrives at the FBI Seattle Field Office (corresponds to MSEL # 3052).	Time taken from JOC analyst log. Other times reported 21:00 and 17:05 PDT (0:00 and 20:05 EDT) by MSEL Team from unknown sources.	Analyst Log	JOC CMG
IA	12-May-03	22:07	From EPA HQ: DOE designated as lead for radiological matters; other Federal agencies are to take DOE's direction on monitoring requests. DOE is to receive all data now, through the FRMAC, but data can be shared concurrently with State and local officials.		Data Collector Log	EPA EOC HQ D.C.
IA	12-May-03	22:30	FEMA EST and OSHA to coordinate an inter-agency health & safety plan		Data Collector Log	EPA EOC HQ D.C.
IA	12-May-03	22:30	First SNS situation report was issued by CDC. Primary area of coordination is supply of Prussian Blue, Ca DTPA or Zn DTPA.		Data Collector Log	CDC EOC Atlanta
WA	12-May-03	22:40	National Controller called WA SEOC Director to inject that the national threat level went Red, effective 1740 PDT.		Data Collector Log	WA State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IA	12-May-03	22:46	NRC alerts FBI information control that it is going to highest level security at nuclear power plants.		Data Collector Log	FBI SIOC
WA	12-May-03	22:58	FBI has completed trail vehicle evidence investigation. FBI identified GLODO involvement (corresponds to MSEL # 3051)	Time taken was from MSEL Team log (source RDD Site Controller). Additional time 21:30 PDT (0:30 EDT) from RDD Site Data Collector, identifying more actions than completion of vehicle evidence collection.	MSEL Team Log	MSEL
IL	12-May-03	23:00	IDPH put out fax alert regarding signs and symptoms (definitions of) of respiratory illness, fever, pain in the chest; 60 suspected cases		Fax Alert	IDPH
IL	12-May-03	23:00	DuPage County Public Health gets notification from IDPH of a TOPS cluster and passes this notification on to all offices and hospitals		Analyst Notes	IL VCC
WA	12-May-03	23:00	King County EOC talked to JOC: confirmed event designated as a terrorist incident and FBI assuming investigative lead.		Component Log	King County EOC
IL	12-May-03	23:00	Last night at 2200 - DuPage County notified from IDPH - notified of "TOPS" cluster - to all PH offices and hospitals		Data Collector Log	DuPage County PH
WA	12-May-03	23:10	Conference call with key state, county, and city players to update status of current situation: PHSKC EOC recommending: safe to remove shelter in place, but unsure how to transport those people out of Exclusion Zone. Will bring in buses from outside the Exclusion Zone to evacuate the public---tell them to go home, bag clothes, put in garbage, shower with water and soap, and await further instructions and info. Final Recommendation: risk of continuing to shelter in place is greater than contamination threat of leaving the area. But, want to transport people out of area using non-contaminated vehicles brought to perimeter of incident area		Data Collector Log	SKCPH EOC
IA	12-May-03	23:23	USMS reports Federal courthouse in Seattle is closed, but a magistrate remains on duty.		Data Collector Log	FBI SIOC
WA	12-May-03	23:30	Incident has been declared a criminal act; FBI has assumed control of the incident site		Data Collector Log	RDD Site
IA	12-May-03	23:30	Washington State request for Federal Disaster Declaration submitted to White House		Federal Response Briefing	DHS-CAT
WA	12-May-03	23:34	Incident Site Update: Command staff transition taking place; HazMat and technical rescue operations still on-going; new tents and lights being erected in command post area for night operations. SPD and SFD command posts side by side but separate. Still no unified command. Federal agencies on scene include FBI and EPA in command post area.		Data Collector Log	RDD site
WA	12-May-03	23:50	FBI has declared event a terrorist incident effective 20:00 PDT (23:00 EDT) & assumed lead investigative agency role. Investigation has associated a Maroon Honda & a blue GMC pick-up truck with the incident. Honda recovered near scene after crash with one non-identified suspect dead-on-arrival. Blue pick-up believed headed north-bound towards Canada.		King County OEM Event Log	KC EOC
WA	12-May-03	23:56	Data from AMS received by FRMAC.		Data Collector Log	FRMAC
WA	13-May-03	0:00	King County Situation Report - King County Metro Transit has made arrangements to provide Water Taxi service from West Seattle to downtown Seattle at 5:15 PDT (8:15 EDT) Tuesday.		Press Release	KC IC
IL	13-May-03	0:14	Central Dupage Hospital alerted Health Dept. of a suspected plague case	The evaluation team does not know if Health Dept. refers to the DuPage County Health Dept. or to IDPH (or both)	Detailed Incident Report	DuPage County EOC
WA	13-May-03	0:15	All patients have been rescued, rubble pile is clear of live victims		Data Collector Log	WA State EOC
WA	13-May-03	0:16	Ongoing discussions between WA SEOC, King County EOC, and Seattle EOC, and public health officials about shrinking the exclusion zone. There were repeated concerns about a lack of data.		Data Collector Log	KC EOC
WA	13-May-03	0:25	Conference Call between WA SEOC (including WA DOH), King County EOC, Seattle EOC, and PHSKC EOC to develop evacuation plan for people sheltering-in-place in industrial area of exclusion zone: First wash down evacuation route(s), coordinate buses into the incident area. SFD, SPD, and DOT available to support the evacuation. Evacuated people will be taken to a holding area, where relatives can come get them or they can go to shelters. At holding area, directions will be given to people about how to decontaminate at home (remove clothing, bag them, shower with soap and water). There is an unknown number of people in industrial area. Buses can transport 60 people at one time. All in area West of I-5 will be evacuated; will wait on more lab data before evacuating those East of I-5.		Data Collector Log	SKCPH EOC
WA	13-May-03	0:30	FBI has overall command and SFD has rescue command; FBI will be on scene all night		Data Collector Log	RDD site
WA	13-May-03	0:30	Unified meeting made up of SFD, SPD, and FBI, to discuss overall situation at incident site		Data Collector Log	WA State EOC
WA	13-May-03	1:00	FBI HMRU Leader's decision to have joint entry teams was based on number factors: Desire to facilitate interagency cooperation; evidentiary concerns with jurisdiction---the mixed teams would allow for a representative from agencies that claim to have jurisdiction of the evidence; levels of experience - some agencies have more experience with blast analysis.		Data Collector Log	RDD Site
WA	13-May-03	1:05	WA SEOC List of Priority Actions: 1) Radiation Footprint and impacts. 2) EST Recovery and Restoration Task Force. 3) Critical Infrastructure Protection. 4) Re-opening of I-5 5) Presidential Declaration		Data Collector Log	WA State EOC
WA	13-May-03	1:09	WA SEOC reports: SFD HazMat confirms detection of Americium 241 and Cesium 137 and relays to IC/ CPS		Data Collector Log	WA State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	13-May-03	1:30	Global e-mail to King County Employees: Only essential King County personnel who's job site is within the following boundaries--Royal Brougham to the North, I-5 to the East, S. Alaskan Way to the South, and Elliott Bay to the West--are being told to report to work tomorrow, Tuesday, May 13. Employees are advised to check with the King county employee hotline, at 205-8600, and the King County Website, at www.metrokc.gov for department specific information		Press Release	KC IC
WA	13-May-03	1:37	WA PFO priorities for night: defining the affected area, developing protective actions, and constructing a consistent message to the communities.		JOC CMG Log	JOC CMG
WA	13-May-03	1:48	SFD determined no viable victims left at incident site; switching from rescue mode to recovery mode.		FBI Log	WA State EOC
WA	13-May-03	2:00	Data from DOE AMS identified an alpha emitter. FRMAC therefore believes that the shelter in place zone is too small. Seattle's initial assessment was based on data from only a gamma emitter (Ce 137) at relatively low levels. FRMAC recommends to WA PFO that Seattle evacuates all people in exclusion zone, but need ground samples to determine exact measures. EPA's makes recommendation to wait until morning (since people are sleeping) when more data has come in--State and locals made the best decision they could with the information they had at the time. WA PFO's decision is to recommend to the city to maintain shelter in place until more data comes in; not to evacuate.		Analyst log	FRMAC briefing
WA	13-May-03	2:02	WA PFO learns that Seattle is planning to evacuate those civilians who have been sheltering in place in industrial area		Analyst log	FRMAC briefing
WA	13-May-03	2:10	WA SEOC faxes a request for the DMAT to the FEMA Region X ROC. They want a medical team to do enhanced primary medical care to augment overwhelmed local emergency departments due to potential affected population zone & "worried well" and screening for emergency reserve.		Fax	FEMA Region X ROC
WA	13-May-03	2:12	WA DOT: City of Seattle recommended opening of state highways, but they lack the authority to do so.	This occurred between 23:12-23:40 PDT (2:12-2:40 EDT)	Data Collector Log	WA State EOC
WA	13-May-03	2:50	Discussions ensue at the Seattle EOC about plans to decontaminate the streets by washing them down; concerns are raised about the sewage system, potential legal issues, and environmental impact	This occurred between 23:50-00:15 PDT (2:50-3:15 EDT)	Data Collector Log	Seattle EOC
WA	13-May-03	3:12	KC EOC reports that Seattle has put out a press release asking people to stay out of contaminated area, but people can go to work downtown.		Data Collector Log	KC EOC
IL	13-May-03	3:58	LaGrange Hospital evaluated current patients and identified a possible case of pneumonic plague		Data Collector Log	LaGrange Hospital
WA	13-May-03	4:00	Decision is made for the SFD to remain in charge of incident scene until 6:00 PDT (9:00 EDT) Tuesday when full FBI returns	This occurred between 01:00 and 01:30 PDT (04:00 - 04:30 EDT).	Data Collector Log	RDD site
WA	13-May-03	4:35	Plans to go forward with the evacuation of those sheltering-in-place in industrial area of exclusion zone is hampered by a lack of data.		Data Collector Log	WA State EOC
WA	13-May-03	5:00	WA SEOC recommends to USCG & Harbor Patrol to reopen the navigable waters for the following Washington State Ferries: vehicle and passenger service only on the Anacortes-San Juan, Edmonds-Kingston, and Fauntleroy-Vashon-Southworth; Passengers-only service on the Mukilteo-Clinton, Keystone-Port Townsend, and Port Defiance-Tahlequah routes. Recommend security measures in place for walk-on passengers to remain in effect.		Protective Action Decision Wksht	WA State EOC
WA	13-May-03	5:00	WA SEOC recommends that all existing highway closures remain in effect		Protective Action Decision Wksht	WA State EOC
WA	13-May-03	5:42	WA SEOC Press release: WA DOH to begin evacuation of immediate blast area. People will be notified by radio and by direct phone calls into the area west of I-5 using telephone numbers listed on business licenses in the city finance department. The area to be evacuated is bounded by Royal Brougham Way on the north, I-5 on the east, S. Alaska St. on the south, and the Seattle waterfront on the west.		Press Release	Seattle EOC
WA	13-May-03	6:28	WA SEOC notified that Seattle Mayor decided I-5 will re-open at 05:00 PDT (08:00 EDT)		Data Collector Log	WA State EOC
WA	13-May-03	6:28	Per WDOT, radiological data has not been confirmed. Therefore I-5 will remain closed.		EOC Supervisor Log	WA State EOC
WA	13-May-03	6:31	Seattle EOC: Retracted opening of I-5 until additional data from DOE AMS fly over comes in.		Agency Log	Seattle EOC
IA	13-May-03	7:10	HHS ASPHEP requests CDC to contact SERT leader in Chicago and tell him to request increased surveillance. CDC agrees to call Chicago.		Data Collector Log	FBI SIOC
WA	13-May-03	7:15	SFD IC & Operations Chief meet face to face with NMRT. NMRT tasked with force protection		Data Collector Log	WA State EOC
WA	13-May-03	7:37	WA SEOC requests Fire Mobilization Authorization on behalf of SFD		Public Information Officer's Log	WA State EOC
WA	13-May-03	7:45	WA SEOC News Release: WA State Ferries to resume full service except for Seattle runs.		Public Information Officer's Log	WA State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IA	13-May-03	8:05	NCEH, lead CDC center responding to radiological event, conducts conference call with Seattle & King County EOCs, Regional X REOC, and CDC's A-team representatives.		Data Collector Log	HHS - SCC
IL	13-May-03	8:10	ARC of Greater Chicago received a phone call from IL SEOC: confirmed Red Alert for IL became effective at 19:00 CDT (20:00 EDT) on Monday. Also informed that IDPH has reported about 100 patients with SARS-like symptoms have reported to Chicago hospitals. Due to this, ARC will discontinue blood collections in this area. All chapters will be notified of alert status. National ARC "Get Info Public" info line has been activated		Data Collector Log	ARC of Greater Chicago HQ
WA	13-May-03	8:30	WA SEOC News Release: WA Governor appointed a Recovery and Restoration Task Force to guide and coordinate state government recovery efforts in areas of King County and Seattle affected by the explosion		Press Release	WA State EOC
IA	13-May-03	8:38	FEMA HQ calls for a CDRG meeting at 0900 on May 13, 2003		Data Collector Log	EPA EOC HQ D.C.
IL	13-May-03	8:45	DuPage County Public Health Dept. goes on 24/7 ops		Data Collector Log	DuPage County PH
IL	13-May-03	8:45	Highland hospital received clarification from IDPH that it wasn't the alert level that went to red; it was the infection alert level		Analyst Notes	IL VCC
IL	13-May-03	8:58	DuPage County Public Health to get surveillance teams up and going		Data Collector Log	DuPage County Health
WA	13-May-03	9:00	WA SEOC was notified by FEMA Region X Liaison that the PDD was signed at 900 EST on May 13. WA SEOC is trying to obtain a copy of signed declaration at this time. Disaster number will be DR-4321-WA.		Situation Report	WA State EOC
IA	13-May-03	9:12	HHS SCC holds a conference call with Region V to discuss biological event. Key discussion points: NCID is the lead CDC center supporting the bio event; needs to engage State & local health officials to convey prophylaxis strategies. Communications staff coordinate with locals to develop messages for media and public.		EP&R activity log	DHS/ HS Center
IL	13-May-03	9:15	CCDPH begins active surveillance. Contact Chicago hospitals by fax, but don't discuss disease with public yet.		Data Collector Log	CCDPH
WA	13-May-03	9:15	FBI locates two safehouses (corresponds to MSEL # 3053)	Time taken was from a RDD site controller log. Other times listed by MSEL Team were 21:40 and 22:30 PDT on May 12 (0:40 and 1:30 EDT on May 13) from unknown sources.	Controller Log	RDD Site
WA	13-May-03	9:15	Seattle Mayor signed a general exclusion order, which restricted public access in an area bounded by S Horton St. on the South, SR99 on the West, Royal Brougham on the North, and Airport Way on the East.		Seattle EOC Situation Report	Seattle EOC
IL	13-May-03	9:23	DuPage County DPH alerts pre-selected prophylaxis dispensing sites to be prepared to be activated in the event that the IL Stockpile or SNS is requested.		Data Collector Log	DuPage County PH
IL	13-May-03	9:30	Chicago Dept. of Public Health dispatches epidemiology teams to 34 Chicago city hospitals		Data Collector Log	Chicago EOC
IL	13-May-03	9:30	Lake Forest hospital received fax confirming pneumonic plague. Fax also received regarding patient flow.		Data Collector Log	Lake Forest Hospital
IA	13-May-03	9:30	DOS stood up task force to liaison with Canada. Border security heightened ; Canadians are intercepting Seattle flights for possible decontamination.		Data Collector Log	CDC EOC Atlanta
IL	13-May-03	9:37	Chicago EOC has received only three reports from 3 hospitals; Chicago DPH to send staff out to hospitals to do face-to-face to emphasize increased reporting. Chicago DPH advising M-95 masks and infection control procedures for emergency responders.		Data Collector Log	Chicago EOC
IL	13-May-03	9:39	Chicago EOC pre-positioned specialized teams (hazmat, dive, rescue); locked down firehouses; activated secondary command post at Fire Academy.		Data Collector Log	Chicago EOC
IL	13-May-03	9:39	IDPH activates Phase I of IL Emergency Medical Disaster Plan. POD hospitals activated.		Data Collector Log	DuPage County Health

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	13-May-03	9:40	Loyola University Medical Center activated as a POD Hospital		Data Collector Log	Loyola Univ. Medical Center
IL	13-May-03	9:43	Chicago EOC notified Mayor's Chief of Staff and brought Mayor up to date; in contact with the IL Governor's Office; more senior staff reporting to EOC; preparing Chicago Declaration of Emergency draft.		Data Collector Log	Chicago EOC
IL	13-May-03	9:45	Highland Park hospital received call from IOHNO to go to Phase I of IL Emergency Medical Disaster Plan - must report back to IOHNO 10:30 CDT (11:30 EDT) that plan is implemented.		Data Collector Log	Highland Park Hospital
IL	13-May-03	9:45	Masonic ER reported to IDPH that Phase I of IL Emergency Medical Disaster Plan activated.		Data collector Log	Masonic ER
IL	13-May-03	9:50	IDPH has reported two cases of pneumonic plague in the Chicago area		SEOC Event Log	IL State EOC
IL	13-May-03	9:51	IL SEOC Director spoke with ISP Director and reported to IL SEOC: Based on intelligence information last night the North and Central (with the Southern team in reserve) SWMDT, National Guard 5th Civil Support Team, and IMERT are being activated. ISP will contact their members and IEMA to make remainder of contacts. They are to report to the College of DuPage. IL SEOC Director also authorized the activation of these special teams.		SEOC Event Log	IL State EOC
IL	13-May-03	9:55	IL SEOC notifies ARC Chicago District Operations Center of 2 cases of pneumonic plague, in addition to SARS - like patients presenting at hospitals over-night. Also notifies that IL SWMDT has been set-up in Dupage County		Data Collector Log	ARC - Chicago HQ
IL	13-May-03	9:55	Good Samaritan called Elmerst Memorial Hospital ER to tell charge nurse that Phase I of IL Emergency Medical Disaster Plan was implemented.		Data Collector Log	Elmhurst Memorial Hospital
IL	13-May-03	10:00	IDPH conference call with IDPH Lab: Top Priority for hospital labs is if they see bipolar staining using Gram stain and patients fit clinical picture; sputum samples, Bronchoalveolar Lavage, lung aspiration, Antibiotic susceptibility.		CCDPH Log	Cook County DPH
WA	13-May-03	10:00	Threat update: State of Washington, orange. City of Seattle, red; King County, red-based on local policy		EOC Supervisor Log	WA State EOC
IA	13-May-03	10:00	HHS Homeland Security Center Incident Report: All NDMS assets have been put on alert per the EP&R Response Division; Additional information from Chicago indicates at least 100 patients with SARS-like illness in Chicago; Epidemiologist in the Chicago area and has deployed to the Illinois Department of Health.		Data Collector Log	MCC
IA	13-May-03	10:00	NRC has increased security at power plants in their 4 regions as a result of DHS going code red. They will give any appropriate information to SIOC information control if necessary.		Data Collector Log	VA Central Office
IA	13-May-03	10:00	Canadians requested that they be allowed to send a liaison to Region X ROC; US Government has no objections.		Situation Report	DHS CAT
IL	13-May-03	10:02	Lake County DPH reports: Hospitals have said that patients who went to United Center are being reported as suspect SARS. Some cases were also at O'Hare Airport. DuPage Hospital suspects plague at 23:42 CDT on May 12 (0:42 EDT on 13 May). Some patients from Canada. DuPage: 13 suspect cases respiratory illness United Center Connection, O'Hare Connection, and Canada Connection		Data Collector Log	Lake County Dept. of Health
IL	13-May-03	10:04	Illinois Masonic activates Phase I of IL Emergency Medical Disaster Plan. Illinois Masonic faxed Swedish Covenant Phase I information sheet because they did not have it, though they are supposed to.		Data Collector Log	Swedish Covenant
IL	13-May-03	10:05	IDPH faxed LaGrange ER to implement Phase I of IL Emergency Medical Disaster Plan - charge nurse calling units and departments to determine beds, blood, vents - etc.		Data Collector Log	LaGrange Hospital
IL	13-May-03	10:15	Central DuPage Hospital activates Phase I of IL Emergency Medical Disaster Plan		Data Collector Log	Central DuPage
IL	13-May-03	10:20	VNN reporting unusual number of flu-like illnesses in Vancouver		Data Collector Log	IDPH
IA	13-May-03	10:20	NRC member of CAT requests copy of ARAC plots		Data Collector Log	FBI SIOC
IL	13-May-03	10:25	Northwest Community Hospital reported to Good Shepherd Hospital via radio that Phase I of IL Emergency Medical Disaster Plan implemented.		Data collector Log	Good Shepherd
IL	13-May-03	10:25	IL Governor has approved the deployment of the National Guard CST		SEOC Event Log	IL State EOC
WA	13-May-03	10:27	WA SEOC: PIOs instructed to NOT disseminate plume data to the media as it is not confirmed		Data Collector Log	WA State EOC
IL	13-May-03	10:30	American Red Cross of Greater Chicago PIO receives request from FEMA to go to the IL JIC		Data Collector Log	ARC - Chicago HQ

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	13-May-03	10:30	IDPH (Springfield): all lab specimens need to be expedited to IDPH Lab for definitive diagnostic testing		Data Collector Log	IDPH
IA	13-May-03	10:30	Homeland Security Center update: CDC recommends starting with Ciprofloxacin and then switching to Doxycycline later if advisable to do so; Several people have arrived in BC with have flu-like illness, on a flight originating from Chicago; HHS working to get SNS moved on a minute's notice.		DOE activity log	DHS/HS Center
IL	13-May-03	10:32	DuPage County DPH suggests dispatch IL State Police or local police as couriers to expedite lab analysis		Data Collector Log	DuPage County PH
IL	13-May-03	10:36	Lake County Health EOC advises Lake County EOC: 89 cases in Chicago area - 1 death from respiratory illness. Samples sent to IDPH Lab - preliminary results by noon - possible outbreak of plague per CCDPH. 10 may have been at United Center.		Data Collector Log	Lake County EOC
WA	13-May-03	10:40	Debriefing meeting with IC: Transitioned from rescue to recovery at 06:00 PDT (09:00 EDT). FBI taking over responsibilities for incident management. Scene monitoring (contaminants) still being performed by SFD HazMat. Decontamination responsibility transferred to NMRT. Jurisdiction over deceased discussed. DMORT on site by 11:00.		Data collector log	RDD Site
IL	13-May-03	10:41	IDPH: Prioritize specimens by bipolar staining or connection with United Center		Data Collector Log	IDPH
IL	13-May-03	10:47	Finalized "TOPS" case definition describing signs and symptoms of infectious disease trend beginning to appear.		Data Collector Log	IDPH
IL	13-May-03	10:54	IDPH notified ARC Chicago they have activated Phase 1 of their Emergency Medical Disaster Plan - IDPH collecting data and checking hospital space		Data Collector Log	ARC - Chicago HQ
IL	13-May-03	10:56	ARC of Greater Chicago reports that the early clinical diagnosis from the IL SEOC is incorrect; there is not enough information to confirm Plague		Data Collector Log	ARC - Chicago HQ
IA	13-May-03	10:57	Seattle FDA office preparing an advisory for consumers; blanket embargo of all foodstuffs in the plume area.		Data Collector Log	VA Central Office
WA	13-May-03	10:59	AMS fly over readings: Kitsap County (WA) readings are above food control limit; I-5 is clean, but people could drive into unsafe areas - so not ready to open. City requests making residential area east of I-5 a priority for measurement.		Data Collector Log	WA State EOC
IA	13-May-03	11:00	HHS/ SCC holds conference call with CDC and other ESF-8 partners; key discussion points: NCEH (CDC radiation lead) has posted worker safety radiation literature on CDC's website (some information is actually on the site, while other information is notionally posted). HHS SERTs sent to Seattle and Chicago. Reviewed current mission assignments/requests for assistance for the states. Seattle has requested the following ESF-8 assets: DMAT, NMRT, DMORT and the WMD DMORT. Additionally, CDC provided A-Team members to support FRMAC.		Data Collector Log	HHS - SCC
IL	13-May-03	11:05	CCDPH: indications that additional cases were presenting with symptoms and specimens consistent with plague, but no clear indication that's what it is. Cases showing from O'Hare and Union Station in addition to United Center.		Data Collector Log	CCDPH
IL	13-May-03	11:09	Chicago EOC update: FBI is at the EOC; 2 hospitals (Gottlieb and Ingalls) report clinical plague cases at hospital - the cases come from far south and far west of Chicago, but both attended recent event at the United Center; the HAZMAT Chief and City of Chicago notified.		Data Collector Log	Chicago EOC
IL	13-May-03	11:10	CCSEMA receives IEMA SitRep: at 09:15 CDT (10:15 EDT) IL State WMD team & IMERT were activated and ordered to assemble at College of DuPage		Message & Event Log	CCSEMA
IA	13-May-03	11:13	2nd SERT team is arriving soon in Illinois; will get additional epidemiological support from CDC.		Data Collector Log	DHS CAT
IA	13-May-03	11:20	Director CDC public health priorities: Focus on immediate needs of Chicago and Seattle - but do not over-commit CDC resources, as we need to consider the potential for multiple events in other parts of the country. Ensure the public health community stakeholders have the requisite information to stay informed as to what is happening. NCID staff needs to strategize on the potential diagnosis of plague, and be ahead if in fact the agent proves to be plague.		Data Collector Log	VA Central Office
IL	13-May-03	11:30	VNN announces patients with flu-like symptoms - possible SARS cases - in Chicago; unconfirmed deaths		Data Collector Log	ARC of Greater Chicago HQ
IL	13-May-03	11:32	At IDPH Lab, suggestion made to utilize "police" to get specimens from hospitals to IDPH lab.		Data Collector Log	IDPH lab
IL	13-May-03	11:40	Briefing at Chicago 911: confirmed pneumonic plague at Gottlieb Hospital in Melrose Park, Ingalls - Harvey and Childrens Hospital-Chicago. FBI notified Chicago Fire Department that the commonality is the Chicago United Center. Chicago Fire Department is sending teams to identify if bacteria still present.		SEOC Event Log	IL State EOC
WA	13-May-03	11:40	Red Cross representative to WA JOC CMG: King County Parks Dept. with support from ARC opened 3 shelters at 20:00 PDT on May 12 (23:00 EDT) for individuals unable to return to their homes.		JOC CMG Log	JOC CMG
IA	13-May-03	11:40	INJECT: FBI Chicago Field Office notified that CDC deploying assets to area (MSEL 3129)		Data Collector Log	CDC EOC Atlanta
IA	13-May-03	11:56	TSA liaison to FBI SIOC: New TFR will be announced with 5 mile radius, 18,000 feet (reduced from 20,000 ft)		Data Collector Log	FBI SIOC
IL	13-May-03	12:00	VNN confirms GLODO has claimed responsibility for Seattle attack		Data Collector Log	ARC - Chicago HQ
IL	13-May-03	12:00	Chicago DPH looking to identify travel history of all patients.		Data Collector Log	Chicago DPH

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IA	13-May-03	12:00	ESF 10 reports missing shipment of nuclear material	Also reported to FBI SIOC	Data Collector Log	FEMA EST
IL	13-May-03	12:04	CCDPH Conference call with Chicago and Collar Counties: Reports coming from hospitals, but do not have active surveillance. EIS officers will be going out in the field following conference call. State recommends that interviews should ask whether they have had exposure to O'Hare, Union Station, or United Center		CCDPH Player Log	Cook County DPH
IL	13-May-03	12:04	CCSEMA receives Sitrep from CCDPH: at 10:20 CDT (11:20 EDT), IDPH has made a presumptive diagnosis of 2 cases of pneumonic plague. DHS notified & SNS placed on standby.		Message & Event Log	CCSEMA
IL	13-May-03	12:05	VNN: IL Governor press release announcing confirmation of pneumonic plague cases and that state disaster plan has been implemented		Data Collector Log	Springfield IDPH
IL	13-May-03	12:07	IL Governor announces respiratory illness clusters in Chicago area. No evidence that illness is related to Seattle attack, but IDPH and other public health departments are working to determine cause of illness - urges citizens to take precautions.		Data Collector Log	ARC - Chicago HQ
WA	13-May-03	12:09	"There are no confirmed dead" - per King County Medical Examiners office, who received information directly from the IC		Data collector log	SKCPH EOC
IL	13-May-03	12:12	Chicago EOC: Plague is strongly suspected. Looks like plague under microscope; several cases known; many cases coming in right now. IDPH has 109 cases. Chicago had 5 cases, other counties have more. Chicago OEMC wants real numbers as soon as possible.		Data Collector Log	Chicago EOC
IL	13-May-03	12:13	Director Chicago OEMC: Via FBI Chicago, respiratory patients from O'Hare and Union Station at Lincoln Hospital. Chicago Fire Dept. to do investigative bio survey at O'Hare and Union Station. Plague presumed until further notice.		Data Collector Log	Chicago EOC
IL	13-May-03	12:14	IL SEOC received EMNet message. Information that IDPH has made a presumptive diagnosis of 2 pneumonic plague cases. The Department of Homeland Security has been notified; the national pharmaceutical stockpile (SNS) to be on standby.		SEOC Event Log	IL State EOC
IL	13-May-03	12:15	Chicago EOC received EMNet Emergency Message: IDPH has made presumptive diagnosis of 2 pneumonic plague cases. Chicago Dept. of Health & Human Services has notified SNS to be on standby for release.		Data Collector Log	Chicago EOC
IL	13-May-03	12:17	Lake County EOC: IDPH has made presumptive diagnosis of pneumonic plague.		Data Collector Log	Lake County EOC
IL	13-May-03	12:18	Lake County EOC notified emergency stockpile (SNS) to stand by		Data Collector Log	Lake County EOC
IL	13-May-03	12:20	IL JIC confirms reports of plague.		Data collector Log	DuPage Co. EOC
IL	13-May-03	12:36	CCDPH directed staff to develop public information message and get a phone bank ready and notify the Bridgeview distribution site, red cross, sheriff, public health clinics, and the PIO at the IL JIC		Data Collector Log	CCDHP
IL	13-May-03	12:40	Chicago 911 Briefing: City of Chicago putting together Disaster Declaration based on their activities dealing with health symptoms. 53 yr. female and 57 year male United Flight attendant both confirmed dead by Cook County medical examiners. Chicago in communication with Vancouver because Vancouver played Chicago Black Hawks this past weekend. Chicago Fire Department, Chicago Bomb Squad, and FBI are checking United Center, Union Station, and O'Hare Airport. Considering a request for CST team.		SEOC Event Log	IL State EOC
IL	13-May-03	12:45	Chicago EOC update: State of Emergency to be declared in in Chicago, recommend public Shelter-In-Place, Strategic National Stockpile requested. Final trigger was a message from Vancouver saying that their initial cases all came from Chicago and that their microbiologists/labs had confirmed Pneumonic Plague.		Data Collector Log	Chicago EOC
IL	13-May-03	12:46	Kane County EOC received an e-mail from iCHNO - WMD Civil Support teams and IMERT activated and are to stage at college of DuPage		Data collector Log	Kane County EOC
IL	13-May-03	12:58	Cook County EOC preparing proclamation of disaster		Data Collector Log	Cook County EOC
IA	13-May-03	12:59	HHS reported 2 cases with presumptive plague diagnosis and 100 additional sick with flu-like symptoms in Chicago. CDC is at the scene with an investigative team. DHS is conducting conference calls to confer on preparation activities.		Situation report from Bureau of Immigration and Customs Enforcement Headquarters Reporting Center	DHS/CAT
WA	13-May-03	13:00	HHS Region X REOC (WA) developing registry for people who were exposed. The Agency for toxic substances and disease registry (ATSDR) estimated 120,000 exposed people, Region X REOC (WA) believes this is probably too high		Data Collector Log	REOC
WA	13-May-03	13:00	Incident site update from WA SEOC: 21 dead on site, injured 51 Red, 43 Yellow, and 45 Green; Working with Seattle EOC to validate numbers.		EOC Supervisor Log	WA State EOC
WA	13-May-03	13:05	FBI determined that bomb went off accidently; may be some other targets or explosives enroute		Analyst log	FSL Conference Call
IL	13-May-03	13:07	Director Chicago OEMC made big announcement - Declaration of State of Emergency in Chicago recommended; Chicago will order shelter-in-place; Chicago Law Department says: declaration of emergency gives authority to take necessary actions immediately. Press Conference will make announcement.		Data Collector Log	Chicago EOC
IL	13-May-03	13:09	IDPH approved memo describing treatment guidelines		Data Collector Log	Springfield IDPH

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IA	13-May-03	13:20	From DHS liaison to SIOC: NRC reports employees of a nuclear facility near Chicago are calling in sick. All of the employees had attended the Chicago Blackhawks game on May 10th. The Blackhawks played Vancouver. In addition 10 percent of the NRC Region III staff called in sick.		Data Collector Log	FBI SIOC
IL	13-May-03	13:20	CFD Chief says, "Field tested at O'Hare, Union Station, and the United Center." Not located any devices; will send swab sample to IDPH lab for culture. Swabbed HVAC system and common areas. Samples to be sent to IDPH laboratories; 48-hour turnaround. CSTs asked to be available to come in and support; on stand-by basis right now. CST has relocated from Peoria to College of DuPage.		Data Collector Log	Chicago EOC
IL	13-May-03	13:20	Chicago EOC talked with IDPH laboratory; They feel that outbreak started on Mother's Day; hazmat unit ran field tests; these field tests compromised by good housekeeping. Also, 48-hour turnaround for samples can be reduced to 3 hours.		Data Collector Log	Chicago EOC
IL	13-May-03	13:20	IDPH lab told that HazMat would organize site checks but based on clues thus far sounds like aerosol exposure. IDPH lab advising HazMat to look for possible devices and to collect perhaps little samples. HazMat believes based on clues/don't expect to find anything - will sample both ends of ventilation system for residual material. Will not do field analysis/will send samples direct to lab. Interagency teams will scour 3 sites for devices.		Data Collector Log	IDPH lab
WA	13-May-03	13:20	Federal JIC (WA) determines that VNN put out erroneous information; VNN announced that DHS was providing Prussian Blue at request of state, but state did not request from Oak Ridge; Oak Ridge automatically brings it.		Data Collector Log	JIC (WA)
IL	13-May-03	13:21	Cook County Epidemiology field teams are out and sending case reports to the state		Data Collector Log	CCDHP
IA	13-May-03	13:21	HHS ASPHEP wants paperwork for declaration of Public Health Emergency ready for the HHS Secretary to sign during briefing with President.		Data Collector Log	HHS - SCC
IL	13-May-03	13:27	IDPH lab reporting *Yersinia pestis* positive samples to IOHNO then to IDPH Springfield.		Data Collector Log	IDPH lab
IL	13-May-03	13:28	IDPH receives confirmation from lab - PCR tests completed; positive for *Y pestis* (3 patients)		Data Collector Log	IDPH
IL	13-May-03	13:30	IOHNO receives confirmation from Chicago IDPH Lab - positive for plague (*Yersinia pestis*) based on PCR test of 3 specimens from Edwards Hospital. No press release yet!		Data Collector Log	IOHNO
IL	13-May-03	13:30	IL Governor declares state of emergency, requests activation of the SNS, mobilizes IEMA & IDPH.		Data Collector Log	Lake County EOC
IA	13-May-03	13:30	HHS ASPHEP: Based on the evolving numbers and a conference call with the DHS Secretary, the illness should be assumed to be plague and intentionally released.		Data Collector Log	FEMA HQ EST
IL	13-May-03	13:34	Chicago EOC received faxes from EMNet Emergency Message regarding activation of Strategic National Stockpile.		Data Collector Log	Chicago EOC
IL	13-May-03	13:35	IDPH activates Phase II of IL Emergency Medical Disaster Plan in response to Governor's Emergency Declaration.		Data Collector Log	Highland Park Hospital
IL	13-May-03	13:36	Plague confirmed - gram (-) rods		Data Collector Log	Sherman
IL	13-May-03	13:40	Elmhurst Hospital received fax from Good Samaritan Hospital instructing them to complete the Phase II worksheet.		Data Collector Log	Elmhurst Memorial Hospital
IL	13-May-03	13:40	IDPH notified Ingalls Hospital of code 99 (Phase II of IL Emergency Medical Disaster Plan)		Data Collector Log	Ingalls Hospital
IL	13-May-03	13:40	Northwestern Memorial Hospital and the University of Chicago-associated hospitals activated Phase II of IL Emergency Medical Disaster Plan		Data collector Log	Masonic ER
IA	13-May-03	13:40	HHS ASPHEP asks CDC to look at ventilators as part of their mobilization strategy.		Data Collector Log	HHS - SCC
IA	13-May-03	13:40	HHS SCC tasking ASPA to draft talking points regarding shelter-in-place, clarifying that they are NOT recommending sheltering-in-place nationwide.		Data Collector Log	HHS - SCC
IA	13-May-03	13:40	British Columbia & CDC confirms pneumonic plague; unconfirmed reports say that all of the sick people were on Air Canada flight 783 from Chicago. Legal will confirm and report back to FBI Chicago		Data Collector Log	HHS - SCC
IA	13-May-03	13:41	VNN report: DHS Secretary, on phone interview, was asked what should people in Code Red cities should do- -urged people to minimize public activity and keep children at home. HHS ASPHEP recommends that people "take a snow day."		Situation Report	DHS-CAT
IL	13-May-03	13:45	Loyola University Medical Center activated Phase II of IL Emergency Medical Disaster Plan		Data Collector Log	Loyola Univ. Medical Center
IL	13-May-03	13:45	Sherman Hospital activated Phase II of IL Emergency Medical Disaster Plan		Data Collector Log	Sherman
IL	13-May-03	13:46	Declaration of disaster signed by Lake County Board Chairman		Data Collector Log	Lake County EOC
IA	13-May-03	13:49	Coast Guard closed all vessel traffic in the Port of Chicago.		Situation report from BICE HQ Reporting Center	DHS-CAT

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	13-May-03	13:50	Lake County EOC PIO tells the Lake County PIO at the IL JIC not to issue a press release of declarations of emergency until all counties release a declaration		Data Collector Log	Lake County EOC
IL	13-May-03	13:51	University of Chicago called to notify South Shore Hospital of activation of Phase II of IL Emergency Medical Disaster Plan . Phase II worksheet filled out by ED supervisor.		Data Collector Log	South Shore
IL	13-May-03	13:55	VNN report: IDPH says probably plague & Canadian officials confirm plague		Data Collector Log	ARC of Greater Chicago HQ
IA	13-May-03	13:55	CDC issues Health Advisory #3, suspect pneumonic plague cases reported in IL.		Data Collector Log	FBI SIOC
IA	13-May-03	13:55	HRT/BDC deployment approved by FBI HQ in accordance with HRT deployment directives.		Region X ROC input to EP&R situation report	DHS/HS Center
IL	13-May-03	13:58	VNN report: DHS Secretary terms preliminary diagnosis of Flu-like symptoms as "plague"		Data collector Log	Kane County EOC
IL	13-May-03	13:59	ARC of Greater Chicago observes DHS Secretary on VNN announce that IDPH has a preliminary finding of plague-like illness - urges residents to restrict movement and stay inside. Vancouver has confirmed plague so Chicago must work on assumption of plague. ARC administration discusses the mismatch between the information in the Secretary's speech and other sources confirming plague.		Data Collector Log	ARC - Chicago HQ
IL	13-May-03	14:00	200 National Guard personnel requested to assist the Medical Examiner in morgue duties; report to Police Areas Centers 1 through 5, First Police District, O'Hare Airport, Midway Airport.		National Guard Request, Police Department	Chicago DPH
IL	13-May-03	14:00	VNN report: DHS Secretary announces plague in Vancouver and also probably in Chicago; recommends public treat it as a "snowday".		Data Collector Log	IDPH
IL	13-May-03	14:10	IDPH Springfield: Recommend IL Governor request National Disaster Medical System (NDMS) and DMAT (need epidemiologic specialists to assist with disease investigations).		SEOC Event Log	IL State EOC
IL	13-May-03	14:12	VNN report: 14 confirmed dead in Chicago.		Data Collector Log	IOHNO
IL	13-May-03	14:17	IDPH arranging web posting of memos on treatment and prophylaxis		Data Collector Log	IDPH
IA	13-May-03	14:22	HHS confirms 14 dead in Chicago from SARS-like illness		EP&R activity log	DHS/HS Center
IL	13-May-03	14:30	FBI Chicago confirming Pneumonic Plague		Data Collector Log	Chicago EOC
WA	13-May-03	14:31	DHS is working on a FRMAC transition plan for lead to shift to EPA from DOE		Data collector log	EPA - RCC
IL	13-May-03	14:38	DuPage County DPH: Plague identified; next steps are to get information out and do contact tracing		Data Collector Log	DuPage County Health
WA	13-May-03	14:40	WA SEOC looking to verify casualty numbers from incident site; number Seattle is putting out is different than what King County is putting out		Data Collector Log	WA State EOC
IA	13-May-03	14:50	CDC EOC: Seattle update - Two confirmed fatalities; 1,200 people evacuated, 600 decontaminated, 41 in critical condition in area hospitals.		Data Collector Log	CDC EOC Atlanta
WA	13-May-03	15:02	Unified Command Brief: Hazmat teams following ERT in rubble. Cadaver dogs on site. Evidence collection to begin soon. FEMA, EPA, and DOE still in support. After bodies have been cleared, will shift focus to long range remediation		Data Collector Log	RDD site
IA	13-May-03	15:08	Federal Radiological Monitoring and Assessment Center (FRMAC) has advised that they completed aerial measurements and ground samples of radiation. The radiation does not pose an immediate threat to life or safety; people within the shelter-in-place area could stay in place for up to a year without exceeding EPA protective action guidelines for radiation dosages; FPS has already evacuated the Federal facilities that had sheltered in place. GSA & FPS did develop a list of people that were sheltered in the Federal buildings as a precaution for future medical review.		Situation report from BICE HQ Reporting Center	DHS/CAT
IA	13-May-03	15:09	CDC (NCID) receives notification from Chicago of PCR confirmation of plague		Data Collector Log	MCC
IL	13-May-03	15:11	DuPage County begins distribution of their pharmaceutical stockpile based on Governor's request for SNS.		Data Collector Log	DuPage Co.
WA	13-May-03	15:15	News release from KC Regional JIC: The State Department of Agriculture has announced that precautionary measures are recommended for the areas: East of the King County /Kitsap County border between N.W. 85th Street and S.W. Admiral Way; South and west of 85th Street to 24th Avenue N.W. to 65th Avenue N.W. to 15th Avenue N.W. to Highway 99 to Denny Way to Interstate 5 to Interstate 90 to Highway 900; North and west of South Columbia Way from Highway 900 to 15th Avenue to South Nevada Street to 4th Avenue to Dawson Street to Highway 99 to Spokane street to S.W. Admiral way to the King/Kitsap County Border. Specific precautionary measures include the following: Avoid purchasing or consuming products stored in open-air markets after 12:10 pm on May 12, 2003; Fruits, vegetables or grain should not be picked; Shell fish harvested after 12:10 p.m. on May 12, 2003 should not be harvested or eaten; Agricultural products should not be transported uncovered through the advisory area; Pets should be restricted to water sources that are covered or are from enclosed underground storage.		Press Release	KC Regional JIC
IA	13-May-03	15:15	CDC EOC confirming 3 cases of plague in Chicago, confirmed by PCR from CRN lab in Chicago.		Data Collector Log	CDC EOC Atlanta

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	13-May-03	15:20	Elmhurst Memorial Hospital receives fax from IDPH regarding signs and symptoms of infectious disease trend beginning to appear. Emergency management coordinator and charge nurse notified by ER staff who also notified infectious control nurse.		Data Collector Log	Elmhurst Memorial Hospital
WA	13-May-03	15:20	Mayor's decision: those east of I-5 can leave home with certain precautionary measures, safe for them to resume daily activities, still need to be monitored, send message that they shouldn't eat home grown vegetables, let their kids play in the dirt, and avoid dust; those west of I-5 will be relocated for 3 days. Very few people remain West of I-5 since 1200 people were evacuated last night. Use outdialer to contact them, get them out with reception points, and decon shelter run by PHSKC. Possibility of hot spots so they may need to be kept for more than 3 days		Analyst log	JOC (WA)
WA	13-May-03	15:30	Meeting between HAZMAT IC and CST commander- indication is that CST is no longer required. CST to redeploy.		Data Collector Log	RDD site
WA	13-May-03	15:34	Agriculture advisory from WA Dept. of Agriculture: The following precautionary measures are recommended in the affected areas: Do not purchase and or consume products that were stored in open-air markets after 12:10 PDT (15:10 EDT) on May 12. Do no pick or harvest fruits, vegetables or grain. Do not harvest or eat shell fish harvested after 12:10 PDT (15:10 EDT) on May 12. Do not transport uncovered agricultural products through the advisory area. Restrict pets to water sources that are covered or are from enclosed underground storage		Advisory	WA Dept. of Agriculture
WA	13-May-03	15:35	WA Disaster Field Office scheduled to open May 15		Data Collector Log	WA State EOC
IL	13-May-03	15:38	Cook County Health Department requests SNS; formal request to be made within several minutes.		Data Collector Log	Chicago EOC
IL	13-May-03	15:58	Cook County Board chairman signs joint Cook County and Chicago emergency declaration.		Data Collector Log	CCDHP
IA	13-May-03	16:00	DHS ALERT AL-03-TOPOFF2-M: "The Secretary of DHS, in consultation with the intelligence community and the Homeland Security Council, raised the national threat level to Code red nationwide as of 1600, May 13...Federal Departments and Agencies, and State and local authorities, are directed to immediately implement protective actions identified in Operation Liberty Shield..."		DHS formal memorandum	DHS
IL	13-May-03	16:10	News Release: The City of Chicago declares a State of Emergency due to Pneumonic Plague. Cites probable release sites of O'Hare Airport, United Center, and Union Station. Chicago Fire Department has determined that no further releases are suspected.		Data Collector Log	Chicago EOC
IA	13-May-03	16:19	City of Chicago requests push-pack from Strategic National Stockpile to treat outbreak of plague-like illness.		Data Collector Log	FBI SIOC
IL	13-May-03	16:20	St. Joseph's Hospital receives fax from IL Poison Center confirming *Y. pestis*		Data Collector Log	St. Joseph's, Chicago
IA	13-May-03	16:21	ICE Situation Command notified its field offices that the British Columbia Center for Disease Control had confirmed that individuals admitted to the Vancouver General Hospital on May 12 with flu-like symptoms had pneumonic plague.		Situation report from BICE HQ Reporting Center	DHS-CAT
IL	13-May-03	16:27	VNN report: Canada Health confirm cases of plague; all cases originated through Air Canada flight 783; currently tracking individuals.		Data Collector Log	IL VCC
IL	13-May-03	16:28	VNN report: rapid response team has determined three target sites for plague in Chicago - Union station, United Center and O'Hare Airport International Terminal		Detailed Incident Report	DuPage County EOC
IL	13-May-03	16:32	Fax message to Chicago EOC: IL Governor announces IDPH Laboratory confirmation of Plague		Data Collector Log	Chicago EOC
IL	13-May-03	16:33	Fax received at CCDPH - IDPH Lab confirmed plague but not confirmed terrorism. Fax sent out to provide reporting numbers for IOHNO		Data Collector Log	CCDHP
IL	13-May-03	16:35	EMS Surveillance for April 30, 2003 through May 13, 2003 showed an increase in respiratory tract symptomology with patients beginning on/about May 12 and increasing through May 13.		Data Collector Log	Chicago EOC
IL	13-May-03	16:37	DuPage County EOC received official fax from IDPH - PCR confirmation of pneumonic plague		Data Collector Log	DuPage County PH
WA	13-May-03	16:45	WA SEOC received report from Seattle EOC: confirming 20 dead and 117 injured		EOC Supervisor Log	WA State EOC
IL	13-May-03	16:50	Fax of IL Governor's emergency declaration arrived at Lake County EOC.		Data Collector Log	Lake County EOC
IA	13-May-03	16:54	Truck with Cobalt 60 that was reported missing located, cargo intact.		Data Collector Log	USDOT CMC
IA	13-May-03	17:00	SNS Operations Center has not received any reqests from the IL Governor for the SNS, even though the IL Governor already announced on VNN that he'd requested SNS	It is not clear from the Situation Report when this happenned, but it was no later than 17:00 EDT	Situation report #4	SNS Operations Center
IL	13-May-03	17:01	Cook County EOC: Cook County has filed and recorded a disaster declaration to ensure authorization of certain emergency procedures		SEOC Event Log	IL State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	13-May-03	17:05	Evidence collection at the RDD site: RDD site broken into 4 quadrants to establish radiological reading per quandrant. EPA will follow FBI on site, then SFD will follow - 2 teams of 2 to mark GPS coordinates.		Data Collector Log	RDD site
IL	13-May-03	17:21	Lake County EOC received fax from IL JIC stating there will be no press release referring to county disaster declarations.		Data Collector Log	Lake County EOC
IA	13-May-03	17:30	A Task Force of 250 Army National Guardsmen has been activated and will be deployed at 06:00 PDT Wednesday morning to relieve Washington State Police troopers manning road closure checkpoints.		FEMA NEOC-EST	DHS/CAT
IA	13-May-03	17:30	All air traffic into O'Hare Airport has been suspended by order of DHS, in coordination with FAA and TSA. An exception was made to accommodate the transport of shipments from the SNS.		FEMA NEOC-EST Situation report	DHS/CAT
IA	13-May-03	17:30	HHS Secretary declared a Public Health Emergency in the City of Chicago, allowing the department to provide Federal health assistance under its own authority.		FEMA NEOC-EST	DHS/CAT
WA	13-May-03	17:32	VTC discussion across EOCs regarding conflicting information over road openings: WA State Police says highways are open, but WA DOT has the authority not the police. WA DOT wants to wait until confirmation from WA DOH that it's safe.		Data Collector Log	KC EOC
WA	13-May-03	17:35	FBI reports that the Seattle port has reopened		Analyst log	JOC CMG
IL	13-May-03	17:40	Chicago EOC obtains Chicago DPH's own stockpile; clinic set up at Westside to prophylaxis Chicago DPH staff; Logistics chief to epidemiology - EOC staff have PPE.		Data Collector Log	Chicago EOC
WA	13-May-03	17:40	DMORT arrived at the incident site. A meeting with FBI, SFD HAZMAT, and DMORT ensued to determine when and where the DMORT should set up their equipment in the hot zone. It was decided that in about an hour, FBI would allow DMORT to set up after FBI was finished.		Data Collector Log	RDD site
IL	13-May-03	17:45	VNN report: HSAS raised to red for entire nation, all transport in Chicago closed, 48 hour halt to all public gathering		Data Collector Log	IDPH
IL	13-May-03	17:47	VNN report: CDC announces health alert in Illinois		Data Collector Log	IL VCC
IL	13-May-03	17:49	Signed request for NDMS and DMAT sent to FEMA Region V ROC		SEOC Event Log	IL State EOC
IL	13-May-03	17:50	VNN report: DHS Secretary announces plague in Illinois; ports, trains, and airports all closed; urge people to stay in place; Hollywood celebrities says stay in place		Data Collector Log	IL VCC
IA	13-May-03	17:50	VNN press conference with DHS Secretary, HHS Secretary, and senior FBI representative. DHS Secretary confirms plague in Illinois; announces UN invocation of UN Charter Article V, announces elevation of HSAS level to Severe (Red) nationwide for 48 hours, associates the Seattle RDD and the Illinois plague with GLODO, and says that he has asked Mayors and Governors to implement Operation Liberty Shield-like protective actions.		Data Collector Log	MCC
WA	13-May-03	17:57	Seattle EOC evacuation overview: implementing plan to let people East of I-5 to leave home with instruction on how to do so. West of I-5 we will use the same protocol as last night to evacuate all people in exclusion area. Military will be providing bus drivers for metro busses. Will use out dialer to call all local residents. People will be told to take possessions for 3 days. Leave pets with three days of food and water. People will get screened at the airport; it will be voluntary screening but we highly reccomended they get screened. We will not mandate the evacuation, especially for seniors. Buses will run from 4-12 pm today. We will evacuate in an orderly manner so that no one is out standing and waiting for a bus to come along. SPD will monitor perimeter and keep out strays.		Data Collector Log	Seattle EOC
IL	13-May-03	18:00	Chicago EOC advised that SNS had been activated; surveillance staff discuss clinic staffing - decide to use existing model with plans for up to 6 distribution sites.		Data Collector Log	Chicago EOC
IL	13-May-03	18:00	IL Governor sent a letter through FEMA Region V requesting a Declaration of Major Disaster under the Stafford Act		SEOC Event Log	IL State EOC
WA	13-May-03	18:00	VNN report: DHS Secretary announcing HSAS raised to nationwide RED. PFO, who is now at the WA SEOC, just recieves confirmation that HSAS raised to red.	This event occurred between 15:00 and 15:30 PDT (18:00 and 18:30 EDT)	Data Collector Log	WA State EOC
IA	13-May-03	18:00	Regional FDA director reports restriction of all food supplies within plume area	The evaluation team could not confirm when this was implemented, but it was no later than 18:00 EDT	DHS CAT Briefing on the Federal Response to Seattle RDD	DHS-CAT
WA	13-May-03	18:04	USAR team arriving now and will be operational at 20:00. Another notional team will be arriving at 08:00.		Data Collector Log	RDD site
WA	13-May-03	18:10	Seattle EOC gradually shrinking contaminated zone based on new "analytic information"		Data Collector Log	KC EOC
WA	13-May-03	18:17	KC EOC policy room wants a copy of that press release - we want confirmation before " we roll that hand grenade out into the EOC".		Data Collector Log	KC EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	13-May-03	18:20	Seattle EOC Policy room: People come in all alarmed because DHS wants to go to Red nationwide. No one knows why but that requires Americans to stay home for 48 hours. The Mayor was not asked about this and this goes against his plan to return to normalcy. Conference in EOC Directions office on about statement. Why is DHS making this statement without contacting state county or city top officials? Recommendation is that we treat this as an unconfirmed rumor and get them (DHS) to back off.	This event occurred between 15:20 and 15:35 PDT (18:20 and 18:35 EDT)	Data Collector Log	Seattle EOC
WA	13-May-03	18:30	FEMA Region X ROC deputy director - directing staff to activate their "RED" plans and procedures		Data Collector Log	FEMA Region X ROC
WA	13-May-03	18:30	WA EMD Director requests guidance from DHS Secretary on steps to take when HSAS raised to RED. We need hard copy of recommended restrictions form DHS.		EOC Supervisor Log	WA State EOC
WA	13-May-03	18:31	WA DOH determines that I-5 can be reopened; WA DOH passes information to WA DOT		Data Collector Log	WA State EOC
IA	13-May-03	18:40	SNS Operations Center received request for SNS and approval to deploy 1 push-pack to Chicago	Follow-up calls by analyst confirm the deployment was approved by FEMA Director, EP&R, DHS, in conference with CDC Deputy Chief of Staff	Situation Report	SNS Operations Center
IA	13-May-03	18:58	HHS/SCC conference call - key discussion points: Prussian Blue availability and the lack of specific guidance on large-scale use; primarily used with people exposed after they are decontaminated. Difficulty of assessing internal exposure within individuals injured in the blast. Public Health officials recommend that travellers be alerted and a "fever watch" instituted for those people potentially exposed to plague. Chicago asked non-essential employees to stay home. That might impact availability of healthcare personnel.		Data Collector Log	HHS
IA	13-May-03	19:00	Memorandum for the President: Request for an Emergency Declaration for the State of Illinois From: Under Secretary, EP&R (Michael D. Brown). Event: On May 12,2003 Governor Blagojevich requested a major disaster declaration due to an outbreak of Pneumonic Plague in the City of Chicago (Cook County) and four surrounding counties. The Governor does not specify a specific type of assistance but rather requests supplemental Federal assistance to preserve lives and property and protect public peace, health and safety.		Data Collector Log	CDC EOC Atlanta
IL	13-May-03	19:18	Director of Chicago OEMC briefing: Press release provided declaring State of Emergency; Closing schools, O'Hare and Midway Airports are closed by DHS Secretary. SNS estimated to be arriving at 10:00 CDT (11:00 EDT) on May 14 at O'Hare Airport with 1 million doses for first responders and those first affected - this is enough meds to treat a single person for a week and is enough for Chicago and surrounding counties; there will be a lag period for breaking down SNS and distribution - hopefully, will begin the distribution on May 15.		Data Collector Log	Chicago EOC
WA	13-May-03	19:20	WA SEOC reviewed air space closures: because of RED alert status, decision was made that restrictions would remain in place		Data Collector Log	WA State EOC
WA	13-May-03	19:20	Road status: I-5 reopened, but not exit to downtown Seattle or West side of I-5; I-90, SR 520, and West Seattle bridge all reopened; SR 99 closed until sampling is completed, results expected in 2 hours.		Data Collector Log	WA State EOC
IL	13-May-03	19:25	Chicago EOC reports EMS volume increased by 10%; 6 ready reserve ambulances placed in service; private ambulance contractor notified for possible activation; 15 spare ambulances will require waiver from IDPH to place in service.		Data Collector Log	Chicago EOC
WA	13-May-03	19:30	WA SEOC News release: Washington State Ferries will resume their full public service schedule beginning at 4:30a.m.on May 14, with some exceptions		News Release	WA State EOC
WA	13-May-03	19:42	Deputy Mayor advises Mayor of I-5 opening. Flushing has already taken place. Public message to indicate significant delays; encourage public transportation.		Data Collector Log	RDD site
WA	13-May-03	19:54	SPD SWAT arrives at suspected GLODO safe house		Data Collector Log	RDD Site
WA	13-May-03	19:55	At 1500 hours, Washington Department of Health provided preliminary lab tests. These results showed the presence of four isotopes: cesium 137, plutonium 238, plutonium 239 and americium 241. Soil samples are being forwarded to DOE for more thorough analysis.		Intelligence Summary Report	WA FBI Field Office
WA	13-May-03	19:58	SPD SWAT completes take down of suspected GLODO safe house		Data Collector Log	RDD Site
IL	13-May-03	20:00	IEMA reported Midway and O'Hare airports are closed by DHS; curious if American Red Cross will attend to needs of stranded travelers		SEOC Event Log	IL State EOC
WA	13-May-03	20:16	SPD IC states crime scene part is done so SFD is in charge.		Data Collector Log	RDD site

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
WA	13-May-03	20:17	SFD requested mutual aid for HazMat to continue recovery operations		Data Collector Log	RDD site
WA	13-May-03	20:18	KC EOC policy room receives report that I-5 and West Seattle Bridge will reopen at 1800 tonight.		Data Collector Log	KC EOC
IA	13-May-03	21:05	The NRC reported yesterday evening at approximately 1800 (MST) the Palo Verde Generating Station received an anonymous bomb threat against the facility. The caller said the environment has been damaged enough through radiation poisoning and he and Allah will take revenge. The caller did not claim to be part of any terrorist organization and there is no evidence to corroborate the threat.		Data Collector Log	HHS
WA	13-May-03	21:14	Unified command meeting: 1) FBI advised their assets are pulled out. 2) FEMA advised they are in charge under FBI; FEMA has given command to locals - SPD and SFD have unified command now together.		Data Collector Log	RDD site
WA	13-May-03	22:40	King County Executive in keeping with DHS Secretary request for all people to remain at home made the following announcements regarding County services effective through Thursday, May 15: Essential County services will be maintained such as public health and safety, however, only essential personnel will be on duty; The District and Superior Court Judges have suspended all scheduled hearings at all court locationjs. Scheduled jurors should not report until further notice; The Regional Justice Center in Kent Jail Division will continue as it has this week; Metro Transit will be operating on a modified holiday schedule. The Downtown Seattle Transit Tunnel will be closed; All King County transfer facilities and Cedar Hills landfill will be closed until further notice. Residents that have garbage should bag their garbage put in a secure place until service resumes; King County is asking all essential personnel to report for work. King County employees should check with their supervisors; Updates on this and other information can be found on our Web site at www.metrokc.gov or by listening to local news.		Press Release	KC IC
IA	13-May-03	22:50	SIOC: recommend that Chicago should stand-up a JOC		Data Collector Log	FBI SIOC
IA	13-May-03	22:50	HHS convenes Emergency Policy Support Group.		Data Collector Log	FBI SIOC
WA	13-May-03	23:22	WA SEOC received call from Seattle EOC that field play concluded		Data Collector Log	WA State EOC
WA	14-May-03	0:25	Consider this a formal request from the State of Washington: City of Seattle is requesting release of prepositioned equipment package being held at Boeing Field by DHS.		Email	WA State EOC
IA	14-May-03	2:55	HS Center report from FEMA EST: The FEMA EST is requesting guidance as to what is the expectations of the States under treat condition "Red."	Period Covered: 0200 May 14, 2003 to 1300 May 14, 2003 PDT	Region X ROC input to EP&R situation report	DHS-CAT
IA	14-May-03	8:10	FEMA conference call with Regions to discuss numerous State inquiries regarding SNS push packages.	Period covered: 0700 hours EDT May 13 to 1730 EDT May 15	EST Situation Report	FEMA NEOC-EST
IL	14-May-03	8:18	DuPage County DPH Director authorized the release of antibiotics to his staff.		Data Collector Log	DuPage Co. Health
IA	14-May-03	8:23	INJECT: DOT FRA activates the Regional FRA COOP plan in Chicago		Data Collector Log	DOT CMC
IL	14-May-03	8:25	Phone conversation between IOHNO and IDPH: per IL Gov's press release, United Center and Union Station was not listed to close down - IDPH recommends those venues be closed until FBI/Law enforcement determines terrorist related and marks those venues as crime scene.		Data Collector Log	IOHNO
IL	14-May-03	8:35	DuPage County DPH morning briefing: at 15:25 CDT (16:25 EDT) on May 13, IDPH released information about plague, requested the SNS, and authorized distribution of antibiotics to those who may have been exposed; at 17:42 CDT (18:42 EDT) on May 13, IDPH reported plague confirmed; people who were at United Center, Union Station or O'Hare on May 10 or later may be exposed and recommended for prophylaxis; a local declaration is no longer needed as the state declaration is sufficient.		Data Collector Log	DuPage Co Health
IL	14-May-03	8:40	DuPage County DPH directed the staff to prepare for the delivery of the SNS.		Data Collector Log	DuPage Co. Health
IA	14-May-03	8:45	TSA and FRA discuss potential rail shutdown. FRA clarifies that STB in the only authority that can shut down rail.		Data Collector Log	VA Central Office
IL	14-May-03	9:00	ARC agrees to support stranded travelers with mass care, health services, and mental health.		Data Collector Log	ARC - Chicago HQ
IL	14-May-03	9:05	DHS Secretary provides update on VNN: terrorist attack, plague confirmed, bioterrorism event.		Data Collector Log	IOHNO
IA	14-May-03	9:11	MST tasked to come up with recommendations for disposing of contaminated bodies. CDC working with MST to do this.		Data Collector Log	DOT CMC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	14-May-03	9:17	IDPH Director authorized distribution of prophylaxis to first responders.		Detailed Incident Report	DuPage County EOC
IL	14-May-03	9:30	Chicago DPH Situation report: NDMS requested.		Situation report	Chicago DPH
IL	14-May-03	9:30	Chicago DPH Situation Report. O'Hare and Midway airports and Union Station in Chicago have been closed by the U.S. Department of Homeland Security (DHS)		Situation report	Chicago DPH
IL	14-May-03	9:30	Chicago DPH Situation report: IL Governor has recommended that non-essential workers in the affected area stay home. Schools in Cook, DuPage, Kane and Lake counties have been closed. DHS has recommended that all non-essential large public gatherings be cancelled.		Situation report	Chicago DPH
IL	14-May-03	9:30	VNN report: DHS Secretary has closed O'Hare, Midway airports and Union Station		Data Collector Log	Springfield IDPH
IA	14-May-03	9:45	Department of Veterans Affairs update to HS Center: VA has informed all facilities of increase in National Threat Level to RED and initiated the implementation of level red protective measures for all VA facilities. In response to alert level RED, VA's pre-COOP team is on alert to deploy (notionally) to VA's primary COOP site at 15:00 this Wednesday afternoon. A Secretarial successor will be on-site. 20 Plague patients presented to VA Medical Center Hine, Illinois; 10 patients were admitted to isolation beds and 10 died. VA provided the White House and HHS inventory of pharmaceutical assets, apporpriate for use in the treatment and management of Plague, located in the Chicago area.		Data Collector Log	DHHS-SCC
IL	14-May-03	9:48	DuPage County DPH notified DuPage County EOC to tell first responders to come for prophylaxis.		Data Collector Log	DuPage Co. Health
IL	14-May-03	9:57	IDPH requesting: 5 IL DOT vehicles and drivers; 5 IL Corrections vehicles and drivers; 27 IL State policemen and 6 cars; and 40 IL National Guard members to be at the FedEx Terminal at O'Hare Airport by 10:00 CDT (11:00 EDT).		SEOC Event Log	IL State EOC
IL	14-May-03	10:00	La Grange Hospital received fax from IL Governor warning employees of non-essential businesses to stay home until further notice.		Data Collector Log	LaGrange
IL	14-May-03	10:00	City of Chicago shut down all passenger transportation in and out of Chicago, including airports.		Data Collector Log	FEMA Region V ROC
IL	14-May-03	10:03	IL Governor signs "Executive Order" considering this to be a possible bioterrorist, suspended HIPAA and Blood Banks...allow state to share communicable disease information with law enforcement; suspended licensing act so that physicians can practice in places where they are not licensed...temporarily supend legal constraints on other professionals so that others can dispense medications, and disseminate at other places other than pharmacies (distribution and administration of antibiotics).		Data Collector Log	Lake County EOC
IA	14-May-03	10:05	The President (notional) granted an emergency declaration (FEMA-4322-EM-IL) to Illinois May 14, to address the health crisis in the Chicago area. The declaration covers Cook, DuPage, Kane and Lake Counties. An FCO was appointed.	Note: A Major Disaster Declaration was requested by the IL Governor, but an Emergency Declaration was granted.	Declaration	DHS/CAT
IA	14-May-03	10:06	The White House, FBI and DHS are looking to HHS for leadership in crafting public health message concerning events in Chicago and Seattle.		Data Collector Log	VA Central Office
IA	14-May-03	10:06	CDC called SIOC: Deployed SNS push pack and re-deployed teams		Data Collector Log	VA Central Office
IA	14-May-03	10:06	FPS has deployed police officers to support CDC operations in Chicago to augment security operations since deaths and plague cases are increasing drastically today.		Data Collector Log	VA Central Office
IL	14-May-03	10:14	IL SEOC reports that DuPage County has begun the prophylactic distribution process.		SEOC Event Log	IL State EOC
IL	14-May-03	10:16	To Lake County Government Employees from County Board Chairman: Lake County joined several other government entities "in declaring a disaster situation in particular jurisdictions... as part of the disaster declaration. Lake County Government offices will be closed beginning tomorrow, Wednesday, May 14th except for those personnel required for the continuation of critical government functions. This is in concurrence with US DHS Secretary's advice that people "take a snow day" in order to remain isolated and safe in their homes."		Email	Lake County EOC
IL	14-May-03	10:30	CCDPH notified of meeting earlier this morning between Cook County Chief Counsel and IL Governor: considering this to be a possible bioterrorist, suspended HIPAA and Blood Banks...allow state to share communicable disease information with law enforcements; suspended licensing act so that physicians can practice in places where they are not licensed...temporarily suspend legal constraints on other professionals so that others can dispense medications, and disseminate at other places other than pharmacies (distribution and administration of antibiotics)...		CCDPH Player Log	Cook County DPH
IL	14-May-03	10:30	Press conference at IL JIC: confirms release of plague at United Center, O'Hare and Union Station - only at these three sites. Governor actions: requests SNS deployment, State of Emergency in IL, deployment of WMD team and IMERT Team to increase security.		EOC Log	Lake County EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	14-May-03	10:30	Lake County EOC report to Lake County Health Department Incident Command Post: DuPage County beginning prophylaxis of first responders with DuPage County Department of Health stockpile.		Email	Lake County EOC
IL	14-May-03	10:35	IOHNO requests Deoxycycline, Ciprofloxacin, surgical masks, and ventilators from VMI		Data Collector Log	IOHNO
WA	14-May-03	11:00	FEMA Region X ROC transferring management of recovery operations to DFO tomorrow at 12:00 and will handle RDD-related issues		Data Collector Log	HHS Region X REOC
IL	14-May-03	11:03	IDPH Lab receives ILexecutive orders suspending privacy rights, etc…		Data Collector Log	IDPH lab
IL	14-May-03	11:03	FEMA Region V ROC reports to IL SEOC that 18 hospitals in Chicago & suburbs are at maximum capacity. FEMA needs to know the names of the hospitals to support. Regarding the NDMS request - please report information to FEMA liaison at IL SEOC for transmittal back to FEMA Region V ROC		SEOC Event Log	IL State EOC
IL	14-May-03	11:08	Chicaco EOC confirmed: O'Hare airport is closed; midway airport is closed; Union station and all railways are shut down; all bus systems in and out of the city are suspended.		Detailed Incident Report	DuPage County EOC
IL	14-May-03	11:10	IDPH has established an information hotline 1-877 867 6332		SEOC Event Log	IL State EOC
WA	14-May-03	11:20	Based on new information, SeaTac is outside the TFR; air traffic controllers can reroute traffic to evoid waivers		Data Collector Log	FEMA Region X ROC
IL	14-May-03	11:25	IL DOT liaison at O'Hare FedEx terminal reported to IL SEOC that SNS has arrived		SEOC Event Log	IL State EOC
IL	14-May-03	11:30	Chicago EOC received clarification of Chicago Transit Authority service: service continues within city limits; no service to suburbs or airports.		Data Collector Log	Chicago EOC
WA	14-May-03	11:30	NMRT arrived at VA Hospital (WA)		Data Collector Log	VA Hospital (WA)
IL	14-May-03	11:32	CCSEMA received fax from DHS/FEMA - IL granted Federal Emergency Declaration		Message & Event Log	CCSEMA
IL	14-May-03	11:33	Vancouver officials acknowledged that their plague victims came from Air Canada flight #783 on May 10 from Chicago.		Agency Log	Chicago DPH
IL	14-May-03	11:35	CDC has arrived at IOHNO to assist with SNS.		Data Collector Log	IOHNO
IL	14-May-03	11:40	IL SEOC advised that the SWMDTs are attempting to rescue a security guard who has been shot behind building 32 at Nalco Chemical Plant		SEOC Event Log	IL State EOC
IL	14-May-03	11:45	Cook County EOC receives CDC Health Alert; recommends prophylaxis and protection of workers at suspected plague release sites. Three sites in the Chicago area have been identified as likely exposure sites based on the initial epidemiologic information. The sites identified are the United Center, Union Station and O'Hare International Airport. Persons who have been in these venues for the period May 10 through May 13 are advised to seek antibiotic prophylaxis.		HAN	Cook County EOC
IL	14-May-03	11:45	IDPH and CDC liaisons at IOHNOI note that Federal SNS assets are being released without a federal disaster declaration.		Data Collector Log	IOHNO
IL	14-May-03	11:47	SNS being loaded onto semis for movement; scheduled for actual move at 12:30 CDT (13:30 EDT)		Command Post Log	Nalco Chemical Plant Bldg 26

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	14-May-03	11:56	CDC formally signs over entire SNS package.		Data Collector Log	SNS Reception Site at O'Hare International Airport
IL	14-May-03	11:56	IDPH Lab hears about shooting in at Nalco Chemical Plant.		Data Collector Log	IDPH Lab
IL	14-May-03	12:00	Ingalls Hospital received fax from IDPH: presumptive plague exposure at Chicago Union Station and O'Hare Airport International Terminal limited to May 10.		Data Collector Log	Ingalls
IL	14-May-03	12:03	VNN clarifies plague cases and deaths in Chicago: 333 dead and 1,676 suspected cases. Presidential declaration made. FBI confirms terrorist attack		Data Collector Log	ARC - Chicago HQ
IL	14-May-03	12:15	FEMA Region V ROC reported to IL SEOC: at 10:05 CDT (11:05 EDT), the President signed an Emergency Declaration for IL ; as of 10:55 CDT (11:55 EDT). FEMA Region V ROC did not have a copy of declaration nor assigned disaster number; not known if declaration applies to entire State or just specific counties.		SEOC Event Log	IL State EOC
IL	14-May-03	12:15	Security guard has been rescued and transported to local hospital; investigations to conduct interview of guard.		Command Post Log	Nalco Chemical Plant Bldg 30
IA	14-May-03	12:25	FEMA and TSA discuss obtaining waivers for emergency flights through restricted airspace.		Data Collector Log	FEMA EST
IL	14-May-03	12:30	Lake County EOC learns that IL granted Federal Emergency Declaration		Agency Log	Lake County EOC
WA	14-May-03	12:30	King County update regarding Airports: Seatac is open and on normal operations. FAA restrictions: TFR reduced to an elevation of 2,000 ft. King County Airport open Renton and Paine Field Airports open.		Coordination Briefing	KC EOC
IL	14-May-03	12:35	DMORT has been activated - they will deploy to Hines VA Hospital (IL); Satellite clinic site requested to be opened at Hines VA		Incident Report	Cook County EOC
IL	14-May-03	12:43	DuPage County EOC requested all county emergency management agencies, City of Chicago, IL JOC, and IL SEOC to join a conference call at 13:00 CDT (14:00 EDT) to discuss SNS prophylaxis strategy. It is suggested that the county board chair/administrator sit in if possible.		Email	Lake County EOC
IL	14-May-03	12:50	IDPH now has 30K + 30K doses available for Chicago; Public messages will be clear about risk groups and not to abuse system. Those who have been in contact with known cases (family members, etc) to be ssued coupons for identification. 300K doses to be delivered by per day.		Data Collector Log	Chicago EOC
IL	14-May-03	12:50	Press Release that Plague outbreak linked to three Chicago area locations from May 10: International Terminal at O'Hare Airport, United Center, and Union Station.		EOC Log	Lake County EOC
WA	14-May-03	13:00	WA SEOC received casualty status from Seattle EOC: 20 Confirmed Dead; 130 Injured		Situation Report	WA State EOC
IA	14-May-03	13:08	FPS has contacted CDC in Atlanta to advise that Emergency Response Team is on stand-by and available to support their security guards in the event that there are protests or attempts to get into their facility for plague anitdotes.		Data Collector Log	DOT CMC
IL	14-May-03	13:10	CCSEMA received call from Cook County Medical Examiner (CCME): report that Chicago Police requested and received a deployment of 8,000 National Guard troops who can assist with mortuary services. CCME's office has requested 200 of these troops to be dedicated to Cook County mortuary operations.		Message & Event Log	CCSEMA

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	14-May-03	13:25	VNN report: DHS Secretary instructing all citizens working at any of the (or was at any of the) target sites should go immediately to a medical facility for medications. DuPage County Emergency Management Agency response is to 1. Call hospitals. 2. Law enforcement.		Data Collector Log	DuPage County EOC
IL	14-May-03	13:25	DuPage County Commissioner recommends immediate PIO release - "Ignore" the FEDS, listen to local officers. Conflict between DHS Secretary's exact comments and what had already been released to Media.		Data Collector Log	DuPage County EOC
IL	14-May-03	13:30	SNS was received at 12:30 by Cook County Sheriff's office; contains only 5% of the shipment we were suppose to receive.		Agency Log	Cook County DPH
IL	14-May-03	13:30	Request came into IL SEOC from EPA to perform monitoring (BIOWATCH) at Union Station, O'Hare field and United Center. EPA is moving some portable sampling devices from Wisconsin to Des Plaines (IEPA's Regional Office). Target to have the additional sampling locations operational is 14:30 CDT (15:30 EDT)		SEOC Event Log	IL State EOC
IL	14-May-03	13:30	VNN report: GLODO claims responsibility for terrorist attack of plague in Chicago. They say "their terror is now our terror."		SEOC Event Log	IL State EOC
IL	14-May-03	13:36	Chicago DPH closing major assembiles and events in Chicago.		CDPH	Chicago DPH
IA	14-May-03	13:59	Cook County has requested VA to supply 25 refrigerated trucks to serve as morgue		Data Collector Log	VACO
IL	14-May-03	14:02	Open conference call between IDPH and the 5 effected counties. Issues discussed involved number of doses and the number of cases which could be addressed. Concern about unexposed people coming to distribution centers to get medications and getting exposed at the site. Media problem - need to get people to understand that if they are not symptomatic, were not at one of the three sites, and were not exposed, they don't need to take medications. Medications are not an endless supply and Illinois may only be the 1st state to be hit.	Earlier request for this meeting suggested top officials be present, they don't appear to have attended	Data Collector Log	Cook County EOC
IL	14-May-03	14:24	Press release: HHS Sends Medical Staff To Chicago		Email	Lake County EOC
IL	14-May-03	14:28	Joint Media Release: HEALTH OFFICIALS ANNOUNCE LOCATIONS OF PLAGUE RELEASE. The office of IL Governor announced this morning three locations where plague was released by terrorists last Saturday, May 10. The locations are Union Station in downtown Chicago, the International Terminal of O'Hare airport and United Center on the city's west side. No other sites have been identified... Those who were at one of the sites on Saturday should receive antibiotics to prevent the development of illness. Those in close contact with someone exhibiting symptoms should also receive antibiotics.		Email	Lake County EOC
IL	14-May-03	14:40	Cook County EOC reports: CCDPH personnel starting to offload and break down SNS; CCSEMA duty officer onsite at Bridgeview dispensing site.		Email	Lake County EOC
IL	13-May-03	14:59	Good Samaritan Hospital ER received call from Loyola Hospital to activate Phase II of IL Emergency Medical Disaster Plan		Data Collector Log	Good Samaritan Hospital
IL	14-May-03	15:00	IL Department of Natural Resources (DNR) closing IL state parks		SEOC Event Log	IL State EOC
WA	14-May-03	15:05	USCG lifted No Sail Order in WA		Agency Log	KC EOC
IL	14-May-03	15:20	Chicago EOC received EmNet Emergency Message: the SNS have been received, broken down and loaded for delivery to the dispensing site.		EmNet Emergency Message	Chicago DPH
IL	14-May-03	15:25	Kane County would like wait to release information about SNS distribution until the morning of May 15 - only 1 distribution site in Kane County; fear that an earlier release would not be beneficial. There appears to be a consensus that information will be released this evening stating that distribution sites will be made public on the morning of the 15th.		Data Collector Log	Kane County DPH
IL	14-May-03	15:35	FEMA provided information to IL SEOC: Presidential Emergency Declaration applies to 4 affected counties in IL: Cook (including Chicago), DuPage, Kane and Lake		SEOC Event Log	IL State EOC
IL	14-May-03	15:45	Call from CCSEMA Staff & Duty Officer - SNS arrived at Bridgeview dispensing site		Message & Event Log	CCSEMA
WA	14-May-03	16:02	Burlington Northern Santa Fe report of a possible complete shutdown of Amtrak & Sounder passenger Service. Some trains in the "hot zone" and won't know the extensive assessment of the contamination for weeks or months. Freight is being routed around exclusion area from Ballard to Tukwila. Potential economic impact discussed		Situation Report	KC EOC
IL	14-May-03	16:10	Kane County has received its allottment of the SNS		SEOC Event Log	IL State EOC
IL	14-May-03	16:10	Lake County EOC to lake County Health Department Incident Command Post concerning SNS eligibility: Shortage of medications through SNS (IL Pharmaceutical Stockpile going to hospitals); need recommendations as to how limited supply would be used. REPLY: Vendor Managed Inventory implemented - number of antibiotics is no longer an issue; however, mass prophylaxis - to any and all - is being discussed by health departments in region.		Email	Lake County EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	14-May-03	16:15	City of Chicago expecting SNS to arrive at 14:45 CDT (15:45 EDT)		Data Collector Log	Chicago FD Training Academy
IL	14-May-03	16:15	ARC of Greater Chicago CEO on VNN: confirms blood supply in Chicago is safe - no need for new donations. Also, ARC of Greater Chicago Disaster Welfare Information System lines are open for separated family members. Red Cross health and mental health workers are at hospitals, airports, and rail stations to support stranded passengers.		Data Collector Log	ARC - Chicago HQ
IL	14-May-03	16:22	Multiple hospitals indicate that there are no medical beds available. Concerns regarding staffing. Hospitals have gone to lock down mode due to increased crowds.		Detailed Incident Report	DuPage County EOC
IL	14-May-03	16:25	Chicago Fire Department Chief: 120 boxes of inbound SNS will stay at Fire Department; the rest will go with City Department of Health to distribution site.		Data Collector Log	Chicago FD Training Academy
WA	14-May-03	16:25	WA Dept. of Agriculture established food control areas and road access checkpoints for agricultural products in potentially affected counties to prevent people consuming contaminated fresh food and milk products.	Don't know if this is the final food control plan	Talking points for TOPOFF 2. Food and Safety Control	WA State EOC
WA	14-May-03	16:32	WA DOH realizing exclusionary zone probably should have been expanded 2 days ago. Concerned about wind increase and dispersement of the elements. WA DOH very concerned about Seattle's plan to further shrink the exclusion zone		Data Collector Log	WA State EOC
IL	14-May-03	16:35	Chicago OEMC requested an additional 4000 IL National Guard troops		SEOC Event Log	IL State EOC
IL	14-May-03	16:55	IL officials concerned that Presidential Emergency Declaration vice Major Disaster Declarion results in loss of (a) crisis counseling and (b) disaster unemployment aid; Department of Justice may be able to fill gap with victim fund.		Data Collector Log	FEMA Region V ROC
IL	14-May-03	16:56	SNS arrived at Lake County drop-off site.		Data Collector Log	Lake County EOC
IL	14-May-03	17:31	Chicago EOC reports that SNS arrived at the Lake County Reception site at 14:50 CDT (15:50 EDT). It has been broken down and distribution to first responders has commenced as of 16:00 CDT (17:00 EDT).	Similar report reached IL SEOC at 16:32 CDT (17:32 EDT)	Emnet Emergency Message	Chicago DPH
IL	14-May-03	17:39	Chicago EOC developing a plan for all city employees to receive training and education on the risks and hazards of the current outbreak. Information being developed by all agencies, with the Chicago DPH taking the lead. Information will go out to all agencies and PIOs from affected groups. Looking at a coordinated program for union and non-union employees. Developing training video: copies to all represented departments and agencies. Training video on Channel 23 – the municipal channel; press releases already on City's internet site; this training video will be on this internet channel too. Chicago OEMC PIOs putting together radio and TV Public Service Announcements – 30 seconds. Chicago Alternative Police Strategies (CAPs) distribution program – to contact block clubs; other languages to reach diverse populations of Chicago: Polish, Spanish, Arabic, English. Leadership by example – management will lead union employees as they enter areas considered to be "at risk."		Data Collector Log	Chicago EOC
IL	14-May-03	17:40	CCSEMA received call from Cook County Sheriff's Command Center: first responders have started to receive the medication at Bridgeview dispensing site		Message & Event Log	CCSEMA
IL	14-May-03	17:40	Cook County EOC Press Release: FOR IMMEDIATE RELEASE - GOVERNOR ANNOUNCES RECEIPT, BREAKDOWN AND DISTRIBUTION OF SNS		Press Release	Cook County EOC
WA	14-May-03	17:51	WA DOH just receives fax with radiological data that arrived at SEOC yesterday. Clear that the readings exceed boundary of City's exclusionary area.		Data Collector Log	WA State EOC
IL	14-May-03	18:00	CFD Fire Academy Commander reports to Chicago EOC: they have notified outside agencies to begin picking up SNS prophylactic meds at Fire Academy; Chicago Police Dept.'s picked up 5500 doses; Chicago DPH will release rest as necessary.		Data Collector Log	Chicago EOC
IL	14-May-03	18:15	Lake County EOC: IL Governor recommends public and employees of non-essential businesses to stay home until further notice; Chicago area - target of terrorist attack.		Agency Log	Lake County EOC
IL	14-May-03	18:22	Chicago EOC: SNS arrived; holding on to drugs until 08:00 tomorrow morning as was decided with the other counties.		Data Collector Log	Chicago EOC
IL	14-May-03	18:42	IL SEOC briefing: Chicago distribution centers will operate 8:00am-4:00pm tomorrow / Cook and Lake Counties will open at 8:00am - closing time not known; DuPage & Kane Counties - no information		SEOC Event Log	IL State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	14-May-03	18:50	SNS Reception Site reported to the IL JOC that the SNS relay had been delivered and the detail secured. The Command Post at O'Hare has been sealed and closed. The relay was completed without incident.		SEOC Event Log	IL State EOC
IA	14-May-03	18:50	Defense Coordinating Officers deployed to Seattle and Chicago	This was reported between 18:50 and 19:20 EDT	Data Collector Log	VA Central Office
IL	14-May-03	19:03	Chicago DPH received EmNet emergency message: DuPage County has begun prophylactic distribution procedures		EmNet Emergency Message	Chicago DPH
WA	14-May-03	20:00	WA SEOC reports in SITREP that WA National Guard will activate 2 additional task forces (a total of 500 soldiers) to support law enforcement agencies.		Situation Report	WA State EOC
IL	14-May-03	20:26	IL SEOC received EmNet emergency message: Cook County Dispensing site located in Bridgeview has closed as of 19:00 CDT (20:00 EDT). The first responders have been given the medications. The dispensing site will re-open at 08:00 CDT (09:00 EDT) on May 15 for dispensing to the public.		SEOC Event Log	IL State EOC
IL	14-May-03	20:37	IL SEOC provided the following inject: Vendor Managed Inventory from the SNS arrived in IL. The State of IL has begun distribution of antibiotics and medical supplies. SNS requests made by local health deptartments and hospitals will continue to be filled for the length of the event		SEOC Event Log	IL State EOC
IL	14-May-03	20:38	IL SEOC report: VMI has arrived at O'Hare. State distribution staff are breaking down and will distribute to local jurisdictions as previously reported		SEOC Event Log	IL State EOC
IL	14-May-03	21:30	SNS Distribution Process: Chicago expected 60,000 doses. SNS broken down at CFA (Chicago fire Academy); only 5,500 sent over.		Data Collector Log	Chicago EOC
IL	14-May-03	22:22	IL SEOC receives report from IL State Police: Unified Command Post advised of suspect in custody who provided following info: (1) Member of Free America Group; (2) No hostages in building; (3) There is lab equipment in men's room of Nalco Chemical Bldg. 32; (4) A rail car on west side of Bldg. 32 has explosives; (5) A tank in Bldg. 32 on north side has explosives; (6) A tractor/trailer parked outside Bldg. 32 with unknown chemicals; (7) There are several booby traps in Bldg. 32		SEOC Event Log	IL State EOC
IL	14-May-03	23:15	IL SEOC sent fax to 4 counties and Chicago that VMI has been received. Being broken down at O'Hare airport. Available upon request to each county and Chicago.		SEOC Event Log	IL State EOC
IL	14-May-03	23:39	Tactical Response Team (TRT) made entry into Nalco Chemical building #32 and are inside		Command Post Log	Nalco Chemical Plant Bldg 146
IL	14-May-03	23:45	TRT advised 3 males and 1 female in custody		Command Post Log	NALCO chem plant bldg 9
IL	15-May-03	0:08	Report to IL SEOC: TRT entered Nalco Chemical Building; 3 male, 1 female in custody. 4 subjects and 16 TRT being contaminated. Preparing to sweep for explosives. Investigating personnel waiting to interrogate.		SEOC Event Log	IL State EOC
IA	15-May-03	0:15	CBP Update: -Holding all containers from high-risk countries (Pinkland, Orangeland, and Redland) transiting through CSI participating countries and increase examination scrutiny up to 100% of containers destined for the US -Deployed Border Patrol Tactical Unit (BORTAC) units (12 members each) to Seattle and to a staging location near Chicago; CBP will coordinate with the US Marshals Service for J-PATS flights to provide air Transportation Security Administration -Passenger Manifests for all international flights departing O'Hare since 11 May shared with State and Foreign LE counterparts to locate potential plague cases		Secretary's Morning Summary Operational Response	DHS HSCenter
IA	15-May-03	0:15	Transportation: -Nationwide: Liberty Shield level 1 and 2 transportation restrictions. -Nationwide: All passenger rail stopped, TSA authority questioned by Federal Railroad Administration -Port of Chicago at MarSec 3 - commercial vessel crews restricted to vessels -Chicago: Second day of transportation restrictions in Metro area		Secretary's Morning Summary Operational Response	DHS HSCenter
IA	15-May-03	0:15	EP&R Update: -EP&R Experts on scene in Chicago: 13 NDMS specialists, 14 EPI intelligence service officers, CCRF: 150 Nurses, 25 Physicians (arrive 15 May), transport of 175 Medical Personnel to Chicago -EP&R Assets in route: 2 DMATS, 1 DMORT, 50 respiratory Technicians		Secretary's Morning Summary Operational Response	DHS HSCenter
IL	15-May-03	0:20	IL State Police: 1 male subject with sucking chest would being transported to Christ Hospital, Oak Lawn. 2 investigators in ambulance, uniformed officer also being sent to hospital for security. Other 3 subjects uninjured, being transported to Bedford Park PD, FBI en route. No injuries to ISP. Chemical still unknown. Decon by Bedford Park Fire department.		SEOC Event Log	IL State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	15-May-03	0:35	IL State Police meeting with FBI. They are in agreement with bringing in team from US EPA		SEOC Event Log	IL State EOC
IL	15-May-03	1:32	Chicago Police Dept. begins distribution of prophylaxis to Police department		Data Collector Log	Chicago EOC
IL	15-May-03	1:41	IL SEOC update on Nalco Chemical Building: ISP reports Bomb Squad has located two explosive devices. Device #1 is attached to rail tank car containing hydrazine and is a briefcase. Device #2 is attached to a rail tank car containing dichlorobutene and is equipped with a motion sensor. Working with Chicago Fire/Police, Bedford Park Fire/Police, IEMA & IMERT to extend evacuation area to 1/2 mile		SEOC Event Log	IL State EOC
IA	15-May-03	5:45	FEMA EST Situation Update: To limit the potential for spreading the disease, the transportation centers of O'Hare Airport, Midway Airport, Union Station and the Port of Chicago have been closed.		Region X ROC Input to EP&R situation report	DHS/HSCenter
IA	15-May-03	7:00	FEMA EST Situation Update: DHS reports transportation restrictions in Seattle have been lifted, except the nuclear power plant.		Data Collector Log	FEMA EST
IL	15-May-03	8:30	Joint media release: Dispensing Site Locations for Antibiotics Announced. Health Depts will provide antibiotics for all those affected by plague outbreak. Clinics: Chicago, 100 W. Virginia Street; Cook County, 120 St. James Place, Bolingbrook, DuPage County: 34 Marvin Gardens, Wheaton, Kane County: 46 Park Place, Aurora, Lake County: 75 Boardwalk, Wauconda		Joint Media Release	Cook County EOC
IA	15-May-03	8:57	VNN report: 103 Deaths in Canada - 54 Vancouver, 21 Toronto, 22 Ottawa, 1 Edmonton, 2 cases Montreal & Winnipeg		Situation report FEMA NEOC-EST	DHS-CAT
IA	15-May-03	8:57	FEMA EST Situation Update: FTA is working with WA DOH to have Ferries and terminals at Seattle, Bremerton, and Bainbridge decontaminated.		Situation report FEMA NEOC-EST	DHS-CAT
IL	15-May-03	9:00	Chicago EOC announced prophylaxis sites open to the public.		Data Collector Log	Chicago EOC
IL	15-May-03	9:00	VNN news notifying the public of dispensing of meds: Symptomatic persons are to seek medical attention. Persons who were at the 3 sites or those persons exposed to people who were at the 3 sites are to go to the facility to get meds.		Data Collector Log	Cook County EOC
IA	15-May-03	9:57	VNN report: Bio lab found in Bedford, IL		Data Collector Log	DOT CMC
IL	15-May-03	10:02	Kane County DPH reports SNS arrives and brought down for distribution		Data Collector Log	IMSA - Kane DPH
IL	15-May-03	10:03	IL SEOC reports: Lake County began dispensing operations at 8:32 CDT (9:32 EDT)		SEOC Event Log	IL State EOC
IL	15-May-03	10:06	IL SEOC reports: Du Page County began dispensing SNS at 08:00 CDT (09:00 EDT)		SEOC Event Log	IL State EOC
IL	15-May-03	10:20	ISP and FBI confirm backpacks with aerosol cans were located at airport and were used for distributing of plague.		SEOC Event Log	IL State EOC
IL	15-May-03	10:32	IL SEOC received EmNet Emergency message from IL JOC: FEMA representative indicated that there has been a toll free # set-up for financial assistance and for hearing impaired. Also reimbursement is available to local and state agencies for eligible costs of equipment, contracts and personnel overtime related to emergency services in dealing with plague event		SEOC Event Log	IL State EOC
IL	15-May-03	10:39	FBI reports that they have information that suspects dispersed aerosolized plague from backpacks - it is not known at this time if they were dispersed at additional sites or same as original attack - state police directed to get decon of possible additional releases.		Data Collector Log	IL State EOC
IL	15-May-03	10:40	IL SEOC is requesting the DMORT assist the medical examiners office of Cook County.		SEOC Event Log	IL State EOC
IL	15-May-03	10:59	IL SEOC reports all SNS distribution sites verified open and operational		SEOC Event Log	IL State EOC
IA	15-May-03	11:06	The Governor of Wisconsin sent a request to FEMA Region V which was passed to DHS EP&R for a disaster declaration: The Governor's request dated May 15,2003 satisfies the various statutory and regulatory requirements of Public Law 93-288, as amended. The Governor has requested a major disaster declaration for the counties of Kenosha, Milwaukee, and Racine. As a result of an outbreak of Pneumonic Plague, the Governor implemented the State Emergency Plan on May 15,2003 and declared a state emergency for these counties on May 15, 2003.		Data Collector Log	DOT CMC
IL	15-May-03	12:30	Report from Chicago EOC that plague is still present at Union station, United Center, O'Hare		Data Collector Log	Chicago JOC
IL	15-May-03	14:00	From IDPH to Dept. of State Liasion: VNN report stated IDPH did not want assistance from other nations due to lesser quality of health care & language barrier. IDPH viewed this as arrogance and requested to know who made this statement		Agency Log	DOS Liaison at IDPH
IL	15-May-03	14:20	FBI announces United Center, Union Station, and Terminal 3 at O'Hare cleared as crime scenes. US EPA says they can be opened to the public.		SEOC Event Log	IL State EOC

Venue	Date (EDT)	Time (EDT)	Description	Analyst Comment	Type of Data	Source Organization
IL	15-May-03	16:10	IL SEOC received request from FBI HMRU unit. Request asks for 2 HazMat officers from 5th CST to assist in operations. CST soldiers are available. Adjutant General has been notified and approved the mission request, with one stipulation - if CST gets talked by State/Feds as a team, 2 soldiers will return to CST control for mission support.		SEOC Event Log	IL State EOC
IL	15-May-03	16:15	IL SEOC received EmNet Emergency Message from IL JOC: FEMA Region V ROC has indicated that the National Homeland Security Advisory System level will be lowered from Red to Orange with the EXCEPTION of Chicago and New York City, which shall remain at Red.		SEOC Event Log	IL State EOC
IL	15-May-03	16:15	Chicago Department of Health & Human Services notifies Chicago OEM of reducted alert status from "Red" to "Orange" nationwide except Chicago and New York City.		Data Collector Log	Chicago EOC
IL	15-May-03	16:50	Chicago EOC receives formal notification that Nationwide Threat level lowered from Red to Orange except for New York City and Chicago		Data Collector Log	Chicago EOC
IL	15-May-03	20:38	JOC received Update from Chicago Fire Department regarding crash at Midway Airport: helicopter was completely destroyed, 10 dead, 51 serious injuries, 59 minor and 79 minimal. CPD says that crash was an accident and not terrorist attack (corresponds to MSEL # 3083).		Data Collector Log	JOC (IL)
IL	15-May-03	20:40	As of 19:30, biological testing results are as follows per the Chicago HMRT and EPA: O'Hare - neg. for *yersinia Pestis* ; Union Station - neg. for *Yersinia Pestis* ; United Center - Positive for *Yersinia Pestis*.		Data Collector Log	JOC (IL)

	Integrated Acronym List
ABS	Arson Bomb Squad
AMS	Aerial Measuring System
ARAC	Atmospheric Release Advisory Capability
ASPA	Assistant Secretary, Public Affairs
ATF	[Bureau of] Alcohol, Tobacco, and Firearms
BC	Britisb Columbia [CAN]
BDC	Bomb Data Center
BICE	Bureau of Immigration and Customs Enforcement
BOLO	Be On Look Out
BOMA	Building Owner and Managers Association
Ca DTPA	[trisodium] Calcium Diethylenetriamine Pentaacetic Acid
CAT	Crisis Action Team
CBP	Customs and Border Patrol
CCC	Crisis Coordination Center
CCDPH	Cook County Department of Public Health
CCSEMA	Cook County Sherrif's Emergency Management Agency
CDC	Centers for Disease Control [and Prevention]
CDRG	Catastrophic Disaster Response Group
Ce	Cesium
CEPPO	Chemical Emergency Preparedness and Prevenion Office
CFD	Chicago Fire Department
CMC	Crisis Management Center
CMRT	Consequence Management Response Team
COOP	Continuity of Operations Plans
CPD	Chicago Police Department
CST	Civil Support Team
CTA	Chicago Transit Authority
DC	District of Columbia
DEST	Domestic Emergency Support Team
DHS	Department of Homeland Security
DMAT	Disaster Medical Assistance Team
DMAT	Disaster Medical Assistance Team
DMORT	Disaster MORtuary Team
DOH	Department of Health
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DPH	Department of Public Health
DPMU	Disaster Portable Morgue Unit
DTPA	Diethylenetriamine Pentaacetic Acid
EDP	Emergency Disaster Plan
EIS	Epidemic Intelligence Service
EMD	Emergency Management Division
EMNET	Emergency Network
EMSHG	Emergency Management Strategic Health Care Group
EOC	Emergency Operations Center
EPA	Environmental Protection Agency

ERT	Evidence Response Team
ESF	Emergency Support Function
ESF-10	ESF Hazardous Materiel
ESF-8	Emergency Support Function 8 (Health and Medical Services)
ESF-9	Emergency Support Function 9 (Urban Search and Rescue)
EST	Emergency Support Team
EST	Emergency Support Team
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCO	Federal Coordinating Officer
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FHWA	Federal HighWay Administration
FPS	Federal Protective Service
FRA	Federal Railroad Administration
FRMAC	Federal Radiological Management Center
FTA	Fedearl Transit Administration
GLODO	Group for the Liberation of Orangeland and the Destruction of Others
Gm	Gram
GSA	General Services Administration
HAN	Health Alert Network
HAZMAT	Hazardous Materials
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HMRT	Hazardous Materials Response Team
HMRU	Hazardous Materials Response Unit
HMRU	Hazardous Materials Response Unit
HMRU	Hazardous Materials Response Unit
HQ	Headquarters
HRT	Hostage Rescue Team
HSAS	Homeland Security Advisory System
HSAS	Homeland Security Alert Status
HVAC	High Volume Air Conditioning
IC	Incident Command(er)
ICE	Immigration and Customs Enforcement
ICP	Incident Command Post
ICS	Incident Command System
IDPH	Illinois Department of Public Health
IEMA	Illinois Emergency Management Agency
IL SEOC	Illinois State Emergency Operations Center
IMERT	Illinois Medical Emergency Team
IMSURT	International Medical SURgical Response Team
IOF	Interim Operating Facility
IOHNO	Illinois Operational Headquarters and Notification Office
ISP	Illinois State Police
JIC	Joint Information Center
JOC	Joint Operations Center
JTF	Joint Task Force

LQRAM	Large Quantity RadioActive Material
MARSEC	Maritime Security
MCC	Master Control Cell
MCI	Mass Casualty Incident
MERRT	Medical Emergency Radiological Response Team (Veterans Affairs)
METRA	Metropolitan Rail Agency
MRV	Mobile Response Vehicle
MSEL	Master Scenario Event List
MST	Management Support Team
NAWAS	NAtional WArning System
NCEH	National Center for Environmental Hazards
NCID	National Center for Infectious Diseases
NDMS	National Disaster Medical System
NJTTF	National Joint Terrorism Task Force
NMRT	National Medical Response Team
NMRT	National Medical Response Team
NNSA	National Nuclear Security Administration
NPP	Nuclear Power Plant
NPS	National Pharmaceutical Stockpile
NRC	Nuclear Regulatory Commission
NRT	National Response Team
OEM	Office of Emergency Management
OEMC	Office of Emergency Management Communications
ONCRC	Office of National Capitol Region Coordination
OSC	On-Scene Coordinator
OSHA	Occupational Safety and Health Administration
OSLGC	Office of State and Local Government Coordination (DHS)
PAT	Preliminary Assessment Team
PCR	Polymerase Chain Reaction
PFO	Principle Federal Official
PHSKC	Public Health-Seattle & King County
PIO	Public Information Officer
PPE	Personal Protective Equipment
Pu	Plutonium
RAP	Radiological Assistance Program
RAP[T]	Radiological Assistance Program [Team]
RDD	Radioloigical Dispersion Device
RDD	Radiological Dispersal Device
REAC	Radiological Emergency Assistance Center
REOC	Regional Emergency Operations Center
RHA	Regional Health Administrator
ROC	Regional Operations Center
RSAN	Roam Secure Alert Network
RTA	Regional Transportation Authority
S-60	DOT Office of Intelligence and Security
SABT	Special Agent Bomb Technician
SAC	Special Agent in Charge
SCC	Secretary's Command Center

SEATAC	Seattle-Tacoma [Airport]
SEOC	State Emergency Operations Center
SERT	[HHS] Secretary's Emergency Response Team
SFD	Seattle Fire Department
SHL	State Health Liaison
SIOC	Strategic Information Operations Center
SME	Subject Matter Experts
SNS	Strategic National Stockpile
SODO	South Of DOwntown [Seattle]
SPD	Seattle Police Department
SPU	Seattle Public Utilities
STB	Surface Transportation Board
SWAT	Special Weapons And Tactics
SWMDT	State Weapons of Mass Destruction Team
TFR	Temporary Flight Restriction
TOPS	TOPOFF Pulmonary Syndrome
TRT	Tactical Response Team
TSA	Transportation Security Administration
UC	Unified Command
UCS	Unified Command System
US&R	Urban Search and Rescue
USAR	Urban Search and Rescue
USMS	United States Marshal Service
USSS	United States Secret Service
VACO	Veterens Affairs Central Office
VCC	Venue Control Cell
VMI	Vendor Managed Inventory
VNN	Virtual News Network
WA	Washington [State]
WH	White House
WMD	Weapons of Mass Destruction
Zn DTPA	[trisodium] Zinc Diethylenetriamine Pentaacetic Acid

	Washington Acyonyms
ABS	Arson Bomb Squad
DEST	Domestic Emergency Support Team
DMAT	Disaster Medical Assistance Team
DOH	Department of Health
EMD	Emergency Management Division
EOC	Emergency Operations Center
ERT	Evidence Response Team
ESF	Emergency Support Function
EST	Emergency Support Team
FEMA	Federal Emergency Management Agency
HAZMAT	Hazardous Materials
HMRT	Hazardous Materials Response Team
HMRU	Hazardous Materials Response Unit
IC	Incident Command(er)
ICS	Incident Command System
IOF	Interim Operating Facility
JOC	Joint Operations Center
MARSEC	Marine Security
MCI	Mass Casualty Incident
MSEL	Master Scenario Event List
NJTTF	National Joint Terrorism Task Force
NMRT	National Medical Response Team
PHSKC	Public Health-Seattle & King County
PIO	Public Information Officer
RAP	Radiological Assistance Program
RDD	Radioloigical Dispersion Device
ROC	Regional Operations Center
SABT	Special Agent Bomb Technician
SEOC	State Emergency Operations Center
SEOC	Seattle Emergency Operations Center
SFD	Seattle Fire Department
SHL	State Health Liaison
SIOC	Strategic Information Operations Center
SODO	South of Downtown
SPD	Seattle Police Department
SPU	Seattle Public Utilities
TFR	Temporary Flight Restriction
TSA	Transportation Security Administration
UC	Unified Command
UCS	Unified Command System
USAR	Urban Search and Rescue
VCC	Venue Control Cell
VNN	Virtual News Network

	Interagency Acronyms
ASPA	Assistant Secretary, Public Affairs
AMS	Aerial Measuring System
ARAC	Atmospheric Release Advisory Capability
ATF	[Bureau of] Alcohol, Tobacco, and Firearms
BC	British Columbia [CAN]
BDC	Bomb Data Center
BICE	Bureau of Immigration and Customs Enforcement
BOLO	Be On Look Out
Ca DTPA	[trisodium] Calcium Diethylenetriamine Pentaacetic Acid
CAT	Crisis Action Team
CBP	Customs and Border Patrol
CCC	Crisis Coordination Center
CDC	Centers for Disease Control [and Prevention]
CDRG	Catastrophic Disaster Response Group
Ce	Cesium
CEPPO	Chemical Emergency Preparedness and Prevenion Office
CMC	Crisis Management Center
CMRT	Consequence Management Response Team
COOP	Continuity of Operations Plans
DC	District of Columbia
DEST	Domestic Emergency Support Team
DHS	Department of Homeland Security
DMAT	Disaster Medical Assistance Team
DMORT	Disaster MORtuary Team
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DPMU	Disaster Portable Morgue Unit
DTPA	Diethylenetriamine Pentaacetic Acid
EMSHG	Emergency Management Strategic Health Care Group
EOC	Emergency Operations Center
EPA	Environmental Protection Agency
ERT	Emergency Reponse Team
ERT	Evidence Response Team
ESF	Emergency Support Function
ESF-10	ESF Hazardous Materiel
ESF-8	Emergency Support Function 8 (Health and Medical Services)
ESF-9	Emergency Support Function 9 (Urban Search and Rescue)
EST	Emergency Support Team
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCO	Federal Coordinating Officer
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FHWA	Federal HighWay Administration
FPS	Federal Protective Service
FRA	Federal Railroad Administration
FRMAC	Federal Radiological Management Center

FTA	Fedearl Transit Administration
GLODO	Group for the Liberation of Orangeland and the Destruction of Others
GSA	General Services Administration
HAN	Health Alert Network
HHS	Health and Human Services
HMRU	Hazardous Materials Response Unit
HQ	Headquarters
HRT	Hostage Rescue Team
HSAS	Homeland Security Advisory System
ICE	Immigration and Customs Enforcement
IMSURT	International Medical SURgical Response Team
JIC	Joint Information Center
JOC	Joint Operations Center
JTF	Joint Task Force
LQRAM	Large Quantity RadioActive Material
MARSEC	Maritime Security
MCC	Master Control Cell
MCCUE	Master Control Cell Un-Evaluator
MERRT	Medical Emergency Radiological Response Team (Veterans Affairs)
MRV	Mobile Response Vehicle
MST	Management Support Team
NAWAS	NAtional WArning System
NCEH	National Center for Environmental Hazards
NCID	National Center for Infectious Diseases
NCID	National Center for Infectious Diseases
NDMS	National Disaster Medical System
NMRT	National Medical Response Team
NNSA	National Nuclear Security Administration
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NRT	National Response Team
ONCRC	Office of National Capitol Region Coordination
OSC	On-Scene Coordinator
OSHA	Occupational Safety and Health Administration
OSLGC	Office of State and Local Government Coordination (DHS)
PAT	Preliminary Assessment Team
PFO	Principle Federal Official
PPE	Personal Protective Equipment
Pu	Plutonium
RAP[T]	Radiological Assistance Program [Team]
RDD	Radiological Dispersal Device
REAC	Radiological Emergency Assistance Center
REOC	Regional Emergency Operations Center
RHA	Regional Health Administrator
ROC	Regional Operations Center
RSAN	Roam Secure Alert Network
S-60	DOT Office of Intelligence and Security
SAC	Special Agent in Charge
SCC	Secretary's Command Center

SEATAC	Seattle-Tacoma [Airport]
SERT	[HHS] Secretary's Emergency Response Team
SIOC	Strategic Information Operations Center
SME	Subject Matter Experts
SNS	Strategic National Stockpile
SODO	South Of DOwntown [Seattle]
STB	Surface Transportation Board
SWAT	Special Weapons And Tactics
TFR	Temporary Flight Restriction
TSA	Transportation Security Administration
US&R	Urban Search and Rescue
USMS	United States Marshal Service
USSS	United States Secret Service
VACO	Veterens Affairs Central Office
VCC	Venue Control Cell
VNN	Virtual News Network
WA	Washington [State]
WH	White House
WMD	Weapons of Mass Destruction
Zn DTPA	[trisodium] Zinc Diethylenetriamine Pentaacetic Acid

	Illinois Acronyms
BOMA	Building Owner and Managers Association
CCDPH	Cook County Department of Public Health
CCSEMA	Cook County Sherrif's Emergency Management Agency
CFD	Chicago Fire Department
CPD	Chicago Police Department
CST	Civil Support Team
CTA	Chicago Transit Authority
DHS	Department of Homeland Security
DMAT	Disaster Medical Assistance Team
DPH	Department of Public Health
EDP	Emergency Disaster Plan
EIS	Epidemic Intelligence Service
EMNET	Emergency Network
EPA	Environmental Protection Agency
GLODO	Group for the Liberation of Orangelandia and the Destruction of Others
Gm	Gram
HAN	Health Alert Network
HazMat	Hazardous Materials
HIPAA	Health Insurance Portability and Accountability Act
HMRT	Hazardous Materials Response Team
HMRU	Hazardous Materials Response Unit
HSAS	Homeland Security Alert Status
HVAC	High Volume Air Conditioning
ICP	Incident Command Post
IDPH	Illinois Department of Public Health
IEMA	Illinois Emergency Management Agency
IL SEOC	Illinois State Emergency Operations Center
IMERT	Illinois Medical Emergency Team
IOHNO	Illinois Operational Headquarters and Notification Office
ISP	Illinois State Police
JOC	Joint Operations Center
METRA	Metropolitan Rail Agency
NDMS	National Disaster Medical System
NPS	National Pharmaceutical Stockpile
OEM	Office of Emergency Management
OEM	Office of Emergency Management
OEMC	Office of Emergency Management Communications
PCR	Polymerase Chain Reaction
PIO	Public Information Officer
PPE	Personal Protective Equipment
RTA	Regional Transportation Authority
SNS	Strategic National Stockpile
SWMDT	State Weapons of Mass Destruction Team
TOPS	TOPOFF Pulmonary Syndrome
TRT	Tactical Response Team
VMI	Vendor Managed Inventory
VNN	Virtual News Network

TOP OFFICIALS (TOPOFF) EXERCISE SERIES:

TOPOFF 2 (T2)
After Action Report
ANNEX B

September 30, 2003

This page intentionally left

TOP OFFICIALS (TOPOFF) EXERCISE SERIES:

TOPOFF 2 (T2) After Action Report ANNEX C

September 30, 2003

This page intentionally left

WASHINGTON, DC | MARYLAND | VIRGINIA

ODP
Office for Domestic Preparedness

DRAFT

NATIONAL CAPITAL REGION FUNCTIONAL EXERCISE

AFTER-ACTION REPORT
MAY 12, 2003

This project was supported by the U.S. Department of Homeland Security (USDHS) Office for Domestic Preparedness (ODP). Points of view presented in this document are those of the authors and do not necessarily represent the official position of ODP.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND – THE FACE OF TERRORISM

September 11, 2001, stands as a day that forever changed the way Americans view terrorism. The magnitude of the events shattered many long-held beliefs regarding the types of terrorist attacks the Nation might face, and has effectively shattered the image of "Fortress America" for many citizens. As former Senator Sam Nunn wrote shortly after the tragedy, "The terrorists who carried out the attack of September 11 showed there is no limit to the number of innocent lives they are willing to take. Their capacity for killing was restricted only by the power of their weapons."

As the Nation worked to recover from the attacks on the World Trade Center, on the Pentagon, and in western Pennsylvania, this statement proved to be prophetic, as cases of anthrax exposure began to appear around the country. Cases first appeared in Florida, then New York and Washington, DC, and then in various locations across the country. Although no one has claimed responsibility for the release of anthrax, the country remains on an overall higher state of alert. Security at buildings, airports, and other facilities has increased, and government officials warn of the danger of further attacks on the Nation.

Many speak of a "new framework for national security" in which the fight against terrorism will take prominence. As President Bush stated on the first weekend after the attacks, "We haven't seen this kind of barbarism in a long period of time. No one could have conceivably imagined suicide bombers burrowing into our society and then emerging all in the same day to fly … U.S. aircraft into buildings full of innocent people…and show no remorse. This is a new kind … of evil. And we understand. And the American people are beginning to understand. This crusade, this war on terrorism is going to take a while. And the American people must be patient." As the war on terrorism continues to take shape, the world remains anxious that the next outbreak of violence could come from any direction, at any time.

As the country responds to and recovers from these attacks, citizens turn to political leaders with one question: "What will be next?" As the latest operations in the war against terrorism begin, the Nation's leaders have reiterated the need for preparedness against all kinds of threats. Long-held taboos have been broken, and today's terrorist has the potential to be far more deadly than ever before. The tools of the terrorist have evolved from pipe bombs and guns to massive ammonium nitrate bombs, the use of airliners as flying bombs, and the dissemination of anthrax.

Extremist and absolutist ideologies allow perpetrators to take extraordinary measures in support of their goals. At the forefront of this in the international arena is al Qaeda, a group of Islamic militants led by Osama bin Laden. Having claimed credit for the September 11 attacks, bin Laden declared that more will occur. In recent years, he has stated that acquiring weapons of mass destruction (WMD) was a goal of his group. As President Bush said in November 2001, "These terrorist groups seek to destabilize entire nations and regions. They are seeking

chemical, biological, and nuclear weapons. Given the means, our enemies would be a threat to every nation and, eventually, to civilization itself."

Because of this, the use of WMD by terrorists has received even greater prominence in the United States as a major national security concern. As Senator Nunn wrote, "We have had a look at the face of terrorist warfare in the 21st century, and it gives us little hope that if these groups gained control of nuclear, biological, and chemical weapons they would hesitate to use them."

In March 2002, the Office of Homeland Security (OHS) developed a national alert system that responds to concerns about terrorist attacks. This system disseminates information regarding the risk of terrorist attacks to all levels of government and the American people. There are five color-coded threat levels associated with the level of risk of terrorist attacks and what protective measures should be taken.

When confronted with the question of "What will be next?" leaders cannot say for sure. However, they reiterate that we as a Nation will be committed for the long term, that we must steel our resolve, and that we must endeavor to ensure that our communities are as prepared as possible to respond to any future attacks.

With that resolve in mind, The Homeland Security Act of 2002 was signed into law thus changing the OHS and creating the U.S. Department of Homeland Security (USDHS) which became operational on March 1, 2003.

EXECUTIVE SUMMARY

The National Capital Region Functional Exercise (NCRFE) was conducted on May 12, 2003, in the National Capital Region (NCR). This included the Federal Emergency Management Agency Headquarters (FEMA HQ) in Washington, DC; The District of Columbia Emergency Management Agency Emergency Operations Center (DC EMA EOC) in Washington, DC; the Federal Bureau of Investigation Washington Field Office (FBI WFO) in Washington, DC; the Virginia Department of Emergency Management Emergency Operations Center (VDEM EOC) in Richmond, VA; and the Maryland Emergency Management Agency Emergency Operations Center (MEMA EOC) in Reisterstown, MD, and the U.S. Department of Homeland Security (USDHS), Office of the National Capital Region Coordinator (ONCRC) in Washington, DC. The exercise was conducted under the aegis of the USDHS, Office for Domestic Preparedness (ODP), in cooperation with the NCR. The NCRFE was designed to coincide with the TOPOFF2 (T2) full-scale exercise in order to assist the NCR jurisdictions in assessing their preparedness and coordination in response to a general attack on the Nation and changes to the Homeland Security Advisory System threat level. The T2 scenario involved a radiological dispersal device (RDD) explosion in Seattle, WA. The NCRFE was a no-fault, functional communications response to the weapons of mass destruction (WMD) terrorism event in Seattle, WA, as well as a simulated but credible threat to the National Capital Region. The NCRFE was designed by the Community Research Associates (CRA) USDHS Exercise Support Team.

The NCRFE scenario incorporated two events: a credible threat of a terrorist event directed at five U.S. cities and a radiological dispersal device (RDD) explosion in Seattle, WA. The exercise included two modules. In Module One (which was simulated as six days earlier, May 6, 2003), the Homeland Security Advisory System (HSAS) national threat level was raised from Yellow to Orange. In Module Two, an RDD exploded in Seattle, with a subsequent change in threat level from Orange to Red. This functional exercise scenario allowed the jurisdictions to assess their overall communication and coordination within the National Capital Region.

One of the exercise's main objectives was to assess the relationship among all jurisdictions within the National Capital Region. Information-sharing and coordination proved to be extremely important in mitigating a terrorist event in the NCR. The DC EOC seemed to be controlling most of the flow of information to Maryland and Virginia. MEMA EOC representatives felt that other than a conference call, they were pulling information from the other jurisdictions, rather than having the information being pushed to them. Also, it was noted that it would have been beneficial to have representatives from FEMA, VA, and MD in the DC EOC during the exercise to further enhance the jurisdictions' relationships.

Technical communications issues within each EOC proved to be an exercise obstacle but all jurisdictions were able to properly communicate with each other. FEMA HQ had issues with videoconferencing, although they noted that in a real-world setting, they would have had the Information Technology (IT) support they needed. The DC EOC had some technical problems with their internal E-Team software that supported their EOC tracking system. At VDEM EOC, sufficient security clearances were not available for the use of the secure video teleconferencing (VTC) system. Changes in homeland security require that a National Guard representative be present at all times that secure VTC equipment is being used.

Overall, the exercise was very successful. DC EOC felt that they had good control of the situation, and that they were disseminating information efficiently. MEMA EOC felt that all of their objectives were met, but that exercise information should have been disseminated more often (from the DC EOC). VDEM EOC needs more funding in order to participate more effectively in exercises. FEMA was very effective throughout the exercise in their role as the coordinator of Federal assets. USDHS's new role of providing policy guidance and coordination for the NCR was accomplished without any problems. The only major question that was not addressed during this exercise was how well the communications network connection would work between the Federal agencies' emergency relocation sites.

EXERCISE DESIGN

PURPOSE

The National Capital Region Functional Exercise (NCRFE) was designed to coincide with the TOPOFF 2 (T2) full-scale exercise (FSE) in order to assist National Capital Region (NCR) jurisdictions in assessing their preparedness and coordination in response to a general attack on the Nation and changes to the Homeland Security Advisory System (HSAS) threat level.

SCOPE

The NCRFE was conducted on May 12, 2003, at various locations within the NCR, including the District of Columbia Emergency Operations Center (DC EOC), the State of Maryland EOC, the Commonwealth of Virginia EOC, the Federal Bureau of Investigation (FBI) Washington Field Office (WFO), the Federal Emergency Management Agency Headquarters (FEMA HQ) at 500 C. Street, and the Office of the National Capital Region Coordinator, U.S. Department of Homeland Security (ONCRC, USDHS). Approximately 100 individuals participated in the exercise.

FOCUS

The NCRFE events focused on the following activities:

- Observe or exercise NCR coordination functions.
- Observe use of physical communications facilities.
- Reinforce established policies and procedures.
- Measure resource adequacy.
- Assess inter-jurisdictional relations.

The NCRFE was played in real time. However, some responses and actions required additional time or accelerated time in order to meet exercise objectives.

STRUCTURE

The NCRFE examined the connectivity, in a free-play environment, of various NCR agencies as they related to the exercise scenario. The NCR agencies that were represented are:

- Virginia Department of Emergency Management
- Federal Emergency Management Agency
- District of Columbia Emergency Management Agency
- Federal Bureau of Investigation—Washington Field Office
- Maryland Emergency Management Agency
- Office of the National Capital Region Coordinator, U. S. Department of Homeland Security

The NCRFE was designed as a 4–6 hour, multi-jurisdictional, weapons of mass destruction (WMD) functional exercise, held on May 12, 2003, in the NCR. It was conducted in conjunction with, but separate from, the T2 national WMD FSE. The NCRFE used and followed the T2 scenario and background material to drive the exercise play.

The NCRFE was designed to exercise individual capabilities, multiple functions, activities within a function, or interdependent groups of functions. It was generally focused on exercising the plans, policies, procedures, and staffs of the managerial or direction and control nodes of each jurisdiction's emergency management agency. Generally, the use of response resources was simulated, and events were projected through an exercise scenario and event updates to stress or drive activity at the management level.

MATERIALS

A comprehensive set of exercise materials was developed, including an Exercise Plan (EXPLAN), Controller/Evaluator (C/E) Handbooks, a Master Scenario Events List (MSEL), and identification badges and hats.

Each controller/evaluator involved in the execution of the exercise received a briefing prior to the exercise that described their duties and responsibilities in depth. They were provided with a C/E Handbook with detailed instructions about the exercise and the scenario, as well as their roles and responsibilities. Evaluation forms for each controller and evaluator were also provided. An EXPLAN was distributed that contained general information regarding basic issues, such as the purpose of the exercise and rules of conduct.

GUIDELINES

- The exercise was not a test, but rather a no-fault learning experience.
- The exercise was intended to be in an open, low-stress environment.
- This exercise served as a realistic setting within which participants were given the opportunity to implement previously identified adjustments in standard operating policies and procedures.
- Responses were based on current capabilities (i.e., only existing abilities and assets).

EXERCISE ASSUMPTIONS AND ARTIFICIALITIES

A number of assumptions and artificialities were necessary to complete the exercise within the time allotted.

Assumptions

The following general assumptions applied to the NCRFE:

- The goals and objectives of the exercise were consistent with functional area operations, technical plans, and procedures, whenever possible.

- NCR agencies, along with the USDHS Office for Domestic Preparedness (ODP) and/or its contractor (Community Research Associates [CRA]), were major participants and/or had significant roles in coordinating the exercise.

Artificialities and Constraints

Although there were a number of artificialities and constraints that may have detracted from exercise realism, the NCRFE planners and participants recognized and accepted that some artificialities and simulations were necessary to carry out the exercise.

SCENARIO

Several variables were selected by the NCRFE planners and used in the development of the scenario and overall structuring of the exercise:

- The NCRFE was connected with the T2 FSE, but was played separately.

- Background intelligence events in Module One triggered a change in the HSAS national threat level from Yellow to Orange.

- A WMD event involving an RDD in Seattle, WA, in Module Two triggered a change in the HSAS national threat level from Orange to Red.

Module One. Module One was played as if it were May 6, 2003, and used the T2 background information that built up a credible terrorism threat against five major U.S. cities, triggering an HSAS threat level change from Yellow to Orange.

Module Two. Module Two was played in real time on May 12, 2003, and focused on an RDD attack in Seattle, WA, and the subsequent HSAS threat level change from Orange to Red.

EXERCISE OBJECTIVES

NCRFE was designed to assist Federal, State, and local agencies located in the NCR in coordinating a response to changes in the national threat level, as a potential but credible region-wide threat of WMD terrorism evolves. Seven specific objectives for the exercise are listed below with comments:

1. **Objective:** Identify and exercise communication capabilities (voice, fax, data, and video) among NCR jurisdictions.

   Discussion: This major objective was clearly met during the planning and execution phase of the exercise. Voice, fax, and data connectivity worked fine among all of the players. However, technical communication issues within each EOC proved to be an obstacle. A video connection among all NCR jurisdictions is needed; not all jurisdictions had the proper equipment to have a video conference meeting.

   Recommendation: Each NCR jurisdiction needs to have its communications divisions review the requirements for full video conferences and establish the budget to gain the equipment and capability.

2. **Objective: Review information-sharing capabilities among NCR jurisdictions.**

   Discussion: This objective was met by each player jurisdiction. During the course of the short exercise, information was passed among the organizations via voice, fax, and computer systems. Had the exercise lasted longer, the information-sharing capabilities would have continued to improve.

   Recommendation: The NCR jurisdictions should continue to exercise their communications capabilities among the organizations on a day-to-day basis to ensure that each system works and that there is a continuing flow of information that is second nature to all involved in this process. This objective should be first and foremost in all future NCR exercises.

3. **Objective:** Develop and coordinate consistent public information strategies.

   Discussion: This objective was addressed very carefully by each jurisdiction's public affairs officer (PAO) before and during the exercise. Each PAO connected with his or her counterpart, and opened all channels of communication to ensure that the public information strategies were properly coordinated. Again, in a longer exercise, this function would have been exercised in depth.

   Recommendation: The PAOs of each NCR jurisdiction should maintain contact with each other on a regular basis in order to keep the lines of communication open year-round.

4. **Objective:** Review connectivity within and among NCR agencies in accordance with USDHS procedures.

   Discussion: Early in the exercise, all of the player NCR agencies made voice, fax, and data connections with their counterparts at all levels (policymakers and staff). Several telephone conference calls were made among the NCR agencies, but the use of radios and video conferencing was not tested. It should be noted that because of the short length of time for this exercise (and the scope of the scenario), the FEMA Interim Operating Facility (IOF) and the USDHS operations center were not used or tested in this exercise.

   Recommendation: The NCR should schedule a longer and more extensive NCR WMD response exercise in the near future, which will force the testing of all NCR emergency operations facilities (and communications) at the Federal, State, and local levels within the NCR.

5. **Objective:** Coordinate the decision-making processes of all three jurisdictions with FEMA and the FBI.

   Discussion: The decision-making processes of all three major NCR jurisdictions were completely coordinated with FEMA, the FBI, and USDHS. Each agency was connected to several senior-level conference calls, which ensured that the decision-making process was properly coordinated.

   Recommendation: The major NCR jurisdictions should ensure that the senior policy council members continue to meet on a regular basis, and hold at least one general teleconference each month to discuss a major policy issue.

6. **Objective:** Review 7 of the NCR's "8 Commitments to Action":

   Terrorism Prevention
   Citizen Involvement in Preparedness
   Decision Making and Coordination
   Emergency Protective Measures
   Infrastructure Protection
   Media Relations and Communication
   Mutual Aid

   Discussion: All of the Commitments to Action listed above received at least a review of required actions by each major jurisdiction during this exercise. The stated goal of the exercise was to follow the elevated threat level recommendations of USDHS (based on the T2 threat scenario), and review the coordinated actions that need to be taken in the NCR for these areas of concern. Each jurisdiction understood many of the required actions, but because of the short length of the exercise, it was impossible to completely test each of these rather complex subjects.

Recommendation: The NCR should take at least three months to plan a longer and more specific exercise that will allow a thorough testing of each of these important aspects of a coordinated response to a terrorist WMD attack on the region. This type of exercise should run about 8 to 12 hours in length.

7. **Objective:** Improve the NCR's readiness to respond to any possible act of terrorism.

   Discussion: Every practice exercise that can be conducted before a real event occurs improves the readiness of an organization, agency, government, or region to respond to a real incident. This exercise was the first step in that readiness improvement process for the NCR region. Most State-level governments and military organizations believe that daily and weekly individual/small organizational training, followed by quarterly or biannual large organization training or exercising, is the proper way to prepare an organization or agency for the real event. The NCR jurisdictions should do no less.

   Recommendation: The NCR Senior Policy Council staff should prepare a three-year, region-wide exercise plan and schedule that can be funded and followed to improve the NCR jurisdictions' preparations for a terrorist WMD attack on the region. Most experts in this field truly believe that it is not a matter of "if" but "when" an attack will occur on the very high-profile District of Columbia and consequently the NCR.

SIGNIFICANT FINDINGS

COORDINATION AND COMMUNICATION AMONG JURISDICTIONS

Before the NCRFE took place, a major concern was the communication and coordination among all NCR jurisdictions (MD, VA, DC, FEMA, USDHS-NCR) in a terrorist event. Although the NCR was not an imminent target for a terrorist event in the exercise, it was understood that being in or near the Nation's capital, as well as having a credible threat to five U.S. cities, required proper action (i.e., communication and coordination among all jurisdictions) in order to protect its citizens. Since the NCR comprises several jurisdictions, it was imperative to assess and enhance their communication and coordination effectiveness during a terrorist event.

- It seemed that the District of Columbia Emergency Management Agency (DC EMA) was controlling most of the flow of information to the other States (MD and VA).

- The Maryland Emergency Management Agency (MEMA) had the most difficulty with communication and information sharing during the exercise. Conference calls were established that included FEMA, USDHS, MD, VA, and DC. It seemed that there was little independent information sharing that took place outside of the conference call format. At no time outside of the prearranged conference calls was DC or VA queried as to how they were handling these issues of concern.

- Representatives from FEMA, VA, and MD were not present in the DC EOC during the exercise. It was stated, however, that in a real-world setting, representatives would be present.

TECHNICAL ISSUES

There were a number of technical issues in each EOC that appeared to hinder the ability of the exercise participants to play efficiently.

- At FEMA HQ, video conferencing was inaccessible during the exercise due to technical problems.

- At DC EOC, computer printers were overloaded; exercise participants were kept waiting for their printed material. The location of the printers also obstructed the view of the Operations Chief. The location of the printers also made it difficult for the participants to move freely throughout the DC EOC to gather information.

- The DC EOC also had difficulties with the new E-Team Software, although Information Technology (IT) representatives were present to help with any problems that participants encountered (such as with training).

- At VDEM EOC, sufficient security clearances were not available for the use of the video teleconferencing system. Changes in Homeland Security policy required that a National Guard representative be present at the VDEM EOC each time that secure VTC equipment is being used.

It is understood that technical issues are ubiquitous and difficult to avoid, and during a real-world situation, things would have gone differently. However, it should be stated that IT support should be available and proper clearances ensured, in order to enhance communication among jurisdictions. Coordination and communication were exercised well, and all participating agencies understood that they could be improved.

CHANGE IN HSAS THREAT LEVEL

The HSAS threat level change is a recommendation for each State. Following the HSAS threat level change from Orange to Red after the event in Seattle, questions arose in MEMA and VDEM regarding whether it was necessary to change the threat level throughout their entire State(s).

- Following the terrorist event in Seattle and subsequent change in threat level from Orange to Red, FEMA immediately responded by activating and dispatching the NCR ERT-N to an emergency relocation site in Maryland, and was kept apprised of all actions thereafter.

- VA controllers noted that VDEM EOC staff verbally questioned whether the entire State should be elevated to threat level Red.

- MD controllers had a lengthy discussion regarding whether the entire State of Maryland should elevate the threat level to Red, or just raise the level within selected vulnerable jurisdictions. MD controllers also noted that the MD decisionmakers recognized distinct liability issues associated with this decision.

ISSUES AND RECOMMENDATIONS

VIRGINIA DEPARTMENT OF EMERGENCY MANAGEMENT
EMERGENCY OPERATIONS CENTER
RICHMOND, VA

General Statement

The initial information and injects were handled well by the EOC staff. Appropriate notifications to State agencies and the Governor's Office and external notifications by fax and the VDEM EOC web site were made. All State agencies were notified within ten minutes of the beginning of the exercise.

The State Police complex that houses the EOC was locked down, one point of entry was established, and mandatory ID use was instituted. The EOC paged the Commonwealth Preparedness Working Group (CPWG) for a conference call, which took place at 1:32 p.m. The CPWG conducted a well-organized conference call with State agencies, and used a checklist for those agencies that were identified to participate in the call. A status review by each agency director was given, as well as the current condition of the EOC.

As exercise play continued in the NCR, FEMA began notifying area representatives. Ms. Cindy Causey, the VDEM NCR field representative, was notified of the incident by FEMA directly on her cell phone. No additional notifications were made to the VDEM EOC. Dual notification should be done by FEMA, however, to ensure that the appropriate agency representative is notified.

During the exercise, it was requested that a video conference call be held among the VA, MD, and DC EOCs. The Virginia EOC cannot open a secure VTC until a National Guard representative is present. The VDEM EOC staff is still undergoing new security clearance investigations.

During exercise play, the VDEM EOC communications center underwent a scheduled dispatcher shift change. Shift change briefings were conducted and there were no noted problems.

All tasks and requests presented to VDEM EOC staff were handled in a timely and appropriate manner. Coordination on the State level was excellent. Policies and procedures are in place that identify tasks associated with an EOC standup, State coordination aetivities, and regional coordination activities.

Overall, the VDEM EOC handled the scenario extremely well.

Specific issues identified at the VDEM EOC:

- FEMA notification to VDEM NCR representative
- VDEM EOC secure video communications
- EOC facilities

Issue: FEMA Notification to VDEM NCR Representative

Observation: During the exercise, FEMA placed a cell phone call directly to Cindy Causey, the VDEM NCR field representative. Although this call was handled appropriately and showed the local coordination between VDEM and FEMA, if Ms. Causey had not been available or if her phone had been out of a service area, no one at VDEM would have been notified.

Recommendation: VDEM EOC should develop a policy that provides all agencies with the central communications phone number for all emergency-related issues. This will funnel all communications directly to the EOC, who can then pass that information on to the appropriate person.

Issue: VDEM EOC Secure Video Communications

Observation: VDEM EOC has the capability and equipment to use a secure video teleconferencing system. Because of changes in Homeland Security policy, existing security clearances of the staff were removed and new clearances are still being investigated. Consequently, a National Guard representative must be present at the VDEM EOC each time that secure VTC equipment is being used.

Recommendation: Security clearances should be expedited to allow the immediate use of secure VTC equipment.

Issue: EOC Facilities

Observation: As a key member of the NCR, Virginia is home to many critical Federal facilities, such as the Pentagon. In this new day of heightened security, and the need to handle complicated and specialized emergency coordination activities, the VDEM EOC is a small and outdated facility. Satellite video downlink capability was not available during the NCR functional exercise.

Recommendation: Although engineering drawings are available to demonstrate the potential of a new VDEM EOC, there is currently no funding for construction. Construction should be a priority, however, and the availability of Federal funds should be investigated.

FEDERAL EMERGENCY MANAGEMENT AGENCY
HEADQUARTERS
WASHINGTON, DC

General Statement

The NCRFE was designed to allow the principal jurisdictions of the NCR (DC, VA, and MD) to exercise their communications and decision-making coordination during an elevated threat of terrorism that uses WMD in or near the NCR. This process had to be tied into and coordinated with the actions of key elements of the Federal Government, or in this case, the FBI, FEMA, and USDHS.

The major issue facing the entire exercise was: Could these major jurisdictions communicate and coordinate what they were doing to protect their citizens, infrastructure, and communities with each other and the Federal Government in an effective manner? Traditionally, FEMA, the FBI, and the governments of the three major jurisdictions (VA, MD, and DC) have learned to communicate and coordinate through their emergency management agencies during times of crisis response to disaster-related problems. This has resulted in a foundation upon which the current process is being built. USDHS is the only new player in this process, and is quickly integrating its organization into the control of the response system. The NCRFE showed that this system will work and that the major objectives were met (as well as possible in a four- to five-hour functional or command post exercise).

The individuals representing FEMA during NCRFE did a superb job. The Federal Coordinating Officer (FCO) (Mr. Davies) was acutely aware of FEMA's roles and responsibilities and was not afraid to make recommendations and decisions when called for by the exercise scenario. He and his team analyzed the information as it was received, decided on what course of action was indicated and prudent, and then either implemented it or recommended to his superiors that it be implemented. The communication and coordination among FEMA, USDHS, and the NCR EOCs was outstanding.

Specific issues identified at FEMA:

- Location of NCR crisis management staffs
- Relationship between USDHS and FEMA during this type of crisis management
- Change in threat level from yellow to orange
- Coordination and information sharing within the NCR
- Press inquires to FEMA
- Fax directing that all States be informed of the threat level change and specific actions
- Post-Seattle blast actions

- Virtual News Network (VNN) broadcasts
- Actions taken after RDD was confirmed in Seattle, and change in threat level from orange to red
- Video conference

Issue: Location of NCR Crisis Management Staffs

Observation: Although FEMA has an Interim Operating Facility (IOF) located near the NCR (that is in effect a Federal EOC that is designed to give the Federal Government a location from which to operate and communicate during an emergency), it was not used for this exercise. FEMA and USDHS were correct in believing that the NCR was reacting to a scenario that presented a "credible threat" to the area, although the actual attack was on another part of the country. Both elements of the government would have been operating (at least during this exercise) from their regular offices.

Recommendation: During future NCR exercises, the Federal Government should exercise the IOF so that DC, VA, and MD can gauge any problems they may have in dealing with that specific location (concerning communications, etc). If the IOF had been used for this exercise, the other players (VA, DC, and MD) might have had a better idea of whether they would have trouble communicating with the Federal Government at that location during this type of crisis response/coordination.

Issue: Relationship Between USDHS and FEMA During This Type of Crisis Management

Observation: Although the relationships are still being developed, the new laws and Presidential Directives are quite clear on the relationships and responsibilities of both agencies. USDHS (through the Office of the NCR Coordinator) has policy and Lead Federal Agency (LFA) responsibility for the NCR. FEMA has the same responsibilities that it has always had, and that is to coordinate the Federal response to the consequences of any type of disaster within the region. The only difference is that the USDHS is acting as the LFA on major decisions that are coordinated with the other State-level jurisdictions. It should be noted that both the USDHS and the Federal Coordinating Officer (FCO) for FEMA did an excellent job of coordinating their actions and responsibilities during this exercise. Both Mr. Ken Wall (USDHS) and Mr. Tom Davies (FCO, FEMA) did an outstanding job of fulfilling their roles during this exercise.

Recommendation: The NCR jurisdictions should continue to conduct a wide range of exercises that will prepare and train the entire region in the complex requirements of coordinating all of the government actions required to protect the NCR community from a WMD terrorist attack.

Issue: Change in Threat Level from Yellow to Orange

Observation: The FEMA team took the time to discuss options and actions based on the information regarding the change in threat level, and took the following actions: They simulated calls up their internal chain of command to make recommendations

and to seek guidance. They simulated alerting all members of the NCR Emergency Response Team – National (ERT-N) of the change in threat level. The FCO ordered his staff to conduct a communications check with all NCR EOCs. This was actually done at 1:15 p.m., with no prompting. The FCO also had his staff begin keeping a log of all activities.

Recommendation: None. Based on the available information, the FEMA FCO and his staff took proper actions.

Issue: Coordination and Information Sharing Within the NCR

Observation: The first of several NCR conference calls occurred at approximately 1:35 p.m. Participants included the senior leaders of the NCR and FEMA. Available information and intelligence were shared and options for action were discussed and coordinated. In response to an injected fax from USDHS, the FEMA FCO stated that under the circumstances outlined in the scenario, FEMA would be represented in the DC EMA EOC in a real-world setting.

Recommendation: During all future exercises, FEMA representatives in NCR EOCs should be able to act on behalf of their respective organizations (decisionmakers).

Issue: Press Inquiries to FEMA

Observation: The FCO fielded the press inquiries himself; to help ensure a coordinated message, he referred the press to USDHS for comment. This was the correct response both operationally and politically. He clearly understood the importance of a coordinated press release.

Recommendation: Each NCR press officer should continue to develop coordinated NCR media response plans.

Issue: Fax Directing That States Be Informed of Threat Level Change and Specific Actions

Observation: The FCO spoke with his chain of command by phone and recommended that the NCR Management Cell be deployed to the appropriate NCR locations as a precautionary measure. He also recommended that the Region 3 Regional Operations Center (ROC) stand up. He had previously notified all FEMA regions of the change in threat level before being prompted by the fax.

Recommendation: None. All proper actions were implemented.

Issue: Post-Seattle Blast Actions

Observation: The FCO took part in another NCR senior leaders conference call and simulated conversations with his chain of command. He also had conversations with USDHS in which he

recommended deployment of the entire NCR ERT-N team. He ordered his staff to ensure that the Continuity of Operations (COOP) site is fully "warm" and that they conduct a communications check with units in the COOP.

Recommendation: None.

Issue: VNN Broadcasts

Observation: Unfortunately, the FEMA representatives taking part in the exercise could not hear the broadcasts because the sound on their PCs did not work, and they did not have control of the volume on the big screen.

Recommendation: Technical support should be available in future exercises to ensure that all participants have the ability to hear what is going on.

Issue: Actions Taken After Seattle RDD Confirmed and Change in Threat Level from Orange to Red

Observation: The FCO, in concert with USDHS and the FEMA chain of command, activated the NCR ERT-N to the emergency relocation site in Maryland. Other pertinent EST activations were also considered so that units would be operational BEFORE an event occurred in the NCR. FEMA operations would have moved to their IOF so as to be out of the DC area prior to an event. FEMA regions and NCR EOCs were kept apprised of actions taken by FEMA.

Issue: Video Conference

Observation: FEMA representatives were unable to access video conferencing during the exercise due to technical problems. The FCO instructed his staff to ensure that all necessary names and phone numbers of points of contact (POCs) are available for real emergencies. He stated that in the real world, he would have had the technical support he needed to take part in the video conference.

Recommendation: Proper video communications support should be made available to all key NCR facilities before the next scheduled NCR exercise.

DISTRICT OF COLUMBIA EMERGENCY MANAGEMENT AGENCY
EMERGENCY OPERATIONS CENTER
WASHINGTON, DC

General Statement

The District of Columbia Government and EMA worked collectively with several other EOCs to exercise their plans. This exercise proved to be beneficial to the DC government and the DC EMA. The DC EMA stood up all Emergency Support Functions (ESFs), even though a few agencies either reported late or failed to report.

The controllers witnessed DC EOC participants working very well with each other and within their respective ESFs. Information was passed among agencies in a proper and respectful manner. Most of the participants understood and performed their roles in the DC EOC. These same participants carried out their responsibilities as they were instructed and as they had practiced in previous training exercises.

In the beginning of the exercise, the leaders of the DC EOC appeared to be somewhat loose with the management of the operations. As the exercise progressed, they gained and maintained control of the exercise EOC staff. The only recommendation that can be offered is to practice, practice, and practice.

Specific issues identified at the District of Columbia EOC:

- Unfamiliarity of the new E-Team Software
- Technical Issues
- Security
- Public Information
- Reports from ESFs

Issue: Lack of Familiarity With New E-Team Software

Observation: Several of the participants in the DC EOC appeared to be having difficulty using this software, at least in the beginning of the exercise. Prior to the start of the exercise, a special training session on using the new software was held in the EOC. Not all participants in the DC EOC were present for this training.

Recommendation: Training for participants who will use this software in the future should have been held several days before the exercise. The DC Information Technology section provided several staff members to assist with questions and problems as they arose. The

participants should have been given more time to learn and experience the advantages of the software prior to using it during a real or simulated terrorism event.

Issue: Technical Issues

Observation: Many participants were forced to wait for data from EOC printers. In many cases, this is a trivial issue. During this exercise, however, many participants were waiting for printed copies in the area where the Operations Chief and his staff were trying to manage the situation. People standing in this area tended to cause several problems: obscuring the Operations Chief's ability to see the participants and the information displayed on the video screen(s); distracting the Operations Chief and/or his staff by the conversations being held; and the ability of other participants to move freely through the DC EOC to gather information.

Recommendation: There should be more than one printer for 45 workers in the DC EOC. This printer(s) should be located close to the ESF areas without obscuring the vision of the Operations Chief and/or staff, and where they will not interfere with the flow of traffic through the DC EOC.

Issue: Security

Observation: During the exercise, many observers passed through the main area of the DC EOC. The majority of these observers were local dignitaries and/or VIPs of the DC Government. The process for checking the identification of all persons entering the EOC appeared to be in place, but many of the visitors were not checked against an "authorized access" list.

Recommendation: Implement a more visible method of indicating that security checks were performed and a person has been cleared to enter the sensitive area. The liaisons for each of the ESFs should be able to quickly determine if a person/observer has the proper credentials to be in the EOC. This ensures safe operations of each ESF Liaison.

Issue: Public Information

Observation: The DC EMA public information officer (PIO) and staff appeared to be very busy dealing with the visiting dignitaries. Their participation in the exercise appeared to be minimal.

Recommendation: It is understood that when a real-world situation is unfolding in the DC EOC, the visitors will not be in the DC EOC. This should free the PIO and her staff to perform those duties as identified in the DC EOC protocols.

DC EOC needs to identify a location where joint regional information can be obtained and verified, briefings can be developed, and contacts can be directed regarding the event(s). The contact information and location of this Joint Information Center (JIC) should be provided to all participants in the DC EOC and the surrounding EOCs. Information to the public and the news media regarding the safety of the public is very critical during an incident.

Issue: Reports From ESFs

Observation: Hourly reports were requested from the ESFs. Several, not all, of the ESFs were able to give their reports. There appeared to be two reasons for this: the importance of the ESF for the particular timeframe, and not enough time allotted for each ESF to make a report.

Recommendation: Three methods could be implemented to deal with this observation. First, develop a template of what information needs to be reported by each ESF; second, through analysis of past exercises, determine which ESFs need to report during a particular work period(s)—develop a checklist to help the DC EMA Operations Chief and/or his staff to manage these reports. Third, set timeframes for the presentation of the ESF reports, and have the ESFs practice making reports in that timeframe.

FEDERAL BUREAU OF INVESTIGATION
WASHINGTON FIELD OFFICE
WASHINGTON, DC

General Statement

For pragmatic reasons, the participation of the NCR in any TOPOFF exercise is indispensable. In any incident, whether natural or man-made, the resources of the Federal Government will require some time to respond and arrive at the scene of an incident. These resources, in the form of personnel and assets, are critical to the preservation of life and the restoration of important infrastructure. This is particularly true when the incident(s) involves terrorists and the use of WMD.

An exercise of the magnitude of T2, with the participation of thousands of individuals (elected and appointed; State, county, and municipal; crisis and consequence responders), jurisdictions within the continental United States, and international implications, necessitates the consideration and active involvement of the NCR. The NCR is the keystone to most if not all of the Nation's central databases; it serves as the conduit for national, regional, State, and local representation and decision-making; it is positioned to activate and dispatch specialized personnel and vital assets to affected areas; it is central in the gathering and dissemination of information and intelligence throughout the United States and internationally; and as the seat of national government and host to commercial associations, nongovernmental organizations, and countless other entities, the NCR is directly or indirectly impacted by events that occur anywhere in the United States and its territories, and even in other countries. Therefore, the NCR should be integral in all aspects of the TOPOFF exercises.

The participation of the NCR in T2 was not integral and its presence was an afterthought, which short-circuited many of the operational procedures that normally take place. The results were confusion, miscommunication, misdirection, and ineffective action. The participation of the FBI WFO is a case in point. It was tasked with the role of performing and executing functions that are not within its normal realm, which contributed to actions inconsistent with proper procedures. As expected, this resulted in questioning of the value of the exercise.

In addition to the pragmatic reasons for NCR involvement, there are also symbolic reasons, such as conveying the command and control of the government by representative leadership. The functioning of the government's departments and agencies is a statement of the stability of the government.

Specific issues identified at the FBI WFO:

- National exercise participation
- Generation of exercise intelligence
- Communications and intelligence release

Issue: National Exercise Participation

Observation: The NCRFE was based on the events of T2, but NCRFE participants were not permitted to intermingle with T2 players. Due to the very nature of the NCRFE, participating agencies raised questions and concerns regarding T2 events and intelligence generated at the Seattle, WA, Incident Command. Because additional exercise information was not available, the FBI WFO was forced to break with NCRFE communication protocols and contact the Strategic Information and Operations Center (SIOC) regarding Seattle incident intelligence, and pass this information on to all participating agencies.

Recommendation: FBI WFO, National Capital Response Squad (NCRS), recommends that future National Field Training Exercises (FTXs) have either the full participation of all agencies involved without limits on communications, or no participation at all in the FTX. Limiting agencies' participation is counterproductive and unrealistic during a true WMD event.

Issue: Generation of Exercise Intelligence

Observation: A raw intelligence product was developed for the T2 exercise and provided to the WFO FBI as part of the NCRFE. WFO was participating as both FBI HQ/SIOC and the FBI Field Office, and did not have sufficient time to generate a working intelligence product to release as exercise intelligence for the initiation of the NCRFE.

Recommendation: Increased preparation time for FBI analysts would allow for generation of a useful intelligence product. This product could then be disseminated to relevant State and local agencies for use in asset deployment and event evaluation.

Issue: Communications and Intelligence Release

Observation: Communication among exercise controllers and the release of exercise intelligence needs to be re-evaluated. Allowing the intelligence products to control the exercise actions is a realistic scenario. However, by providing all NCRFE participating agencies with the same intelligence product at the same time through exercise controllers defeats the nature and objectives of the NCRFE exercise. Appraising the command and control issues among the various agencies is nullified by this action.

Recommendation: FBI WFO NCRS recommends that the agency responsible for generating the intelligence should control the product and disseminate the information accordingly.

MARYLAND EMERGENCY MANAGEMENT AGENCY (MEMA)
EMERGENCY OPERATIONS CENTER
REISTERSTOWN, MD

General Statement

As part of the NCRFE, MEMA sought to evaluate its own processes and capabilities while engaged in a simulated domestic security incident of significant scope. Representatives from various relevant Maryland agencies were present, and the participation level from all players was high.

Representatives from the State of Maryland participated in the exercise primarily from a conference room area located within the State of Maryland EOC, and all injects were received there and disseminated to the participants around the table for discussion. This design led to a cooperative information-sharing environment and was a benefit to the exercise participants. The State of Maryland was also able to use a secure video conference capability that was shared with DC and VA, which would have been critical for any necessary secure teleconferences. Unfortunately, due to technical problems with some outside systems, the video interface was minimal. However, the Maryland EOC was able to receive the VNN live feeds that originated from the State of Washington, which was invaluable for information acquisition, enhancing the exercise as a whole.

The State of Maryland participated to the fullest extent in a highly effective functional exercise environment, and some very significant issues were brought to the surface throughout the day.

Specific issues identified at the Maryland Emergency Operations Center:

- Regionalized domestic security threat condition change
- Information sharing among the NCR jurisdictions
- "Essential Employee" designation

Issue: Regionalized Domestic Security Threat Condition Change

Observation: A critical issue of concern that Maryland had throughout the NCR exercise dealt with the shifting of domestic security threat level conditions. Questions arose from the State about whether it was a USDHS requirement for Maryland to issue a statewide threat condition elevation, or whether that threat condition could be elevated regionally, i.e., affecting only the NCR jurisdictions. Maryland stated that a series of required security and legislative protocols would be put into effect if the domestic security threat level condition is raised to red, and that the State should have the ability to regionalize the threat level elevation to include the areas of highest vulnerability, but not be so inclusive as to prohibit "normal" operations statewide in

areas of lesser vulnerability. Maryland did recognize through its discussions that there is a distinct liability issue, as well as a reliance on other jurisdictions and cooperative efforts, that exist within the NCR jurisdictions. Decisions for the State of Maryland would not be made without, at the very least, consultation with the DC and VA.

Recommendation: It was clear that this issue needs to be examined further. Consider a collaborative panel discussion or workshop with representatives from the NCR jurisdictions; the State of Maryland; the State of Virginia; the District of Columbia; USDHS; and other relevant regional and Federal partners and stakeholders, with regionalized domestic security threat level condition change as the principal subject for discussion.

Issue: Information Sharing Among the NCR Jurisdictions

Observation: During the NCRFE, there was a minimal level of information sharing and collaboration among the NCR jurisdictions within the allocated response timeline presented in the scenario. The sharing of information was primarily done through pre-scheduled conference calls in which all relevant jurisdictions and Federal agencies participated. The conference calls were facilitated by USDHS and primarily dealt with global issues relevant to all involved. There was very little independent information sharing that took place outside of the conference call format. The State of Maryland struggled with some critical issues throughout the afternoon that were presented to them as a result of the exercise events. Similar issues were likely encountered within the other participating NCR jurisdictions as well, but at no time outside of the pre-arranged conference calls was DC or VA queried as to how they were handling these issues of concern. This observation goes both ways: neither NCR jurisdiction reached out to the State of Maryland to discuss situations or share information during the exercise. As critical regional partners, the sharing of information is essential to a coordinated and effective response.

Recommendation: Continue to foster a regional relationship with DC and VA as NCR partners through exercises and training such as the NCRFE. Continued collaboration and partnership in training, exercises, and plan development only enhances the NCR's overall level of domestic preparedness.

Issue: "Essential Employee" Designation

Observation: There was a great deal of discussion among players about Maryland's current "essential employees" list. This list was designed to address the State's critical employee needs in the event of an emergency triggered by a natural disaster. It lists those employees who would be required to report to work despite a situation that would warrant the closing of government offices. Players noted that this list may not accurately reflect the State's employee requirements in the event of a domestic security threat or act of terrorism. There was some discussion as to how this situation could or should be resolved. Also, players discussed how, exactly, such an order would be carried out on a statewide basis. That is, would a domestic security disturbance in the Washington, DC, or Annapolis area necessitate the closing of government offices in other regions? The question remains: how should the recommendation be written to reflect these

needs? In many ways, these discussions mimicked those that players had about the elevation of the NCR threat level on a regional vs. statewide level.

In addition, players discussed the financial ramifications of such a move and what variables would allow the State to be (or not be) reimbursed. For example, would a liberal leave or administrative leave be the best financial approach for the State? Would the State he compensated under a Code Red threat level?

Recommendation: This is by no means a "simple fix" problem, and will require a concerted effort and meaningful discussions to resolve. Representatives from all primary State agencies should formulate an idea of what types of personnel would he necessary in the event of a terrorist attack or other domestic disturbance. Employee lists unique to each region may very well be the best approach.

Anything that can be clarified immediately, however, should be. For example, a clear understanding needs to he reached between the Federal Government and Maryland as to what employee expenses, if any, are reimbursable. This is a particularly acute problem if there is an expectation that all NCR jurisdictions will react to the same threats in the same manner.

U.S. DEPARTMENT OF HOMELAND SECURITY
NATIONAL CAPITAL REGION
WASHINGTON, DC

General Statement

The USDHS, ONCRC was actively involved in the exercise and participated in their role in providing policy guidance and coordination for the NCR jurisdictions. This aspect of the exercise went very smoothly.

Unfortunately, the actual NCR Coordinator was detailed to Seattle for T2, so his deputy participated in the exercise and did a great job. In the future, it might be beneficial for all principals to participate in these types of exercises.

The Deputy NCR Coordinator operated out of his office, as this is where he would begin during an actual incident until the time that the Federal agencies' relocation sites were activated. In future exercises it would be beneficial to take the scenario to the point where these sites are activated so that agencies can adequately assess how this process will occur, as well as the ability to effectively communicate with one another.

Specific issues identified at the USDHS:

- Coordination and Policy Guidance
- Communication and Coordination with Other NCR Jurisdictions

Issue: Coordination and Policy Guidance

Observation: Providing policy guidance and coordination for the National Capital Region is a new role for the U.S. Department of Homeland Security, and it was accomplished without any problems. The Deputy Coordinator has a good understanding of what actions he needed to take in order to provide the necessary information to the NCR jurisdictions.

Recommendation: Conduct more NCR response exercises to further improve new working relationships.

Issue: Communication and Coordination with Other NCR Jurisdictions

Observation: The Deputy Coordinator was actively involved in all conference calls that took place during the course of the exercise between the Federal agencies and the NCR jurisdictions.

Recommendation: As noted by the Maryland EOC evaluator, more direct communications between NCR jurisdictions is needed in future NCR exercises.

APPENDIX A
EXERCISE PARTICIPANTS

DC EOC

(b)(6) DC WASA
(b)(6) DC WASA
(b)(6) USSS
(b)(6) G.U.
(b)(6) G.U.
(b)(6) G.U.
(b)(6) G. U.
(b)(6) G.U.
(b)(6) DC O.C.T.O.
(b)(6) DC WASA
(b)(6) MDW
(b)(6) DC Hospital Association
(b)(6) DC DPW
(b)(6) DC DPW
(b)(6) DC FO
(b)(6) DC FO
(b)(6) HAWDC
Ghermay Aranga, O.C.T.O.
(b)(6) DC Fire
(b)(6) O.C.T.O.
(b)(6) GWU
(b)(6) DCMA
G. Bryan Jones, DHS/PHS Region III
(b)(6) EMA
(b)(6), OPM OSKA
(b)(6) OCP/PSC
(b)(6) PEPCO
(b)(6) FPS-DHS
(b)(6) MPD-SOD
(b)(6) USCP
(b)(6) DDOT
(b)(6) O.C.T.O.
(b)(6) DDOT
(b)(6) DCNG
(b)(6) DC WASA
(b)(6) DC WASA

MD EOC

Don Keldsen, MEMA
(b)(6) DHMH
(b)(6) MEMA
(b)(6) MIEMSS
(b)(6) MSP
(b)(6) MSP
(b)(6) MDE
(b)(6) MEMA
(b)(6) MEMA
(b)(6) MEMA
(b)(6) MEMA
(b)(6)
(b)(6) MSP
(b)(6) City of Annapolis
(b)(6) MEMA
(b)(6) MEMA
(b)(6) DHMH
(b)(6) MDOT
(b)(6) DHMH
(b)(6) DHMH
(b)(6) MIEMSS

VA EOC

(b)(6) VDEM
(b)(6) VDEM
(b)(6) VDEM
Dawn Eischen, VDEM
(b)(6) VDEM
(b)(6) VDEM

FBI-WFO

(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI

(b)(6) FBI
(b)(6) FBI
(b)(6) FBI
(b)(6) FBI

FEMA

Tom Davies
Richard Rowley

USDHS, NCR

Ken Wall

TOP OFFICIALS (TOPOFF) EXERCISE SERIES:

TOPOFF 2 (T2) After Action Report ANNEX D

September 30, 2003

This page intentionally left

TOPOFF2 CYBEREX

AFTER ACTION REPORT

JULY 2003

INSTITUTE FOR SECURITY TECHNOLOGIES AT

DARTMOUTH COLLEGE

TABLE OF CONTENTS

TOPOFF2 CYBEREX

EXECUTIVE SUMMARY

The national infrastructure of the United States is vulnerable to disruption by physical attack because of its interdependent nature and by cyber-attack because of its dependence on computer networks. Those who intend to do harm to the United States will seek to exploit vulnerabilities using conventional munitions, weapons of mass destruction (WMD), and cyber-weapons. Over time, such attacks are increasingly likely to be delivered through computer networks rather than using conventional munitions alone, as the attractiveness of cyber-attacks and the skill of U.S. adversaries in employing them evolve. Cyber-attacks will provide both state and non-state adversaries with new options for action against the United States beyond mere words.

TOPOFF2 is the second Congressionally mandated, counter-terrorism exercise involving senior U.S. government officials, multiple Federal / State / Local agencies, and Canadian government agencies. The goals of TOPOFF2 were to improve the nation's capacity to manage extreme events; create broader operating frameworks of expert crisis and consequence management systems; validate authorities, strategies, plans, policies, procedures, and protocols; and build a sustainable, systematic national exercise program to support the national strategy for homeland security. While traditional crisis and consequence management organizations were the principal foci of TOPOFF2, there exists another element of our country's critical infrastructure that experts consider highly vulnerable to terrorist-related attack: the national information infrastructure.

TOPOFF2 CYBEREX was a functional exercise to examine, in an operational context, the integration of inter- and intra-governmental actions related to a large-scale cyber-attack synchronized with a terrorist WMD attack against a major urban area of the United States. In the course of these proceedings, players addressed those actions needed to limit the potential damage caused by network compromise and to minimize the impact on operations resulting from the loss of these resources. While exploring the vast complexities of these individual and inter-related actions, this exercise provided an opportunity for

decision-makers and staffs to identify, discuss, and resolve critical issues associated with a cyber-attack and other significant disruptions to their network infrastructures. During these activities players explored potential vulnerabilities and anticipated responses to determine if and what changes might be necessary to existing cyber-security programs and organized responses. Approximately 125 people participated in the exercise on the 6th and 7th of May, 2003. The exercise was held at the Washington State Emergency Operations Center in Camp Murray, Washington.

Lessons Learned:

Participants saw value in a regionally coordinated cyber-security efforts-- in timely exchange information and collective response. The development of this regional approach between State and Local government agencies that participated in TOPOFF 2 will continue post exercise.

The exercise highlighted a need to examine how cyber-response plans and procedures correspond to changes of the color-coded national threat condition promulgated by the Department of Homeland Security (DHS). From a cyber-perspective, what proactive steps should be taken when the threat condition escalates from yellow to orange and then to red? The players examined these and other similar questions.

There are no formally established processes, similar to those in place for a physical attack or natural disaster, that address coordination between the federal government and its state and local counterparts in the event of a cyber-attack

The ability to maintain information technology (IT) infrastructure is predicated on the fact that individuals will be able to get to their workspace. In those instances where this is not true, government agencies responsible for IT infrastructure should examine how they would perform mission-critical functions such as backups and systems maintenance from alternate locations.

During the pre-exercise period, federal government agencies responsible for infrastructure protection were not yet completely evolved due to the stand-up of the new Department of Homeland Security. The federal government should develop an integrated cyber-response plan that addresses crisis support to both state and local governments. There is a need for a single point of direct contact between the federal government and State and Local governments for dissemination of information related to cyber-attacks.

SECTION TWO:

TASKING

INTRODUCTION

The Institute for Security Technology Studies at Dartmouth College (ISTS) is a federally funded Institute which was founded in the FY 2000 appropriation as a national center for counterterrorism and cyber-security R&D. Our mission is to work to secure computer networks against attack, enhance Law Enforcement investigative capabilities in cyber-crimes, and serve as a center for counterterrorism technology research, development, testing, and evaluation. To accomplish this goal we have over 70 researchers at Dartmouth College and employ 20 researchers from other institutes working on research projects related to this mission.

Funding for the ISTS at Dartmouth College was supported under Award number 2000-DT-CX-K001 (S-2) from the Office of Justice Programs, National Institute of Justice, Department of Justice.

The Office of Domestic Preparedness (ODP) had decided after TOPOFF 2000 that TOPOFF II should include a cyber-component. Representatives from ODP met with the Director of the ISTS at Dartmouth College early in 2002 and the two organizations agreed that the ISTS should take a lead role in preparation and conduct of a cyber-exercise for TOPOFF II. Not only does this task align with the mission of the ISTS, hut this relationship ensured that the ISTS could provide funding necessary to conduct the cyber-exercise for TOPOFF II at no cost to ODP, a necessary condition for completion of the project on schedule.

SECTION THREE

STAKEHOLDERS

PRINCIPAL STAKEHOLDERS

TOPOFF2 CYBEREX players were primarily those Federal, State, County, City, private sector, and personnel from the Government of Canada who have active roles in the daily operations, management, and security of their information networks, systems, or infrastructure within their organizations. These participants would most likely play key roles in responding to or managing the consequences of a significant regional cyber-disruption or attack. The principal stakeholders in the exercise were:

- IT organizations and Top Officials from:
  - Washington State
  - King County
  - City of Seattle

Supporting these players were representatives from the following organizations:

- A commercial telecom provider and local Internet Service Provider (ISP)
- Federal computer incident response agencies
- Federal law enforcement agencies

ORGANIZATION AND ROLES

The following is a summary of the organizations involved in the exercise.

- Five Network Operation Centers (NOCs) participated in this exercise:
  - City of Seattle
  - King County
  - Washington State Department of Information Services (DIS)
  - Washington State Department of Transportation (DOT)

- Washington State Emergency Management Department (EMD)

Each exercise NOC was composed of individuals from within the organization who are assigned to these NOCs on a routine basis. These groups responded to and managed consequences presented in the exercise. Because of the restricted time available during the exercise, not all elements of an organization's response were addressed. Unresolved issues necessary to keep a NOC's actions and deliberations flowing were resolved by a group's facilitator or the Control Team and brought forward during the final plenary session. The general responsibilities of the NOCs included:

- Assessing network status.
- Exploring the impact of differing proactive response strategies.
- Responding to network disruptions.
- Providing periodic summaries to Top Officials (TOPOFFs).
- Developing recommendations for TOPOFFs.
- Sharing information with other NOCs.
- Sharing resources with other NOC's.
- Responding to mock media inquiries.

- A group of Top Officials from Federal, State, County, and City government organizations participated in TOPOFF2 CYBEREX. In addition to observing exercise activity and assessing their ability to work as a team, these officials acted as an executive body to address and resolve cyber-security issues challenging the NOCs. These senior executives were incorporated into the TOPOFF Coordination and Communication Group (TCCG). The function of the TCCG was to provide a forum for senior executives to:

  - Gain and maintain situational awareness of emerging events, develop strategic courses of action to conduct a concurrent and integrated response, and direct appropriate actions.
  - Mitigate consequences of enterprise network disruption or loss.
  - Address and resolve the allocation of limited resources among competing demands.

- Collect, analyze, formulate, and disseminate information to stakeholders in and outside the state, including the media.
- Develop recommendations for political leadership (chief executive) approval or action.
- Respond to inquiries from senior executives of the Federal government.

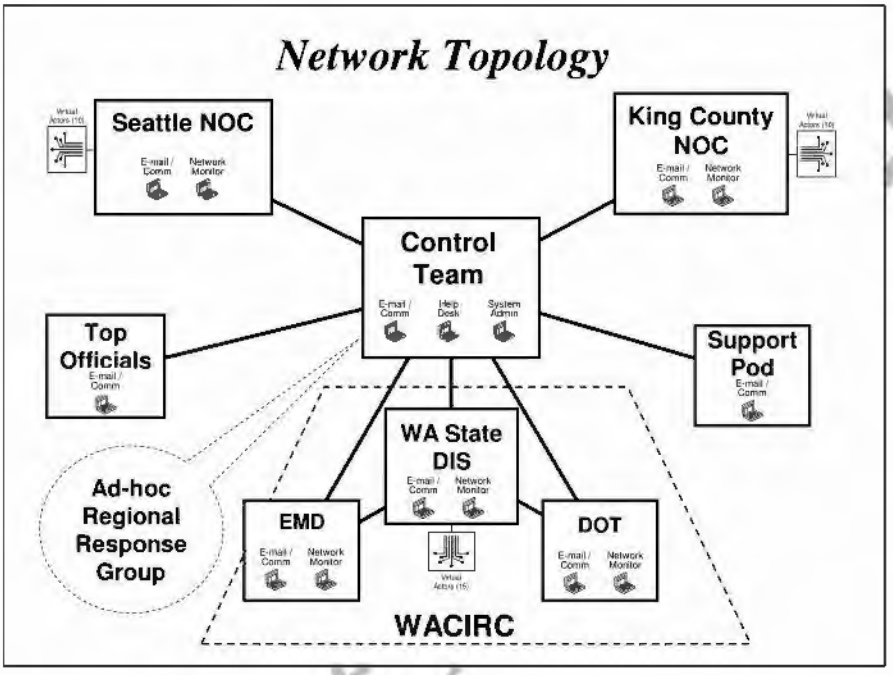
Accordingly, to work effectively in an inter-governmental environment, the Top Officials from each organization assigned to the TCCG had experience, authority, and access to the organization's political leadership. Chief information / chief technology officers (CIO / CTO) and/or members of their immediate staffs filled these positions during the exercise. Top Officials came from the following organizations:

- State of Washington CIO / Director of Washington State DIS
- State DOT (Information Technology Section)
- State EMD (Telecommunications Section / Director's Office) and National Guard
- Office of the Governor
- King County (Information and Telecommunications Services Division / Office of Information Resource Management)
- City of Seattle (Department of Information Technology)
- University of Washington (University Computing Services)
- Top Officials played by the Control Team:
  - Governor
  - County Executive
  - Mayor
  - Department of Homeland Security (DHS)

Another group, acting in support of the TCCG, consisted of regional government and corporate representatives who would have a logical role to play given the scenarios. Unlike the NOCs and the TCCG, the Support Pod had no direct "play" in TOPOFF2 CYBEREX. Rather, their role was to provide information to, and respond to resource requests from, the principal players. Representatives of support organizations had an in-depth understanding of the

technologies, capabilities, and processes that their organization would provide the principal players, and the methodologies to avail these resources.

The following diagram depicts the overall organization of TOPOFF2 CYBEREX.



EXERCISE OBJECTIVES

TOPOFF2 requirements stated that: "This series of exercise components will also improve 'crisis resistance' through opportunities to measure plans, policies, and procedures required to provide an effective response to a weapons of mass destruction (WMD) terrorist incident." This type of incident would be more complex and significantly challenge the capabilities of organizations assigned the responsibility of providing a first response if government-related information networks were simultaneously and maliciously disrupted due to a large-scale cyber-attack. Accordingly, within the context of a TOPOFF2-like WMD event, the players gave due consideration to the following issues and objectives during the development of the CYBEREX:

- The effectiveness of the various cyber-security plans, policies and procedures of the City, County, State, and Federal levels to adequately address issues and support the response for a large-scale cyber-attack on government-related information networks.
- The ability of participating NOCs to organizationally integrate and effectively conduct or manage a sustained response to a cyber-attack.
- The planned flow of communications and information in an operational context.
- The decision and coordination processes in a range of potential consequences.

Within these overarching set of objectives, each of the principal stakeholders had their own objectives for this exercise. These included:

- DIS - Determine that the Washington State Computer Incident Response Center (WACIRC) procedures -- including incident reporting, response, escalation, communications, containment, etc. -- were sufficient to effectively mitigate the effects of cyber-attacks.
- City of Seattle & King County - Develop policies and procedures relating to large-scale cyber-attacks, including federal notification and response.
- City of Seattle & King County - Determine the effectiveness of the draft policies and procedures along with federal notification procedures.

Throughout the development of the exercise, these objectives guided the design and methodologies used to achieve the stakeholders expectations. A flexible design structure was used for the development of this exercise, thus allowing for the incorporation of new objectives should they arise.

It became apparent during the design of the game that the principal stakeholders realized that there might be significant value in developing a regional approach to a response to a major cyber-attack. The stakeholders held several meetings to address this regional approach to the prohlem. One outcome of these discussions was the proposal for a regional information sharing system to be used by the stakeholders to report significant anomalies occurring on each organization's networks. This prototype system, entitled the Regional Information and Intelligence Gathering (RIIG) was exercised in the two-day event. Additional refinement on this initiative was planned after the exercise based on how the RIIG was used during the event.

Additionally, this exercise was designed so that principal stakeholders may develop strategies and planning frameworks to:

- Coordinate inter-governmental responses and consequence management to cyber-attacks.
- Maintain continuity of operations within participating organizations.
- Develop alternatives and recommendations to senior or executive decision-makers in responding to potential cyber-crisis events.
- Sustain confidence in government information networks during a cyber-attack and, if necessary, regain public confidence.

Each participating organization developed its own self-evaluation criteria for the exercise. Inclusion of these criteria and the results of their assessment go beyond the scope of this report. Here we address information and resources sharing between organizations.

The following is a summary of the organizations participating in TOPOFF2 CYBEREX:

King County

- Department of Executive Services
- Department of Natural Resources and Parks
- Department of Public Health
- Department of Transportation
- Information and Telecommunications Services Division
- Office of Emergency Management
- Prosecuting Attorney's Office
- Sheriff's Office

City of Seattle

- Department of Information Technology
- Department of Transportation
- Police Department
- Seattle Center
- Seattle City Light
- Seattle Public Utilities

Washington State

- DIS
- DOT
- EMD
- Office of the Governor

Canada

- Office of Critical Infrastructure and Emergency Preparedness
- Province of British Columbia Ministry of Management Services
- Province of Ontario Information Protection Center

Other Participants

- Boeing Corporation
- Federal Bureau of Investigation – Seattle office
- CERT at Carnegie Melon
- National Communication System
- Microsoft Corporation
- Qwest Corporation
- United States DHS
- United States Department of State
- United States Secret Service – Seattle Office
- United States Attorney
- University of Washington

SECTION FOUR

SEMINARS

As part of the exercise development and learning process for the stakeholders, we held two seminars in the Seattle area at the Criminal Justice Training Center. Each was attended by about 125 people from the stakeholder community including State of Washington, King County, and City of Seattle's government agencies. Representatives from the Port of Seattle, Boeing, Microsoft and the University of Washington also attended. The seminars were held at no cost to the participants. In general, presenters donated their time and travel expense.

Seminar 1: Notification Policies Seminar – to review areas of responsibilities of federal agencies, reporting thresholds, trigger points to access resources, and escalation procedures.

- Held 6 February, 2003.
- Moderator: (b)(6) former Director of the Department of Defense Cyber Crime Center.
- Presenters
  - (b)(6) – NIPC
  - (b)(6) - FBI, Seattle
  - (b)(6) – USSS, Seattle
  - (b)(6) – US Attorney's Office
  - (b)(6) – National Communications System
  - (b)(6) – Qwest
  - (b)(6) and (b)(6) – OCIPEP of Canada
  - (b)(6) - ISTS-Dartmouth College on the recent Slammer Worm

Seminar 2: Threat Assessment Seminar – What are the threats, what are the tools we have to defend against them, how do we conduct a cost benefit analysis to determine which tools to invest in?.

- Held: 11 March 2003
- Moderator: Dr. (b)(6) CIA Senior Scientist - Info Ops Center
- Presenters:
  - Dr. (b)(6) – National Security Council, Office of Cyberspace Security
  - (b)(6) – ISTS at Dartmouth College – end effects and methods
  - (b)(6) – CERT
  - (b)(6) – NIPC Unclass Threat Assessment
  - (b)(6) – University of Washington
  - (b)(6) – City of Seattle CISO and founder of Agora
  - (b)(6) – Defense in Depth

SECTION FIVE

SIMULATION

As the CYBEREX portion of TOPOFF2 was conducted on a not-to-interfere basis with the principal exercise, the network operation centers (NOCs) of participating organizations employed a simulated network, developed by the Institute for Security Technology Studies (ISTS) at Dartmouth College as a primary source of exercise-related stimuli.

This simulated network replicated the functional elements of regional wide area networks, inter-governmental networks, and access to the public Internet. Exercise designers worked with network managers of participating organizations to develop a plausible emulation of the organizations' networks, while ensuring that the simulation did not reveal critical vulnerabilities or disclose exact security measures. Participants had final approval on the network simulation used by their organization during operational exercise activity. The below diagram depicts a simulated network display used by one of the stakeholders:

Employing a Master Scenario Event Listing (MESL) developed before the exercise with the assistance of stakeholder Trusted Agents, simulation controllers were able to generate disruptions to simulated network hardware, such as workstations, routers, firewalls, servers, and to the connectivity "pipes" connecting them. These controlled disruptions were based on actions of the attacking agents and included malicious events and normal disruptions. The effects of these disruptions were revealed to the players on a Web-based display application that highlighted the location of the disruption and often its severity. Remediation of these problems was made through player interaction with members of the network control team. Details of the MSEL are included as an appendix to this report.

In addition to stimuli being provided by the network simulation, participants received injects through an exercise communication system developed for the CYBEREX. From a single computer workstation, participants could send and receive e-mail and replicate the use of telephone, facsimile or pager systems.

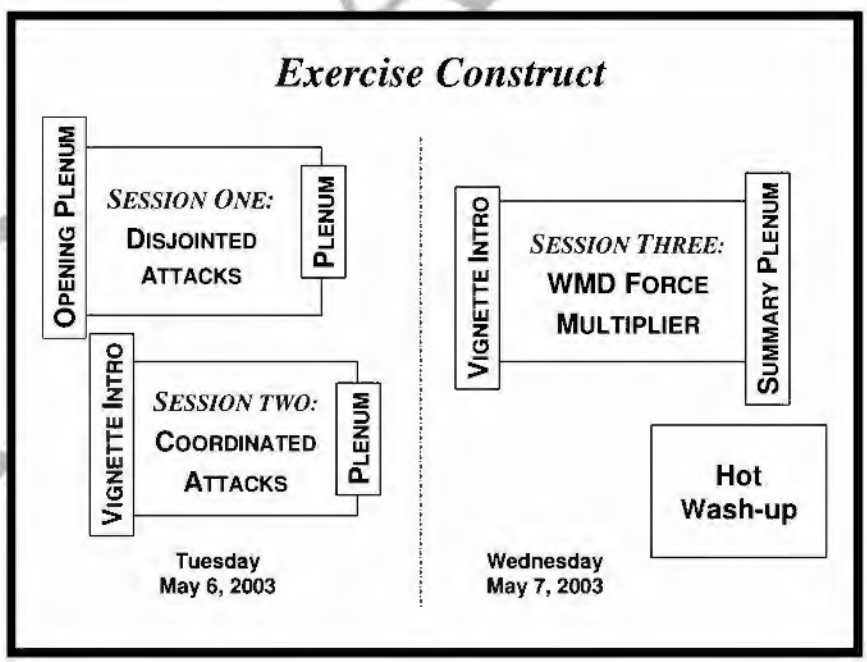
Before interactive play of the exercise began, operators of the network status display consoles were indoctrinated on its use. A briefing of this network was also provided to participants as part of the opening orientation session.

SECTION SIX

EXERCISE DESIGN

CONCEPT OF EXERCISE ACTIVITY

TOPOFF2 CYBEREX was a facilitated, computer assisted, one and one-half day, immersive, scenario-supported, and network-aided interactive exercise where executives and staffs of governmental information technology (IT) organizations explored the challenges of managing disruptions to critical computer networks caused by a terrorist cyber-attack. Participant activity was centered on three vignettes, each associated with different aspects of the complex cyber-security problem. The successive vignettes represented escalating levels of attack and stress for the players. The attacks simulated during the exercise were designed to expose players to a series of exploits which have all been seen in the wild, but which they themselves may never have seen before. The following diagram depicts the construct and flow of these vignettes:



The following is a brief description of each vignette.

- **Vignette One:** Sporadic attacks that affect the State, County, and City network operations. These attacks were not to occur simultaneously, and appeared somewhat disjointed. The intensity of the attacks represented an above-normal level of malicious activity.

- **Vignette Two: Coordinated** attacks of longer duration that reflected multiple attack methodologies. Attack intensity corresponded to the high-end of normal malicious activity and was intended to cause minor to moderate disruption of government information networks.

- **Vignette Three:** Attack coincident with the weapons of mass destruction (WMD) event that **incorporated** the gamut of public-knowledge attack methods. This compound attack was intended to be a "force multiplier" of the WMD event and was directed at specific networked entities with crisis or consequence management roles.

A Hot Wash-up concluded the interactive portion of this exercise. Each group presented the significant and unresolved planning and management concerns, critical issues, and recommendations identified in each session.

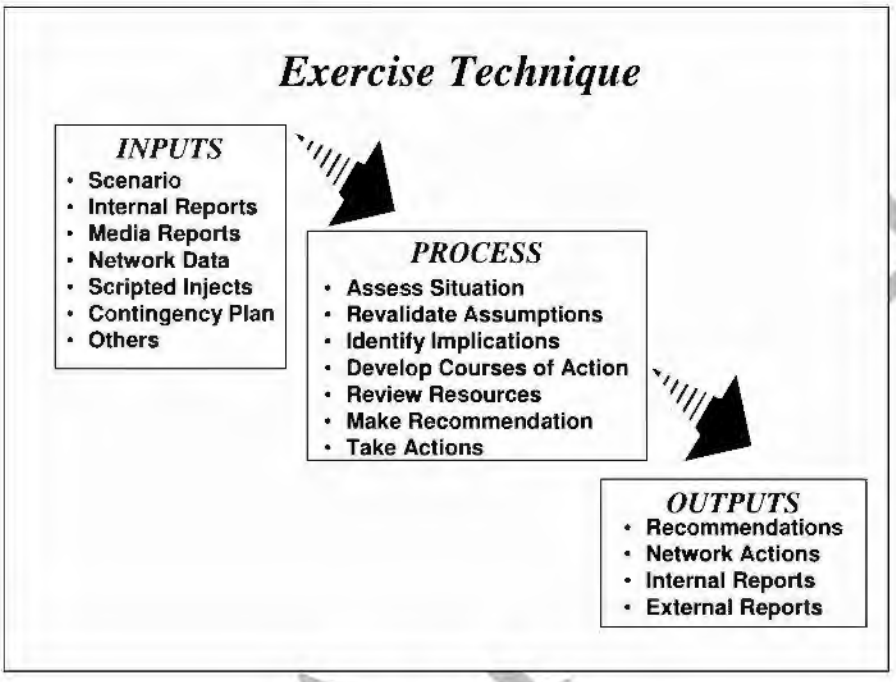
First and foremost: **This exercise was not a test.** Rather, it was an opportunity for participating organizations and individuals to stress their plans, policies or procedures, improve coordination and confidence, augment skills, refine roles and responsibilities, reveal weaknesses and resource gaps, and build teamwork.

Although the incident management and cyber-security plans used by participating organizations provided a foundation for players' actions, these actions and decisions were not constrained by these plans or other current, real-world plans and management concepts.

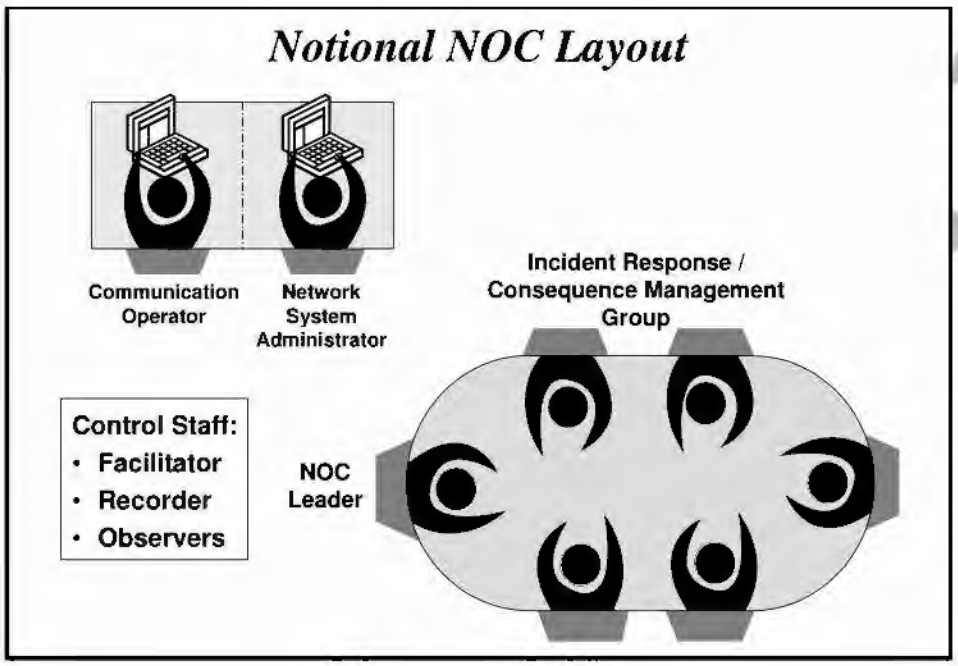
EXERCISE TECHNIQUE

The overall technique employed for this exercise was based on an input ⇒ action ⇒ output paradigm. Using information provided by a scenario, injects, or network status displays,

participants responded to issues related to a vignette. Facilitators assigned to each group assisted the participants through the exercise process and discussions. The following depicts the general flow of this interactive technique:



The principal organizational structure for each stakeholder was a Network Operations Center (NOC). The diagram below provides a notional layout of an organization's NOC:



Each NOC had three primary entities:

- Network Systems Administrator (NSA)
- Incident Response / Consequence Management Group (IR / CMG)
- Communications Operator

The following discussion details the roles and responsibilities of members of the NOC.

- **Network System Administrator (NSA):**

Using data and information provided from a computer display, the NSA was responsible for monitoring the network, and identifying, documenting, and recommending solutions to problems discovered. Additionally, the NSA took actions, within his / her authority, to respond

to the network situation. The NSA also performed network systems troubleshooting to isolate and diagnose system problems. This individual was experienced with the organization's network topology and NSA procedures. Additionally, the NSA possessed an understanding of the underlying technology behind the hardware operating the network and the principal software applications residing on the network. The NSA had the ability to order equipment to be taken off-line, rebooted, and could install filters and block ports.

- **Incident Response / Consequence Management Group (IR / CMG):**

The function of the six (6) individuals composing the IR / CMG was to respond to a significant network disruption or security incident using the organization's plans, policies, and procedures in order to contain, investigate, recover from, and report the incident or disruption. The City of Seattle, King County, and Washington State Department of Information Services (DIS) NOCs each had a six-member IR / CMG. The NOCs for the Washington State Department of Transportation (DOT) and Emergency Management Department (EMD) had a smaller group.

The activities of this group included, but were not limited to: analysis of the situation to determine potential consequences; employment of an organization's mitigative or defensive strategies and resources; documentation of the incident; forensic evidence collection; and investigation. The utility of the IR / CMG was similar to each participating organization's incident response team (IRT) or computer emergency response team.

Most IRT's have both an investigative and a problem-solving component. These functionalities resided in the NOC IR / CMG. This group included management personnel who understand the organization's security, emergency, legal, or network policies, and has the authority to act; technical personnel with the knowledge and expertise to diagnose and resolve problems; security personnel able to track security issues and perform in-stride and post-mortem analysis; or communications personnel able to keep the appropriate individuals and other organizations informed as to the status of the problem and, if necessary, assist in developing

crisis response strategies. One of the six members of this group acted as the leader for the organization's NOC.

- **Communications Operator**

The function of the communications operator was to monitor external communications (e-mail and telephone) for the NOC and relay information coming from these sources to the NOC.

EXERCISE CONTROL

An exercise Control Team oversaw the execution of this exercise and was composed of personnel familiar with the exercise objectives, process, and construct. This group monitored all activities throughout the exercise and adjusted the process as necessary to keep the participants oriented toward outcomes that support exercise objectives. The Control Team had overall responsibility for directing the exercise process, administration, and plenary sessions. Facilitators and data collectors appointed to each pod were members of this group. The Control Team also tracked and evaluated critical outcomes at the conclusion of each session. This group assessed the activity of each pod and, if necessary, provided supplemental information that clarified the scenario.

The exercise technical control staff resided with the Control Team. This staff generated scenario injects depicting the status of an organization's network for viewing on each pod's network status display and injected scenario elements depicting challenges that consequence managers would have to address.

The exercise Design Team indoctrinated members of the Control Team, stakeholder facilitators, NSAs, and communicators prior to the conduct of the exercise. Included in this training were:

- The exercise process, including the organizational structure, the flow of activity, and the expectations at the end of each session. A walk-through of the participant handbook and facilitator guide also occurred.
- Exercise pre-play to demonstrate the expected levels of discussion and required session products.
- A tour of the exercise site to understand the flow of the interactive process and to prepare the pods for exercise activity.
- An indoctrination and practice period using the simulated network (NETSIM) display console and communication laptops.

This training provided members of this team with the requisite information and practice to effectively perform their roles.

SECTION SEVEN

GAME PLAY

In addition to responding to the stimuli provided by the simulated network (NETSIM) and other injects, we tasked participants to prepare responses to questions addressing key issues associated with the theme of each vignette. During the plenary sessions held at the conclusion of each vignette, a member of each pod discussed the organization's responses to these questions. The following summarizes this activity and the players' discussions.

VIGNETTE ONE: NORMAL DAY AT THE OFFICE

The theme of this vignette was an "above normal" level of disruptions to the information networks of each organization. Using information and data provided through network status displays or injects provided by the Control Team, each pod responded to these stimuli by employing their incident plans, policies, and procedures. In addition to exercising these tools, during this session participants were tasked to review their incident response plan assumptions, review the internal and external communication flows of their Network Operations Centers (NOCs), and discuss relevant cyber-security issues. Following this, they identified and prioritized the organizational implications of prolonged periods of "above-normal" network disruptions and how these might influence planned processes, courses of action, and resource requirements detailed in their response plans.

Questions for Plenum

- **What does the Department of Homeland Security (DHS) "Coudition Yellow" meau to your organization, in particular to its uetwork security?**

City of Seattle:

- Practice information technology (IT) callout and alerting plan / verify numbers.
- Consider alternative work schedules of operational staff. If situation escalates, plan to maximize staffing & response capabilities.
- Increase frequency of review of firewall logs and monitoring of other intrusion detection systems.
- Pass advisory to department emergency contacts.
- Introduce measures outlined in BLUE advisory.
- Consider canceling or rearranging vacations and other time off to insure recall capability.
- Conduct security check on all critical systems.
- Be aware of physical access to restricted areas, e.g., communications closet, server room.
- Consider increasing frequency of backups, ensure offsite storage.
- Review network segmentation plans.
- Ensure employees (especially those with field / remote responsibilities) remain vigilant for spotting suspicious activities and behavior and are prepared to report it immediately to Seattle Police Department (SPD).

King County:

- Condition Yellow is normal (elevated level of network security post-Sept. 11).
- King County has developed an incident management plan detailing roles and responsibilities in the event of various disrupted services.

Washington State Department of Information Services (DIS):

- DHS Condition Yellow does not invoke any additional security activity at DIS. This situation is considered a normal activity.
- At Condition Yellow, DIS is at heightened awareness for physical issues -- such as building security.

Washington State Department of Transportation (DOT):

- Send notification of increased alert level to employees for increased awareness.
- Increase frequency of system log scans.
- Contact response team members to coordinate a plan of action.

Washington State Emergency Management Department (EMD):

- Our organization is always at its highest level of network security.
- Block all executable files on a daily basis.
- Daily - run McAfee, updating DAT files.
- Daily - run IP Sentry to monitor network.
- Daily - run full back-up (13-14 hours).
- Subscribe to various LISTSERV - Multi-State (MS), SANS, Federal Computer Incident Response Center (FedCIRC).

- **How is a "normal day" determined in your organization?**

City of Seattle:

- Power is generated, water flows, bad guys get arrested, fires are extinguished, lives saved, people play in parks.
- National threat level is stable.
- Minor problems as indicated by number of Help Desk tickets.
- External pings – Internet Team notified of failures.
- Main systems up – no major outages.

King County:

- A "Normal Day" is assumed until indications are otherwise.
- An extraordinary day looks like:
- Global outage.
- Global e-mail server attack.
- Global phone service disruption.

- Mainframe outage.

Washington State DIS:

- Monitor network on a regular basis.
- Experience on-going scans from the Internet.
- Develop and implement on-going security changes.
- Hold internal security meetings.
- Continue to monitor logging information.

Washington State DOT:

- Equipment failures, network configuration issues, training and use issues, SPAM, questions from customers about viruses, testing and application of system patches, responses to changing architecture software.
- More exciting than a normal day.
- System monitors indicate problems, notification of threats are received, and incoming messages are received that contain unknown content.

Washington State EMD:

- All network services are live and accessible.
- Network latencies to these services do not exceed 300 ms.
- Electrical services are functioning on commercial power.

- **What do you consider your organization's most significant cyber vulnerabilities?**

City of Seattle:

- Access levels to applications and data are not audited on a regular basis.
- Internal 802.11 Wireless and other remote access e.g., CDPD, Digital Subscriber Line (DSL), Inter-Governmental Network (IGN), Integrated Services Digital Network (ISDN).
- Employees: background checks, training, discovering wayward behavior.
- Gaps in communication protocols with other agencies / partners / vendors.
- Lack of policy and staff training for dealing with suspicious e-mails.

- Establish consequence management team (IT managers).
- Viruses externally introduced to the environment.
- Trust issues with sharing passwords and common logins.
- Lack of network segmentation and redundancy.
- Patch levels on old systems – legacy applications cause them to break.
- External virtual private network (VPN) Access – lack of audit ability for firewall and virus protection.

King County:

- Limited County-wide standard for patch and configuration-management.
- Budget constraints prohibit us from implementing inter-department security standards.
- Very limited internal firewalls -- perimeter security only.
- Some external-facing resources on internal network segments (available to public).

Issues:

- No inventory of structured query language (SQL) database and IIS servers within the County network.
- Policy guidance for investigative queries from legal entities.
- Governing authority by ordinance to set and enforce security policy (cyber world).

Washington State DIS:

- Non-disclosure agreement (NDA) would be required before we can answer this question.
- Standard e-mail and Web portal traffic, security awareness.
- In a confederation of government organizations, we are subject to the "weakest link" syndrome.

Washington State DOT:

- Lack of backup data "hot" site should the primary become unavailable.
- Incoming e-mail / viruses from attachments.
- Lack of monitoring tools.

- Social engineering.
- Constantly changing architecture of hardware and software.

Washington State EMD:

- Our biggest vulnerability at this point is our single connection to the Internet through DIS. We have redundancy.
- Lack of internal firewall / intrusion detection systems (IDS)
- Currently, only e-mail is authorized to be transmitted on the State Governmental Network (SGN). Authorization and setup of VPNs is time consuming and cannot be done solely by EMD.
- Internal customers storing files with viruses on their computers. Internal firewalls on each computer are needed and will be installed in the immediate future.

Solutions to overcome these challenges:

- Additional funding is being sought to install two new T1s for Internet connectivity. One T1 should be to a tier one service provider such as Sprint or Uunet. The second T1 should he satellite providing Internet connectivity. All of our circuits will be on physically diverse routes terminating in geographically diverse regions.
- We have purchased and will be installing firewall and IDS systems as well as routers specifically for doing our perimeter or outer layer of cyber-security.

What single events might cause your Incident Response Team (IRT) to activate?

- A local area network (LAN) outage causing disruption to more than 10% of the network services.
- A wide area network (WAN) outage.
- Detection of a virus / worm outbreak.

What cumulative events might cause your IRT to activate?

- Network probe accompanies by an intrusion or intrusion attempt

VIGNETTE TWO: COORDINATED ATTACKS

The theme of the second vignette was a low-level coordinated cyber-attack against stakeholder organizations. Players addressed issues or actions necessary to respond to these attacks in a combined manner and to resume network operations. After recognizing indications of abnormal events, participants analyzed the problem and responded to re-establish the operations of their networks. Working in their respective NOCs, participants initially assessed the situation, implemented their response plans, and determined what additional actions, coordination, and/or resources were necessary. As the situation presented may become greater than what was anticipated by each organization, it may have outstripped available internal resources. This session provided the opportunity for participants to discover the need to revise policies, procedures, resource allocation, and/or communication flows to account for vulnerabilities identified by this vignette that were not addressed hy the organizations' plans.

Questions for Plenum

- **What does the DHS "Condition Orange" mean to yonr organization, in particular to its network security?**

  City of Seattle:

  - Pass alert on to department emergency contacts.
  - Continue or introduce measures listed in YELLOW advisory.
  - Via call-out lists, contact all essential personnel regarding their recall availability.
  - Exercise test alert of all 24 x 7 on call staff between departments and coordinate schedules for critical staff across departments.
  - Test communications: e-mail, 800 MHz radio, carrier pigeon.
  - Suspend public tours of infrastructure.
  - Increase staffing and backup for system monitoring.
  - Change passwords and physical access codes.
  - Verify availability of key vendors.

King County:

- Notify staff and review policies and procedures on how to respond to an attack that occurs during DHS Condition Orange. Condition Orange would command different actions from those previously executed in Condition Yellow.
- Communicate with other agencies to coordinate policies and procedures that are implemented at various DHS alert levels.

Washington State DIS:

- Increased security in all buildings.
- Broadcast message to all DIS personnel about heightened state.
- Be more vigilant, higher awareness among receptionists to ask for ID.
- Facilities staff would ensure backup generators, etc. are ready to go.
- Network Security: same as "usual day" activities, with reinforcement among staff to be aware of their surroundings and people in the area.
- Look for anomalies in network activity.

Washington State DOT:

- Limit pbysical access to computer facilities.
- Deny access to outside vendors.
- All non-DOT IT personnel will be escorted at all times.
- Increased attention to system monitoring.

Washington State EMD:

- How does this differ from a "normal level" of security? It does not.
- How does this differ from DHS "Condition Yellow"? It does not.

- **What is the role of your IT organization in the emergency management organization?**

City of Seattle:

- Provide logistical and communications systems support,.
- Monitor IT infrastructure status
- Respond to IT related problems
- Restore service, e.g. radio, telephone, computer network, e-mail, messaging, file and print services, dispatch, and critical databases.

Gaps:

- Focus on City IT resources as an asset, implement policies and practices to safeguard, protect, facilitate recovery and assure continuity of business.

King County:

- Provide support to King County Emergency Organization.
- Clarify access procedures regarding King County "meet me" room locations.
- Clarify access procedures for Comcast POPs.
- Clarify physical access requirements for all staffing and networking areas relative to DHS conditions.

Washington State DIS:

- DIS has a practice of sharing security incident information with EMD through the Washington State Computer Incident Response Center (WACIRC)
- DIS general rule is to:
- Be a focal point for sharing security information with regional partners.
- To conduct incident notification and response coordination.
- To carry out monitoring and mitigation for SGN and IGN systems, and regional partners (City of Seattle, King County EMD, and DOT).
- DIS Computer Incident Response Team (DISCIRT) was formed in 2002 as an IT organization internal to DIS. DISCIRT is the starting point for statewide incident response that includes EMD.
- DIS and EMD have joined the multi-state Information Sharing and Analysis Center (ISAC) started in New York. EMD represents the physical side, DIS represents the cyber side.

Washington State DOT:

- External - communication with WACIRC via e-mail, fax, pager, phone, and cell.

- Internal - As a support organization for our internal Emergency Operations Center (EOC). We specifically support EOC e-mail and hardware (printers, PCs, faxes, etc.).

Washington State EMD:

- To help coordinate resources when the resources of the local jurisdictions are overwhelmed. To act as liaison between the Local, State, and Federal response agencies.

- **What are your recommendations for a regional response / defense to a wide-scale cyber-attack?**

City of Seattle:

- Develop relationships and protocols related to vertical lines of business: public safety, utilities, human services, etc.
- Organize an inter-agency "Crisis Response" Team to immediately activate and begin analysis and classification of the agent of attack and coordinate response in a real time manner.
- Support LISTSERV for WACIRC Level 2 & 3 problems.
- Activate and communicate with WACIRC, once activated by DIS for Level 1 problem.

King County:

- Establishment of inter-agency communication points of contact list.
- Create inter-agency roles and responsibilities plan.
- Analyze data generated from a host-based and network-based IDS inside King County Wide Area Network (KCWAN) perimeter.

Washington State DIS:

- Early information sharing about potential security incidents and status of incidents in process.
- Central coordination through regional and statewide LISTSERVs. Out-of-band, non-dependent notification system is in place for WACIRC. All regional partners should consider similar.

- Process for states, cities, and counties escalating to federal and international agencies is not yet solidified.

Washington State DOT:

- Obtain management approval for dropping outside internet connectivity.
- Increase system monitoring effort.
- Increased reliance on out-of-band communications.
- Have Public information Officer (PIO) send alerts via television stations carrying DOT camera feeds.

Washington State EMD:

- In this case, the best defense is a good offense. Having cyber-security best practices in place.
- Having redundant paths to your services.
- Early detection determination, and warning with IDS and firewall protection.
- Coordinating response efforts with stakeholders and vendors involved.

- **What is your organization's responsibility to entities outside your jurisdiction with regard to a wide-scale cyber-attack?**

City of Seattle:

- Post WACIRC Level 2 and 3 incidents to LISTSERV.
- Contact DIS Help Desk for Level 1 incidents.
- Contact King County operations and management.
- Engage Internet Service Providers (ISPs) in incident response.

Gaps requiring clarification:

- To be determined (TBD): relationship with FedCIRC, National Infrastructure Protection Center (NIPC), DHS.
- Suburban cities: utility services.
- Business Partners: regional wholesale water and power customers.
- Regulatory Bodies: Environmental Protection Agency (EPA), Department of Energy (DOE), Federal Energy Regulatory Commission (FERC), North American Electric Reliability Council (NERC), Western Electricity Coordinating Council (WECC).
- Auditors.

King County:

- Notification and coordination.
- Mitigation of attack traffic.
- Information sharing relative to temporary or permanent solution.

Issues:

- King County needs a policy for inventory of externally facing websites and where they logically reside within our King County network. This will allow us to better mitigate risk.
- King County needs a global security policy relative to DHS conditions.
- Review authorities for threat conditions.
- Cooperation / coordination with Canada.

Washington State DIS:

- Federal:
- Provide for information on suspected illegal activity.
- Communication and notification about incidents that could have national impact or that could be coming from other nations.
- City/County:
- Primary responsibility is notification.
- Cities and counties who have computing assets in DIS environments.
- Neighboring states:
- Currently, no process for providing information. Responsibility as good Net citizens is to notify them that there may be a threat against them.
- Canada:
- Currently, no process for providing information. Responsibility as good Net citizens is to notify them that there may be a threat against them.
- Example in exercise - requested specific network information from British Columbia (BC) to allow us to block the worm coming from the SGN directed toward them. We also notified them that we had blocked traffic.

Washington State DOT:

- Develop information exchange with DIS / WACIRC to coordinate response efforts.
- Notify Public of any impact to any DOT external web sites, traffic cameras, ferry schedules, etc., via PIO release.
- Being a good neighbor and alerting others in "neighborhood."

Washington State EMD:

- Our procedure is to notify our local emergency management facilities of the threat and have them contact DIS for further information regarding the IGN or SGN.

VIGNETTE THREE: WMD FORCE MULTIPLIER

The theme of the final vignette was an overwhelming, coordinated cyber-attack acting as a "force multiplier" for a combined terrorist WMD attack. Issues and actions necessary to re-establish or maintain network operations to permit crisis and consequence management were addressed by the NOCs. In a process similar to the previous sessions, participants received indications of the events leading to significant disruptions to critical networks. Participants then assessed the situation and took necessary actions to re-establish these networks to enable necessary response and governmental operations to continue.

Questions for Plenum

- **What does the DHS "Condition Red" mean to your organization, in particular to its network security?**

City of Seattle:

- Assumes Orange readiness in place, plus…
- Stop all IT changes.
- Mayor declares emergency, activates EOC.
- Take specified actions geared to whether Seattle assessed as a target.
- Deploy a 24x7 NOC.
- IT infrastructure staff scheduled 24x7 for EOC.
- Confirm call-out information and notify all IT staff.
- Notify all IT customers of potential emergency disruption of services.

King County:

- Obtain intelligence.
- Obtain direction from King County High Level Officials.
- Establish POA consistent with King County plans and Policies.
- Posture and respond accordingly.

Washington State DIS:

- Increased security in all buildings.
- Broadcast message to all DIS personnel about heightened state.
- Be extremely vigilant, higher awareness among receptionists to ask for ID.
- Facilities staff should ensure backup generators, etc. are ready to go.
- Network staff would be on heightened awareness, with reinforcement among staff to be aware of their surroundings and people in the area, watch more closely for anomalies in network activity.
- Review logs more carefully and backup systems more frequently.

Washington State DOT:

- Notify all employees of change in threat level.
- Ensure 24-hour access to management team regarding threat level.
- Poll and brief IT emergency response personnel.
- Continuous monitoring for IT infrastructure abnormalities.
- Increase physical security at IT facilities (possible assistance from Law Enforcement / National Guard).
- Ensure operational condition of backup power generators.

Washington State EMD:

- Awareness and monitoring.
- How does this differ from a "normal level" of network security? No difference.
- How does this differ from DHS "Condition Orange"? No difference.
- What extraordinary actions do / might you take under this threat condition? Increase physical security to our network hardware.

- **If a regional NOC undergoes a "catastrophic" loss, what resources might your organization offer to support the NOC's continuity of operations?**

City of Seattle:

- Staff.
- Vendor relationships.

- On-call expertise.
- Diagnostic support.
- Communications support.
- Provide alternative sites for hosting of critical Public Info Web pages and Critical Response and Recovery Applications.

King County:

- Physical location.
- Workstations.
- Network accessibility.
- Personnel.
- Voice communications capabilities.

Washington State DIS:

- DIS could act as a conduit to provide possible network technical staff assistance.
- Possibly provide hardware / software network assistance and a facility (management decision).
- Leverage vendors to get priority delivery for equipment and services, and public information assistance.

Washington State DOT:

- Use of satellite-based internet connection
- Use of 800 MHz radio system

Washington State EMD:

- Talking to vendors and making sure that TWP is being followed.

- **If this loss occurred to your organization what resources might you need and how would you get them?**
  - Satellite Internet connectivity. Purchase dish from a local vendor and activate service.

- **What are your major requirements for a "NOC in a box"?**
  - 24-hour switch, liquid crystal display (LCD) / keyboard, video, mouse (KVM) switch, 1 dual=processor Win2K=based server not to exceed 4U.

- **If yonr organization's networks are degrading gracefully, but rapidly, what are your priorities for system continuity?**

City of Seattle:

- Systems and Infrastructure required to manage IT resources.
- Ports, segments and servers required for Public information and internal coordination of event--e.g., e-mail.
- Utilities: distribute water, provide drainage distribute power, generate /buy / sell power, serve critical customers, bill customers (Supervisory Control and Data Acquisition (SCADA), wholesale B2B links, Out-dialer, Interactive Voice Response (IVR), On-call, geographical information system (GIS) / Asset Management., etc.).
- Public Safety: 800 MHz radio, dispatch, mobile communications, records systems.
- Administration: post payments, pay employees, make purchases, pay vendors.

King County:

- Protect critical applications.
- Communicating with systems and application owners to ensure they implement their business continuity plan.
- Investigate the cause and develop a protection plan.
- Inform the public of the impact.

Issues:

- Policies and procedures do not provide a process to formulate response (e.g., assess, define challenges, and develop response options).
- How to coordinate internal activities?
- How to coordinate external activities?
- Intelligence behind the decision to escalate to Condition Red -- what does it mean to us?

Washington State DIS:

- Keep Access Washington running for the Governor and other government organizations to use as a communication tool to the public - in support of public safety, health, and welfare.
- Work with customer agencies to prioritize and keep network resources up that support emergency services.

Washington State DOT:

- E-mail and phone systems are the most critical support assets for Transportation infrastructure recovery.
- Public internet access can be jettisoned as a means of maintaining internal system integrity (PIO can be employed to establish and maintain public information flow).

Washington State EMD:

- Network hardware (routers, switches, firewalls, IDS, VPN).
- Servers (Domain controllers, Exchange, Dynamic Host Configuration Protocol (DHCP)).
- EOC Workstations (Based on needed pods).
- Printers.

EVACUATION PHASE -- KING COUNTY RESPONSE

As a result of the scenario induced effects, King County was forced to evacuate its downtown facilities with no opportunity to perform maintenance and critical system configuration changes. All employees in the downtown areas evacuated, with critical management personnel assembling to assess the initial consequences and define a course of action to restore services to the employees and the public. Management chose to perform the following:

- Define the situation.
- Identify the major challenges.
- Identify solutions.
- Summarize the impact sustained by this crisis.

The following products were developed:

- **Problems encountered by the crisis**
  - The following facilities were evacuated:
    - Jail
    - County Courthouse
    - All of King Street
    - Key Towers
    - Wells Fargo
    - Exchange
    - Etc.
  - All Core cyber-services abandoned and in an immediate state of decay.
    - Transportation system was affected.
    - Impacts on employees evacuated.
    - Work status is undefined, organization is in disarray.
    - Accounting functions are lost and driven to manual recovery and restoration.

- **Challenges facing King County**

  - Safety of staff.
  - Restoration of essential services poses challenges in the following areas:
  - Restoration of security and infrastructure.
  - PIO (information to employees and public) / critical function restoration / confidence building actions to restore public confidence.
  - Legal challenges and authorities - who will make decisions during the rebuilding process - especially early when many employees are without a workplace?
  - Coordination and Leadership with respect to restoration activities.
  - Prioritization of required actions and activities.
  - Human Resources.

- **Solutions**

  - Evaluate and assess facilities and capabilities.
  - Contract / define alternative facilities - some are defined in plans (work through Property Management).
  - Establish initial network connectivity (including home connections).
  - Develop work plans and assignments.
  - Develop plans to communicate to internal and external audiences.
  - Organize internal and external agencies.
  - Coordinate with other agencies.

- **Impact of the Crisis / Evacuation**

  - In a week
    - Few lost or essential services will be restored. System is in a state of decay.
    - 911 will have been rerouted.
    - Buses are running.
    - Sewage treatment is operating.

- Payroll is questionable - a stop-gap manual method at best will be in operation.
- Human resources will be strapped.
- Court system is not operational.
- Public safety and confidence in disarray.

➢ In a month

- No significant improvement in the Data Processing System.
- Limited improvement in the other systems.
- Automatic funds transfer payroll is still a problem - in manual mode.

It was assessed the County services would take four to six (4-6) months to be fully restored.

TOPOFFs Questions during Vignette Three

- **What does DHS "Condition Red" mean to your collective organizations?**
  - How might you coordinate your cyber-security operations in this threat condition?

- **What are the most critical elements of your IT infrastructure?**
  - If your organization's networks are degrading gracefully, but rapidly, what are your priorities for system continuity and restoration?

- **In the event of a wide-scale cyber-attack that disrupts significant portions of your critical infrastructure, from a cyber perspective, what are the essential elements of information that TOPOFFs need?**
  - How do you get this information?

- **How do you regain and maintain public confidence that government organizations can respond and provide for adequate security to critical infrastructures, particularly the IT infrastructure?**

The major findings for the top officials are as follows:

- There are corollaries between a physical attack and cyber-attacks as to the impact on the continuity of operations of governments and their agencies. The ability to react to a physical attack or natural disaster has appropriate processes in place with the role of the Federal government understood by the State and Local governments, this is not true when there is a cyber-attack.

- The ability to maintain IT infrastructure is predicated on the fact that individuals will be able to get to their workspace. In those instances where this is not true, the impact on the IT infrastructure of the various government agencies varied as to their ability to do backups and to access their systems from alternate locations.

- During the pre-exercise period, the Federal government was changing its official way of responding to cyber-attacks through the standing up of DHS and its assimilation of a number of organizations with cyber-responsibilities. The attempt by the Federal government is to develop an integrated cyber-response capable of many tasks to include support

to both State and Local governments. There is still a need for a single point of contact within the Federal government for the dissemination of information related to cyber-attacks to the State and Local governments.

During Vignette 3, TOPOFFs received a phone call from the Office of the Secretary of DHS. In the phone call, he asked participants to provide an update to him on the status of the situation and any assistance they may need. The following is their response:

THIS IS AN EXERCISE

This is in reply to your faxed questions of DTG xxxx May 7, 2003. (TOPOFF2 Exercise Messages)

1. We are experiencing several denial of service interruptions over several of our networks most are tapering off, many Websites have been defaced and Hackers have attempted to add additional confusion and delay first responder actions through a misinformation campaign over official government sites. King County NOC a key information node has been evacuated and is in the process of determining how to restore services since no backup facility exists.

2. While the cyber-attack has not affected 1st Responder's ability to attend to the WMD incident, there has been disruption of our ability to respond to other effected populations; hut on a limited basis, we are working through these issues. Our concern is what information being broadcasted to the general public through media outlets.

3. We have our FEMA LNO at the State EOC, and have sent our LNO to the DOJ JOC, DOE FERMAC assistance is inhound for plume definition and advise local medical responders to treat contamination individuals. FBI is conducting an investigation into the attacks. Alternate communications were established with NCS using SHARES.

4. We need you to provide resources to assist in the rapid restoration of the jurisdictions networks. A unique, single, federal response cell is needed to assist in the coordination of restoration of our communication and information networks.

HOT WASH-UP

The Hot Wash-up concludes the interactive portion of this exercise. Each group presents the significant and unresolved planning and management concerns, critical issues, and recommendations identified in each session. As part of this activity a moderated discussion among participants will occur. The outcomes of this plenary session requiring action will be carried forward by respective organizations and will be included in the final report.

- **What are the three most significant insights gained from TOPOFF2 CYBEREX?**

City of Seattle:

- Need a clear prioritization of services, assets, and functions for return to service (business continuity).
- Need a co-located IT management level consequence team for "real."
- Need a working definition of "normal" and thresholds for triggering escalation.
- Ongoing "tug of war" between adding and sustaining services vs. security vs. cost.
- The high-level view of system status is important.

King County:

- Need a review of Policies and Procedures to better reflect activities required under DHS Alert Conditions.
- Must define authorities consistent with Alert Conditions and span of control among King County agencies (Who has precedent?).
- Transfer of authority (How does it occur? How do we identify the need?)

Washington State DIS:

- We affirmed that our incident response plans and processes are effective.

- Communications capabilities, having them and using them, are a key to success.
- Learning how other organizations work in similar situations, and where gaps are in response integration across jurisdictions.

Washington State DOT:

- The complexity of regional IT structures in the Pacific Northwest.
- A greater appreciation for "normal day" services from many different government providers.
- The inter-relationships of all governments providing IT support for public health and safety, and significance of (and risk to) the Washington State DOT DMZ services.

Washington State EMD:

- Coordination between Local, State, and Federal entities is critical.
- Redundancies in systems and networks are needed, to include "Hot" or "Warm" sites.
- Normal security measures need to be at their highest level.

- **What are the three most important recommendations we intend to take home?**

City of Seattle:

- Bring Incident Command System (ICS) to cyber-response: NOC, Management CIRT team.
- Need the system-wide network management view / map complete with a network segmentation plan.
- Need web site redundancy, hackup, and redirection.
- Need a redundant NOC.

King County:

- Review Plans and Procedures to reflect observations from this exercise.

- Develop procedures for an integrated cyber and physical approach to security (remembering that there is a physical element to cyber protection).
- Develop procedures for physical relocation and restoration of services.

Washington State DIS:

- Develop backup or alternate methods for obtaining information when primary resources are compromised.
- We want to work on solidifying our regional notification and response strategy for cyber events.
- We want to review our own processes for upper management notification and issue escalation during incidents.

Washington State DOT:

- Continue established relationships and maintain current contact information, especially fax numbers.
- Define regional IT standard actions for each threat condition (THREATCON) level, publish guidance and keep current.
- Share RIIG information with Washington State DOT directly.

Washington State EMD:

- Revisit restoration plans and priorities, both TSP and internally.
- Refine plans for IT COG with government and industry.
- Assist in all efforts to improve the coordination between the IT and Emergency Management communities at all levels, industry, Local, State, and Federal.

- **What is the most significant operational cyber-security question that we still need an answer to?**

City of Seattle:

- What is our dependency on external cyber-nodes?

- Where is the money coming from?

King County:

- How do we elevate the priority of cyber-security at levels above operations to defend against the growing threat?

Washington State DIS:

- How, when, what…. gets conveyed to the Federal level during such incidents? And to whom?

Washington State DOT:

- What is clear-cut definite authority needed in an emergency to decide when to do the following:
- Employ internet filters, block external ports.
- Take down external servers.
- Hardening of internal devices and isolating internal routers.
- How do we prioritize services / systems capahilities in a changing emergency environment?
- Is there a basic protocol?
- Will "best judgment" guidance be used?

Washington State EMD:

- Improving, improving, improving… Takes everyone sharing information.

State of Washington Department of Information Services

TOPOFF2 CYBEREX Review and Assessment

Introduction

On May 6-7, 2003 the Washington Department of Information Services (DIS) participated in the TOPOFF2 Cyber Exercise (T2 CYBEREX) at Camp Murray. Funded by the National Institute of Justice and designed and executed by Dartmouth's Institute for Security Technology Studies (ISTS), the T2 CYBEREX was conceived to test local, state, and federal response capabilities in the event of a coordinated physical and cyber-attack. While the CYBEREX was conducted separate from the federal TOPOFF2 initiative, it referenced the same physical event as the main exercise – using the cyber-attack as a force multiplier.

Participants in the T2 CYBEREX included DIS, the City of Seattle, King County, Washington Department of Transportation, and the Washington Emergency Management Department. Support resources from commercial and federal entities were also included in the exercise.

The primary focus of the T2 CYBEREX was to test, "The ability to respond to the challenges posed by anticipated and unanticipated disruptions of government-related information networks due to a large-scale cyber-attack within the framework of a WMD event will address the requirement for increasing complexity." According to documents prepared by the exercise developers, the exercise scenarios were focused on helping the participants evaluate the following:

- The effectiveness of the various cyber-security plans, policies and procedures of the City, County, State, and Federal levels to adequately address issues and support the response for a large-scale cyber-attack on government-related information networks.
- The ability of participating network operations centers to organizationally integrate and effectively conduct or manage a sustained response to a cyber-attack.
- The planned flow of communications and information in an operational context.
- The decision and coordination processes in a range of potential consequences.

The specific objective of the Department of Information Services was to "Determine that WACIRC procedures - including incident reporting, response, escalation, communications, containment, etc. -are sufficient to effectively mitigate the effects of cyber-attacks."

Issues/Observations

Because the exercise involved the use of a simulated network environment, simulated support services, and narrowly controlled communications vehicles (single terminal for all email, listserv, and telephone communications), the primary focus of the DIS Team evaluation was on the following:

- How decisions were made
- Clear and measurable escalation policies
- How do we interact internally (DIS Incident Response Team to DIS Management)? [Internal Interaction]
- How do we interact externally (DIS to state agencies and regional partners)? [External Interaction]
- Use of available resources

An overall assessment of the performance of the policies and practices of the DIS Computer Security Incident Response Team (DIS CSIRT) and the related Washington Computer Incident Response Center (WACIRC) processes indicates that the significant work done in developing and implementing these programs has paid great dividends. The DIS CSIRT team worked effectively in developing and implementing response activities as well as coordinating effective communications to impacted parties. This was clearly a result of sound and tested processes combined with quality, well-trained personnel.

While no key processes were absent, DIS understands that the key to an effective incident response process is to engage in continuous process improvement. To that end, the DIS team used the T2 CYBEREX to identify areas that would benefit from further assessment and process improvement activities.

The identified issues/observations include:

1. **Improved categorization of incident severity levels**

- Define distinct communication processes for all DIS CSIRT Severity Levels (SL1, SL2, SL3).
- Determine criteria for declaring SL1 when multiple agencies are effected.
- Define metrics for declaring SL1/SL2/SL3 and security incident.
- Determine if there is benefit in mapping the DIS CSIRT Severity Levels more closely with the color-coded federal kinetic alert indicator model to enable better communication on a federal level.
- Investigate feasibility of using the multi-state ISAC cyber-alert indicator model, which maps to the federal kinetic alert indicator model.

2. **Improved management communication and engagement**

- Refine the processes by which high priority security incidents are elevated to DIS management, specifically to address:
  - Specific procedures for communication with DIS Management, DIS Director, and the Governor's office, during a security incident.
  - The process and criteria for notifying DIS management of specific impact to DIS services.
- Establish a DIS CSIRT "management" liaison for communication with DIS Executive Management during a security incident.

3. **Improved customer communications**

- Review process for notifying customers of impact to DIS services (WA-STATE-NOTIFICATION listserv). Include marketing the listserv, and security process training.
- Review and adjust the current backed web site process to include determination of whether DIS hosts the compromised customer agency site or the customer hosts the compromised site and the communication process for both DIS-hosted and customer-hosted sites.

4. **Improved regional communications**

- Define the process for communicating to PIOs @ City of Seattle and King County during a security incident.
- Pursue the use of the Regional Incident Intelligence Gathering (RIIG) listserv with regional partners.

5. **Improved "public" communication**

- Define what information is released when a state web site has been defaced.
- Define WACIRC/DIS CSIRT roles in disseminating information when non-network, non-state related major event occurs (RDD, 9-11, threat level RED).

6. Improved use of external resources

- Obtain "preferred" status (sign up for alerts/early warning) for DIS with CERT.
- Who/How/When to notify "Feds" or in getting information, or securing any additional resources.
- Develop "hack up" or alternative methods for obtaining and validating information when primary resources are compromised (i.e., commercial web sites, Internet access, private security resources, telephones, etc.).

7. Improved response procedures

- Review and document process and procedures to quarantine a potentially compromised device (Who? How? What procedure and under what authority) WACIRC recently adopted "WACIRC Law Enforcement Guidelines for Reporting and Responding to Computer Crimes.
- Revise web page defacement incident response procedure to include check for DIS hosting.
- Document the procedure for notifying DIS IT when Access WA link must be removed or restored.
- Obtain Law Enforcement notification process and procedures for state agency web page defacement. (See WACIRC Law Enforcement Guidelines for Reporting and Responding to Computer Crimes).
- Add full set of all DIS contact numbers to Incident Response Handbooks.
- Define the process, procedure, and actions taken for the DIS CSIRTeam and cyber incident response, should the US move to "threat level" RED.
- Review DIS Disaster Recovery Plan for node sites impacts and communications during "physical" events.
- Define DIS CSIRT involvement in combined Cyber/Physical incidents.
- Develop process and procedure for responding to a security incident of exceptional long duration. (i.e. 24 hour staffing, staff relief or rotation, home/family staff needs, site evacuations, etc.).

Resulting Actions

Under the direction of the DIS CSIRT Coordinating Team, actions are already under way to address the issues identified during the T2 CYBEREX. The following is a summary of some of the current activities:

- A DIS CSIRT Severity Level Evaluation Subcommittee has been formed to address incident severity categorization issues
- DIS Communications personnel assigned to the DIS CSIRT team have initiated the develop and documentation of updated communications procedures and will provide appropriate training to DIS CSIRT personnel

- All of the identified issues have been assigned to a recommended lead resource(s) and oversight of the issues has become a regular part of the DIS CSIRT management process.
- A draft "Rules of Operation" for the proposed Regional Incident Intelligence Gathering (RIIG) Listserv has been prepared. Planning is underway to engage the regional T2 CYBEREXparticipants in finalizing the "Rules of Operation" and initiating a pilot operation of the RIIG listserv.

Conclusion

It is the collective opinion of the those DIS personnel who were involved in the T2 CYBEREXthat the investment of time and resources in exercise participation resulted in significant value in both the confirmation and potential improvement of incident response communications processes and the benefit of expanding the boundaries outside of state government to city and county government organizations as well as our private industry partners. The DIS CSIRT team and WACIRC participants look forward to addressing these issues in a continuous effort to provide the best possible environment to protect the information assets of the State of Washington.

King County Perspective of TOPOFF2 Cyberex.

Purpose

This document is King County's preliminary after-action-report (AAR) for the exercise. The point of contact for comments and updates to this report is (b)(6) in the Information and Telecommunications Services Division of the Department of Executive Services.

Exercise Participants

The Top Officials 2 Cyber-Terrorism Exercise (TOPOFF2 CYBEREX) was conducted at the Washington State Emergency Operations Center on May 6-7 2003. An orientation session for some of the key participants was held on May 5th. TOPOFF2 CYBEREX was designed and controlled by the Institute for Security Technology Studies (ISTS) of Dartmouth College. Primary exercise participants included the City of Seattle, King County (DES (ITS), KCSO, DNRP, DoT (Transit)), and the State of Washington Department of Information Services (DIS), Emergency Management (EMD) and Transportation (DOT). In addition, a group of senior managers from each public agency served in the role of "Top Officials." For King County, this included DES (ITS and OEM), KCSO, and PAO. Representatives from the University of Washington, Microsoft, Boeing, Qwest, the U.S. Secret Service (representing the Seattle Joint Task Anti-Terrorism Task Force - FBI, USSS, US Attorney's Office), and the National Communications Systems (representing the Department of Homeland Security) were present, serving as a support pod during the exercise.

Exercise Overview

The exercise occurred in three scenarios or vignettes: (1) normal day at the office, with "normal" network and computer problems; (2) an escalating series of events - computer

and network problems which might be preliminary symptoms of a directed cyber-attack; and (3) a major cyber-attack on participants' computer networks, coupled with a weapons of mass destruct (WMD) attack – a radioactive detonation device (RDD) terrorist bomb exploding in Seattle.

Exercise Play

The CYBEREX was computer-assisted. Each participant group or "pod", the controller functions and the support pod had computer terminals to use for communication with each other. In this fashion the communications between functions (communications normally conducted via telephone, fax, pager and e-mail) were captured for later analysis. In addition, ISTS developed a simulated network for each agency. This network was represented on a network map displayed on computer terminals, and included functions such as end-user computers, network switches, firewalls, e-mail servers, application servers (applications such as computer-aided dispatch systems or world-wide-web sites), and the networks linking such devices and linking agencies with each other and with the Internet. A series of injects occurred during the exercise. These events included, for example, failure of network switches or applications, failure of electronic mail, overloading of devices or firewalls by a flood of traffic (a "denial of service" attack), defacing or "hijacking" an agency's website – placing false information on the site to incite public panic; and physical evacuation of key buildings. But the CYBEREX play was mainly about team working relationships. In response to each event, the participants' teams – both technical teams and management teams – had to determine and implement a technical response to the event, and a management or top officials' response to the event.

Injects (For reasons of confidentiality, this is not a complete list)

- Computer virus attack.
- "Worm" propagated via the Internet (A "worm" is a malicious computer program which exploits a specific vulnerability in commercially available software. Worms usually have payloads intended to cripple computer systems or networks.).
- Defacing or "hijacking" a government web site (intent: provide misinformation to the public).

- Cyber-attack on government computer systems coincident with a physical or kinetic attack, e.g. weapon of mass destruction.
- Attack by rogue computer programmer or team intended to breach, commandeer or compromise a key governmental computer system or network.

Vulnerabilities (For reasons of confidentiality, specific vulnerabilities are not listed here.)

What Worked

- An ad-hoc IT management team assembled specifically for this event made key decisions which prevented compromise of some key systems and networks, reducing the effect of the attacks on the simulated county government network.
- We have a large amount of redundancy in our existing IT infrastructure which is quite useful when the primary systems fail or are attacked.
- Collaboration with the City of Seattle and Washington State agencies proved very valuable. The preliminary workshops leading up to the CYBEREX were of good value and well attended. The ability to identify peers with similar interest.

Lessons Learned

- The County's siloed culture is a strong inhibitor to an effective inter-agency response. A major cyber-incident or even our response to a major natural disaster is likely to require a coordinated effort, at least for the departments with major IT resources and dependencies. If we daily work in a siloed environment, that is the way we are likely to respond in a major disaster.
- The cyber-environment is becoming more difficult to assess. We do not completely understand a "normal" day. Normal days are filled with many small cyber-incidents, computer and network problems which may or may not be indicative of looming larger issues. Related to this is our need to promote more peer to peer exchanges of information to help with the early detection of a potential major incident.
- Physical co-location of the team during a cyber-event vastly speeds decision-making and actions to counteract attacks. The Network Operations Center (NOC) we simulated for the CYBEREX is analogous to the EOC activated during disasters. While we have facilities at the Key Tower that could support inter-agency NOC activities during a major incident, we have no fall-back facility if we lost the Key Tower.
- Having an integrated team (staff responding to actual cyber-incident as well as staff supporting IT management response) was not effective. It was too easy to focus on the details of some of the technical issues and miss management issues that also needed attention.
- No participating government agency (and perhaps few or no private firms) fully understand our dependence on external cyber-nodes – places where private telecommunications networks meet and interconnect.

Recommendations

- The County needs to more formally prioritize its business functions and, then, the related information technology services, assets and functions for return to service during disasters in general and cyber-attacks in particular (in order to maintain continuity of government and public confidence in government).
- The County should create a formal inter-agency incident response team that includes representatives who have real skin in the game. Having every County agency involved will not be effective. It is recommended that we explore a bifurcated structure with a group responsible for responding to the technology related aspects of the incident and another group responsible for supporting the management decisions and interagency communications. The efforts of the two should be closely coordinated with the former receiving direction from the latter.
- Existing response plans (e.g. ITS' Cyber Incident Response Plan, OEM's Homeland Security Plan) need broader distribution and vetting.
- Network segmentation plans – plans to purposefully break apart the County's internal network to protect key systems and functions – need to be more formal and more practiced.
- Interactive, computer-based, network views or maps, if created and maintained, greatly improve understanding of an event and our ability to react to it, in the same way GIS (geographical information system) maps are useful in understanding and responding to any disaster.

City of Seattle Perspective of TOPOFF2 Cyberex.

What Worked?

- The established City of Seattle technical incident response team (called the Internet Infrastructure Team (IIT) worked well together using established procedures to counteract many of the injects or events.
- An ad-hoc IT management team assembled specifically for this event made key decisions which prevented compromise of some key systems and networks, reducing the effect of the attacks on the simulated City government network.
- We have a large amount of redundancy (alternative paths or systems) in our existing IT networks which are quite useful when the primary systems fail or are attacked.

Lessons Learned

- We do not completely understand a "normal" day. Normal days are filled with many small cyber-incidents, computer and network problems, which may or may not be indicative of looming larger issues.
- Physical co-location of the team during a cyber-event (preferably in a City government NOC) vastly speeds decision-making and actions to counteract attacks. This NOC is analogous to the EOC activated by large public agencies during disasters.
- ICS can be formally applied to information technology (IT) teams responding to cyber-attacks.
- No participating government agency (and perhaps few or no private firms) fully understands our dependence on external cyber-nodes, those places where private telecommunications networks meet and interconnect.

Recommendations

- The City needs to more formally prioritize its business functions and, then, the related information technology services, assets and functions for return to service during disasters in general and cyber-attacks in particular (in order to maintain continuity of government and public confidence in government).
- The ad-hoc IT management team should be formally established and trained to make decisions during cyber-events.
- Interactive, computer-based, network views or maps, if created and maintained, greatly improve understanding of an event and our ability to react to it, in the same way GIS maps are useful in understanding and responding to any disaster.

SECTION EIGHT

OBSERVATIONS

The following comments are based on player observations during the TOPOFF 2 CYBEREX.

NETWORK FORENSICS

In analysis of the "problems" witnessed, players relied heavily on normal diagnostic equipment that showed only aggregate (i.e. combined in & out) traffic rates, and simple indicators (e.g., green / yellow / red / black) about server status. This is typical of network management software, so this in and of itself is not a negative thing. During an actual attack, however, this does not provide enough information to allow a rapid response and reaction (part of their behavior may have been a side-effect of using the simulation, which is less detailed than the tools they are used to using).

In some cases, players asked more detailed questions from network provider support staff, but the standard modus operandi (MO) of typical regional network providers (and of the Northwest GigaPOP (Point of Presence) is not to do detailed traffic capture and analysis as a matter of normal policy and procedure to assist in incident response. This means that customers of large Internet Service Providers (ISPs) and GigaPOPs should have their own capability for network traffic capture and analysis. It is not know if this is typically something that GigaPOP customers know about and take into their own hands.

Further more, at the GigaPOP level, fine grained filtering on traffic based on classless inter-domain routing (CIDR) blocks or specific Internet Protocol (IP) addresses, or rate limiting of any type, is not a normally provided service. Bandwidth utilization is so great and the design of the network so optimized for speed and ease of management, that such services are simply not available or are not used in fear of affecting network availability or performance. Customers want to avoid blocking traffic using access control lists (ACLs) on their routers, to save router computer processing unit (CPU) cycles (and ingress interfaces on

a distributed denial of service (DDoS) victim's network are not the place to deal with a massive bandwidth consumption attack anyway). The upstream provider doesn't want to use ACLs on their routers, or rate limiting features, to save their router CPU cycles. Network operations will only provide all-or-nothing filters based on routing tables that leave customer networks either wide open or fully disconnected. This was the response that the Support cell gave to requests to block attack traffic to Canada in Scenario 2, and block Port 80 traffic in the face of a zero-day worm. (In the case of the first days of the Slammer worm, the Northwest GigaPOP did, for the first time, block all traffic to / from the affected user datagram protocol (UDP) port, but moved as quickly as possible to try to remove these filters).

Instrumentation in the network infrastructure that gives detailed information about traffic flows, in a form that can he easily provided to customers and shared in venues like Information Sharing and Analysis Centers (ISACs), and policies and procedures that supported network traffic capture and analysis, would greatly speed up incident response, especially in multi-site attack scenarios, such as Scenarios 2 and 3 in TOPOFF2. These services are not currently provided for many reasons, some of which are technical, some financial, and some political. As there is currently no significant demand for such services, or regulation requiring them, network providers are not voluntarily designing them into their networks.

HOST BASED FORENSICS

If one or more systems are found to actually be under attack (or involved as stepping stones in an attack) the contents of those systems' hard drives are critical evidence. During the exercise, the City team contacted Microsoft and the Computer Emergency Response Team (CERT) when an inject came confirming one of their systems was flooding a site in Canada. Microsoft requested the City provide the system to them to analyze, which the City agreed to. At that point, the City asked for assistance from the University of Washington (UW), but with the system physically in the possession of Microsoft, and no image copy of the drive made prior to handing it over to Microsoft, there was no way to independently

analyze the system (or to verify the integrity of the system) from that point on. Had this been an incident that involved law enforcement action, this could compromise an investigation. Had this been a real attack, the lack of initial recognition of the significance of the attack and the proper handling of potentially valuable evidence could have also delayed the response.

RESPONSE TO DENIAL OF SERVICE ATTACK

While handling the radiological dispersal device (RDD) force-multiplier attacks on web services of the City and State, players tended to not focus on the actual traffic going to / from affected servers, and in several cases their action was to ask for the systems to be taken out of service (which effectively accomplished a DoS as effective as the attackers were attempting). Given that they have little support to analyze traffic, and no option to rate limit traffic or block to / from specific IP addresses or CIDR blocks, there aren't many other options in the face of a concerted attack. This is a vulnerability that directly creates a situation where it will be impossible to guarantee 24x7 publicly available network based services (even though the general public may expect 100% availability).

Earlier, in the web server worm inject, players also used patching / rebooting and disabling of servers, to respond. The lack of detailed network traffic analysis capabilities (or perhaps just flow direction data in the simulation) made it so players could not accurately determine if their actions had in fact solved the problems or not. In one case, a player had asked for ports to be blocked by the network provider (whose reply that they would not honor that request was missed). Just after this, the attacker stopped the attack (which had the same effect of lowering the traffic line on the network graph), so the player thought the blocks had been put in place. When the attacker restarted the attack a short while later, the player (thinking the blocks *were* in place) could not tell if the worm had re-infected the server or if the server was attacking another site with outbound traffic. (A common theme was not asking "what traffic is flowing on my network and in which direction?" but instead asking "is the status green / yellow / red / black" and "how much traffic is flowing?") Without more detailed analysis tools and procedures in the simulation software, the players

found defense against a concerted attack extremely difficult. Again, this was an artifact of the exercise.

Responding to a DoS attack by blocking traffic based on black-listing specific IP addresses, ports, even blocking an entire protocol, can be easily defeated by shifting the attack methods. This means the most effective defenses against a bandwidth consumption or resource consumption attack will be rate limiting or white-listing to allow only a subset of known "good" traffic to get to a host / network. As was discussed earlier, however, these defenses are not available to the players from their upstream provider.

Domain Name Server (DNS) Cache Poisoning Attack

The DNS cache poisoning attack on the City of Seattle's servers redirecting them to a UW system could have had longer term effects because DNS time to live (TTL) values are set to long (in terms of response - typically 24 hours) values. Again, there would he little help provided in a normal situation from the Northwest GigaPOP (and perhaps not from commercial providers either, if the City uses any other providers.)

Information Sharing and Analysis

At the point in the exercise where teams knew they were attacked, there was no venue for them to disseminate information to other agencies above and below them regarding the attack. There is currently no state or regional ISAC, or other incident response related communication venue. All teams rely on the same network providers, but even at this level there is no means or policy for dissemination of information regarding an attack. Players had to ask the support cell if the same kind of traffic was being seen by other players. There was no regular status or warning service to push information out to, with the exception of CERT's standard advisories (even in the case of the Slammer worm, Washington State DIS, King County, the City of Seattle, and the Northwest GigaPOP did not voluntarily contact or share information among themselves. It was only when individuals took it upon themselves to make contact that communication in occurred). A new Research and Education Network

ISAC is now in place, but the Northwest GigaPOP and UW are currently not members of this ISAC.

SECTION NINE

RECOMMENDATIONS FOR TOPOFF 3

1. **Campaign-level cyber-attacks and attackers pay no attention to international borders.** These types of potential attacks are of most concern to members of the National Security Council and Homeland Security Council. The policy decisions related to attribution to a particular nation-state or equivalent adversary, and the practice of operational and strategic-level decision-making related to crisis coordination and consequence management between international stakeholders in government and private industry (including large multi-nationals) are critical areas that require further investigation and practice within an exercise environment. These will be examined a very basic level in Livewire; they are important enough issues to merit further advancement within TOPOFF.

2. **Integrate physical attacks and consequence/crisis management with the consequences of the loss of critical information infrastructure.** Either engage operational managers of first responders in the cyber-exercise so that they could provide improved feedback as to the impact of the loss of critical IT services, or engage IT service providers in the physical side of the exercise.

3. **TOPOFF 3 should be expanded to include multiple venues in the exercise.** Given the ability to distribute the exercise to many locations, we would suggest engaging multiple venues simultaneously.

4. **The federal sector should be even more engaged.** Although the federal sector fully supported TOPOFF 2, we feel that due to the changing responsibilities in the cyber arena with the standup of DHS, it is important to include as many federal entities as possible in cyber play planned for TOPOFF 3. This would include the Department of Defense and possibly even include simulated attacks against the non-military networks of consequence management agencies such as FEMA, the CDC, and the private sector players such as the Red Cross.

5. **Start early.** Exercises are new to IT departments. Police and fire have been doing them for years, but not IT departments. It takes a long time to bring them up to speed and explain what an exercise is, and what it is not. It is definitely not a vulnerability assessment, as many think. It takes time to build trust and understanding among the stakeholders. Each player needs to understand that the risk of failure is low, that they are not being graded or exposed to undue business risk, and that there is justifiable business value in improving their response capability through inter-organizational coordination and resource sharing. It also takes time to organize meaningful seminars.

APPENDIX A

PROBLEM CHAINS

1. Background/Normal Activity:

These injects will be run-of-the-mill challenges that the network operators are accustomed to dealing with on a daily basis. There is no terrorist motivation for these injects, and they are largely unrelated to one another.

Equipment failures will affect all domains. Routers to city utilities and county metro transit will die. A router that connects state DOT to State DIS will die. A cable to the city PD will be cut. The email server at EMD will die.

Probing surges will periodically occur on all domains.

A wave of Spam will hit everyone.

Software vulnerabilities will be identified by CERT. Patches will be made available by Microsoft. The players can choose to be proactive or lazy in their response.

A Klez-like worm will spread an email message (spoofed from (b)(6) recommending lax security and containing insulting language.

2. The Super Flood (Code Red III) coincident with the WMD

This problem chain will be much like the Code Red worms in that it will exploit a vulnerability in a popular web server software application (IIS), scan for other vulnerable hosts, and then attack a series of government domains. It will also be a near zero-day exploit in that the vulnerability will be announced by CERT the day that the worm starts spreading (vignette2). Initial probes for vulnerable versions of the software on port 80 will be largely undetected in the normal volume of web traffic. Infected machines are both inside and outside of the stakeholder networks. The worm itself will be released in vignette 2, scanning for 15 minutes before going dormant. The malicious part of the worm will sleep for several hours before waking up to contact a master machine (overseas) for attack instructions. This could be done via a normal http get request. The master will provide the infected machines with a list of 50 IP addresses to attack which will be spread over the City, County, and State domains. The attack instructions will also specify how long to attack, and when to contact the master again for further instructions.

Several machines inside the City, County, and State will be infected, so that the attacks will be coming from both inside and outside. We may reward aggressive patchers by minimizing the internal infections in domains that aggressively patched after the CERT warning.

The attack mode will be modeled loosely after the Trinoo network of DDOS zombies. The malicious code will spawn 50 threads, each one dedicated to attacking a different host. The attack packets themselves will be randomized TCP syn packets and UDP packets of different size on destined for different ports, some containing text such as DIE_AMERICA. The attack will be timed to coincide with the physical terrorist event in the City. The net effect will be a paralyzing DDOS that will last at least 1 hour.

3. Destructive worm combines Slammer and Magistr Virus/Worm

A scanning worm exploits a vulnerability in MS_SQLbuffer overflow vulnerability. It will scan for other hosts listening on port 1433. After scanning for 10 minutes it will activate the malicious payload which will

- Erase CMOS on some hosts
- Erase the Flash BIOS on some hosts
- Overwrite every 25th file with the text "We Win-America Loses" as many times as it will fit in the file
- Delete every other file
- Overwrite a sector of the first hard disk

This will destroy the machines and require either factory reconditioning or new machines along with installing complete backups.

4. Anti-American sympathizers deface web pages

Due to world events, anti-American sympathizers work to sow confusion in two waves. The first wave will be attacks on actual web servers in the DMZ of the various domains. The second wave will be a DNS poisoning situation where web sites all over the country (including City ,County, and State) will be re-directed to a domain at a university which will contain more anti-American propaganda.

5. Non-terrorist Criminal Forensic Activity

Various King County computers are noted by law enforcement as trying to break into a database holding credit card information. The computer is actually under control of a remote host, but the software to do its nefarious deeds was somehow installed on the computer. Law enforcement shows up and is asking about a computer which was logged on some time ago using DHCP and so the logs have to be consulted to go from DHCP address to MAC address and identify the specific computer. Sometimes the logs are on backup tapes. Sometimes they are gone because it is too long ago.

Seattle has a threatening e-mail to the President and the Attorney General. Dennis will construct header portion to give to USSS to use when they show up at the door. The header information will show that it came from a wireless device at

Seattle City and Light, and again, DHCP logs will have to be traced to find out the source, if they have been preserved long enought.

RIAA sends strong letters from their attorney to the Attorney General of the State threatening to take legal action if the State does not stop their employees from downloading MP3 files. This is directed at DIS, EMD, and DOT.

A federal law enforcement agent will go to each of the player cells to discuss these issues for about 30 minutes.

6. Logic bomb engages in cross-border game play (desktop Trojan)

An email containing a suspicious attachment and several web links will be sent to multiple recipients on every domain. The email will have news about a new security vulnerability, and recommend that the user download a patch or open the attachment. The attachment will contain a malicious payload that installs a timed logic bomb. The links appear to be to Microsoft, but they are redirected to a malicious gopher server will likewise infect anyone using Microsoft IE. The infected users will become unwitting attack agents for a timed DDOS against a domain in British Columbia. The attack target and time are hard-coded, but a machine in the City with a bad clock will start its attack hours too soon, tipping off a smart sys admin that the machine is infected. A local expert will be called in to look at the problem. After a memory dump and some code analysis, he or she will determine that the attack will take place in several hours, and realize that potentially hundreds or thousands of zombies are waiting for the appointed time. He will have to notify the appropriate American and Canadian officials to mitigate the attack. The attack will not actually occur as this problem chain is designed to exercise the various fan out procedures.

7. DHSS Threat level escalation from Yellow through Red

The exercise will begin at condition Yellow. The level will be raised to Orange by DHS when the possibility of a bio-terror event elsewhere in the country emerges. The players will be notified by the VNN news network (power point slides) or by email from "appropriate authorities".

The level will be raised from Orange to Red when the physical terrorist event occurs in the City. The offices of the County will be evacuated, including the County NOC.

Workers hear about it and log on to VNN to find out more. This loads the newtworks to some degree. Terrorists detonate a Radioactive Dispersal Device (RDD) in the flats area south of downtown. The wind is

blowing north. As events unfold, the first responders determine there is radioactivity at the site, and are concerned over how much and how far it may have spread. The reason for the evacuation of county offices and not city offices is that different officials receive different inputs and also respond to the same inputs differently.

Appendix B

Master Event Scenario Listing (MESL)

Vign.	Start	Inject Nature	Prob Chain	Injector	Stimulated
1	0:03	Port scans within expected range in daily report by County Net Admin	1	Network Admin-County	COUNTY
1	0:04	Router (CityLightR) to Seattle Public Utilities fails	1	Senior Network Controller	CITY
1	0:04	EMD e-mail server (StEMDEmail)dies	1	Senior Network Controller	STATE EMD
1	0:05	Router (County_TransitR) to King County Metro Transit fails	1	Senior Network Controller	COUNTY
1	0:05	EMD NetAdmin reports EMD e-mail server has died	1	Network Admin-State EMD	STATE EMD
1	0:05	Port scans within expected range in daily report by City Net Admin	1	Network Admin-City	CITY
1	0:06	City Police Dept writes e-mail complaining of loss of router	1	Help Desk	CITY
1	0:10	Port scans within expected range in daily report by EMD Net Admin	1	Network Admin-State EMD	STATE EMD
1	0:10	Port scans within expected range in daily report by DIS Net Admin	1	Network Admin-State DIS	STATE DIS
1	0:10	Port scans within expected range in daily report by DOT Net Admin	1	Network Admin-State DOT	STATE DOT
1	0:12	CERT sends e-mail about urgent Security patch - Microsoft Windows	5	CERT rep	STATE EMD
1	0:13	EMD help desk reports that users are reporting they have received an e-mail purporting to be from Microsoft with a clickable link to download a critical patch. Users want to know if they should do this.	12	Help Desk	STATE EMD
1	0:14	CERT sends e-mail about urgent Security patch - Microsoft Windows, mentions relationship to past scanning activities	5	CERT rep	CITY
1	0:14	CERT sends e-mail about urgent Security patch - Microsoft Windows	5	CERT rep	STATE DOT
1	0:14	CERT sends e-mail about urgent Security patch - Microsoft Windows, mentions relationship to past scanning activities	5	CERT rep	COUNTY
1	0:15	DOT help desk reports that users are reporting they have received an e-mail purporting to be from Microsoft with a clickable link to download a critical patch. Users want to know if they should do this.	12	Help Desk	STATE DOT
1	0:15	CERT sends e-mail about urgent Security patch - Microsoft Windows, mentions relationship to past scanning activities	5	CERT rep	STATE DIS
1	0:16	DIS help desk reports that users are reporting they have received an e-mail purporting to be from Microsoft with a clickable link to download a critical patch. Users want to know if they should do this.	12	Help Desk	STATE DIS
1	0:17	King County help desk reports that users are reporting they have received an e-mail purporting to be from Microsoft with a clickable link to download a critical patch. Users want to know if they should do this.	12	Help Desk	COUNTY
1	0:18	EMD e-mail server is restored	1	Senior Network Controller	STATE EMD
1	0:18	Seattle DoIT help desk reports that users are reporting they have received an e-mail purporting to be from Microsoft with a clickable link to download a critical patch. Users want to know if they should do this.	12	Help Desk	CITY
1	0:19	EMD e-mail server is rebooted and seems to be fine. Don't know cause	1	Network Admin-State EMD	STATE EMD

1	0:21	County NetAdmin receives e-mail from Microsoft (without PGP signature) telling of urgent security update and directing people to web site to download the patch	12	Network Admin-County	COUNTY
1	0:22	Router to King County Metro Transit restored	1	Senior Network Controller	COUNTY
1	0:23	EMD NetAdmin receives e-mail from Microsoft (without PGP signature)telling of urgent security update and directing people to web site to download the patch	12	Network Admin-State EMD	STATE EMD
1	0:25	Router to SPU restored	1	Senior Network Controller	CITY
1	0:25	County Net Admin reports router plug had been knocked out, now restored	1	Network Admin-County	COUNTY
1	0:26	County Exec has received a media request about the loss of the Metro Transit Website and is concerned that county government networks are weak. Please prepare talking points for County Exex	1	County Executive's Office	COUNTY
1	0:27	Network Admin-router had been accidently unplugged, now restored	1	Senior Network Controller	City
1	0:30	Law enforcement officer comes over to talk about threatening e-mail written to President, e-mail header indicates source is the city network.	11	JTF Rep	CITY
1	0:33	DOT NetAdmin receives e-mail from Microsoft (without PGP signature) telling of urgent security update and directing people to web site to download the patch	12	Network Admin-State DOT	STATE DOT
1	0:34	load from outside internet directed at DOT server (StDot_Data) grows to 95%	1	Senior Network Controller	STATE DOT
1	0:34	e-mail servers (StateEmail) start to bog down with traffic	1	Senior Network Controller	STATE DIS
1	0:34	load from outside internet directed at EMD mail server (StEMDEmail) grows to 95%	1	Senior Network Controller	STATE EMD
1	0:35	help desk e-mails complaints of e-mails from various addresses with newspaper columns concerning war, taxes, environment, religion; some include links to web sites	1	Help Desk	STATE DIS
1	0:35	help desk e-mails complaints of excessive spam	1	Help Desk	STATE EMD
1	0:35	help desk e-mails complaints of excessive spam	1	Help Desk	STATE DOT
1	0:36	Secretary of Transportation has media inquiries about spam e-mail on DOT computers- PIO please respond	1	Secretary of Transportation	STATE DOT
1	0:40	e-mail from EMD Net admin advises of a malicious link-cross site scripting	12	Network Admin-State EMD	STATE EMD
1	0:40	e-mail from DIS Net admin advises of a malicious link-cross site scripting enclosed in e-mails and the possibility of compromised computers	12	Network Admin-State DIS	STATE DIS
1	0:40	Governor has received a call from media asking about Spam on State Accounts- please respond with talking points for Gov.	1	Governor's Office	STATE DIS
1	0:40	e-mail from DOT Net admin advises of a malicious link-cross site scripting	12	Network Admin-State DOT	STATE DOT
1	0:41	Governor has received a media inquiry about virus' in DIS e-mails. Please prepare talking points paper	12	Governor's Office	STATE DIS
1	0:54	load from outside internet drops back to normal due to installation of filters	1	Senior Network Controller	STATE EMD
1	0:56	County NetAdmin determines that the e-mail is not from Microsoft but is a hoax containing a Trojan	12	Network Admin-County	COUNTY
1	0:56	EMD NetAdmin determines that the e-mail is not from Microsoft but is a hoax containing a Trojan	12	Network Admin-State EMD	STATE EMD
1	0:56	DOT NetAdmin determines that the e-mail is not from Microsoft but is a hoax containing a Trojan	12	Network Admin-State DOT	STATE DOT

1	0:58	EMD NetAdmin writes expressing concern that upon reviewing the logs the same Trojan (Microsoft) e-mail has gone to most other users on the system	12	Network Admin-State EMD	STATE EMD
1	1:01	extra traffic on port 80 only from Far East (StEmdData), enough to show up on strip chart	5	Senior Network Controller	STATE EMD
1	1:01	a server (County_EmgData) in county seems to have a lot of load on it-not overloaded, but a lot	11	Senior Network Controller	COUNTY
1	1:01	FBI comes over to ask about a user who appears to be receiving personal data which could be used for identity theft	11	JTF Rep	COUNTY
1	1:01	extra traffic load all State DOT port 80 from Far East to (StDot_Data), enough to show up on strip chart	5	Senior Network Controller	STATE DOT
1	1:01	extra traffic to DIS on port 80 only from Far East (St_aceme_s), enough to show up on strip chart	5	Senior Network Controller	STATE DIS
1	1:02	Net admin reports a user has been receiving two e-mails per day, one with names, the other with bank account and social security numbers	11	Network Admin-State DOT	COUNTY
1	1:02	DIS Net Admin reports scanning traffic from Far East on port 80, but against non-web machines also - appears random	5	Network Admin-State DIS	STATE DIS
1	1:02	Port 80 scanning traffic noted in e-mail from EMD net-admin, showing up on non-web servers	5	Network Admin-State EMD	STATE EMD
1	1:03	extra scanning traffic on port 80 noted in e-mail from DOT net-admin, unique because it is also against non-web hosts	5	Network Admin-State DOT	STATE DOT
1	1:04	extra scanning traffic noted in e-mail from DOT net-admin	5	Network Admin-State DOT	STATE DOT
1	1:05	help desk e-mails complaints of excessive spam	1	Help Desk	COUNTY
1	1:10	e-mail from County Net admin advises of a malicious link-cross site scripting	1	Network Admin-County	COUNTY
1	1:15	traffic from Far East drops off partially	5	Senior Network Controller	STATE EMD
1	1:15	traffic on DIS from Far East drops off partially to 5%	5	Senior Network Controller	STATE DIS
1	1:15	traffic from Far East to DOT drops off partially to 15%	5	Senior Network Controller	STATE DOT
1	1:16	traffic from South America to DIS drops off completely	5	Senior Network Controller	STATE DIS
1	1:16	traffic from South America to DOT drops off completely	5	Senior Network Controller	STATE DOT
1	1:17	traffic from South America drops off completely	5	Senior Network Controller	STATE EMD
1	1:20	NIPC has notified State DIS via NASCIO only of extensive probing going on nationwide on port 80, may be related to earlier CERT advisory	5	DHS rep	STATE DIS
1	1:30	law enforcement comes and asks for disk image of computer serving MP3 files	11	JTF Rep	STATE DOT
1	1:31	DOT NetAdmin writes expressing concern that upon reviewing the logs the same Trojan (Microsoft) e-mail has gone to most other users on the system	12	Network Admin-State DOT	STATE DOT
1	1:32	City Police headquarters main line (City_Police_r) (City_r3) goes down and rolls over to a slower connection.	1	Senior Network Controller	CITY
1	1:32	Fire suppressant discharge in mainframe room at DIS	1	Network Admin-State DIS	STATE DIS
1	1:32	Loss of gateway router (StEmdR)	1	Senior Network Controller	STATE EMD
1	1:33	Loss of server (St_info_s) in mainframe room of DIS	1	Senior Network Controller	STATE DIS
1	1:33	EMD Communications line fails and automatic rollover to backup fails. (StEmdR) (St_client_)	1	Senior Network Controller	STATE EMD
1	1:33	USSS writes to say that a computer in county clerk's office has been attempting to crack into a personnel computer containing SSN's. They want to know which computer had a certain IP address 2 weeks ago.Police of slow response	11	JTF Rep	COUNTY

1	1:34	EMD reports loss of connectivity to their NOC, may be software problem	1	Network Admin-State EMD	STATE EMD
1	1:35	EMD reports that users are complaining they cannot get to the internet	1	Help Desk	STATE EMD
1	1:35	City Police hosts (City_Police_HQ)(Europe) generate heavy load as they are trying to download big files from somewhere	1	Senior Network Controller	CITY
1	1:35	help desk complains of users who cannot get out	1	Help Desk	STATE EMD
1	1:36	EMD Net Admin reports primary line is dead and secondary line did not activate - investigating	1	Network Admin-State EMD	STATE EMD
1	01:36	EMDNet Admin reports he just upgraded IOS before failure	1	Network Admin-State EMD	STATE EMD
1	01:37	City Help desk reports watch commander is really upset	1	Help Desk	CITY
1	01:38	Mayor has received an inquiry from the press saying the Police have lost access to their computer network. Please prepare a set of talking points for the Mayor	1	Mayor's Office	CITY
1	01:38	DIS Equipment failure (St_client_r) - rtr to DOT - coordinated event, not connected with fire suppressant	1	Senior Network Controller	STATE DIS
1	01:38	EMD Net Admin reports the router is fine, must be a telco problem on both lines	1	Network Admin-State EMD	STATE EMD
1	01:40	Equipment failure- rtr to DOT - no action required, done in DIS inject	1	Senior Network Controller	STATE DOT
1	01:40	City help desk reports police department noted utility workers in front of their building digging a trench	1	Help Desk	CITY
1	01:45	law enforcement comes and asks for disk image of computer serving MP3 files	11	JTF Rep	STATE EMD
1	01:45	Director of EMD has media inquiry about EMD being taken off-line by a hacker - please provide talking points	1	Director of EMD	STATE EMD
1	01:53	DIS Server returns to service	1	Senior Network Controller	STATE DIS
1	01:54	If required, EMD Net Admin reports he spoke with CISCO help desk and diagnosed problem	1	Network Admin-State EMD	STATE EMD
1	01:55	DOT Router returns to service	1	Senior Network Controller	STATE DIS
1	01:55	If EMD has not fixed problem by now,	1	Network Admin-State EMD	STATE EMD
1	01:56	DIS NetAdmin in control reports rtr to DOT unplugged by accident, now back in service	1	Network Admin-State DIS	STATE DIS
1	01:56	EMD Net Admin - if required- reports now on backup line	1	Network Admin-State EMD	STATE EMD
1	01:56	System back up and running normally	1	Senior Network Controller	STATE EMD
1	01:56	Note from DOT help desk that rtr was unplugged, now restored	1	Help Desk	STATE DOT
1	02:02	heavy load on host machine (St_HHSadm) (St_HHSs) in HHS	11	Senior Network Controller	STATE DIS
1	02:03	law enforcement comes and asks for disk image of computer serving MP3 files	11	JTF Rep	STATE DIS
1	02:03	County Communications line fails County_f1) (County_r4)	1	Senior Network Controller	COUNTY
1	02:04	load from outside internet directed at City mail server (CityEmail) grows to 95%	10	Senior Network Controller	CITY
1	02:05	help desk e-mails complaints of excessive spam	10	Help Desk	CITY
1	02:05	County Help desk reports failure in comms to outside world	1	Help Desk	COUNTY
1	02:05	Secretary of Transportation has media inquiries about a DQT employee using DOT computers to serve MP3 files. PIO please respond.	11	Secretary of Transportation	STATE DOT
1	02:07	County Net Admin reports primary line dead, secondary line works, but router not seeing it	1	Network Admin-County	COUNTY

1	02:09	County Net Admin reports router is fine, must be telco problem	1	Network Admin-County	COUNTY
1	02:10	e-mail from City Net admin advises of a malicious link-cross site scripting	10	Network Admin-City	CITY
1	02:10	Governor's office asks for a response to media about DIS employees operating MP3 servers on their computers.	11	Governor's Office	STATE DIS
1	02:22	If County has not requested by now, County Net Admin reports that router did not rollover to backup ISP automatically, he will take care of it	1	Network Admin-County	COUNTY
1	02:24	load from outside internet drops back to normal due to installation of filters	10	Senior Network Controller	CITY
1	02:25	County Net Admin reports that the rollover problem has been fixed and they are on backup	1	Network Admin-County	COUNTY
1	02:25	City Network admin sends e-mail that filters installed	10	Network Admin-City	CITY
2	00:01	Large amount of traffic out of Seattle City records host (inside of firewall). Causes server to waver between red and yellow and will not stop.	12	Senior Network Controller	CITY
2	00:02	netsim raises volume of internet traffic from internal County users to 80% to the outside US world as workers check news	13	Senior Network Controller	STATE DIS
2	00:02	netsim raises volume of internet traffic from internal City users to 80% to the outside US world as workers check news	13	Senior Network Controller	CITY
2	00:02	netsim raises volume of internet traffic from internal DOT users to 80% to the outside US world as workers check news	13	Senior Network Controller	STATE DOT
2	00:02	netsim raises volume of internet traffic from internal County users to 80% to the outside US world as workers check news	13	Senior Network Controller	COUNTY
2	00:02	netsim raises volume of internet traffic from internal EMD users to 80% to the outside US world as workers check news	13	Senior Network Controller	STATE EMD
2	00:03	Notice of threat change from NIPC per attached letter forwarded by NASCIO ISAC	13	Network Admin-State DIS	STATE DIS
2	00:04	EMD Users complaining that response on system is slow	13	Help Desk	STATE EMD
2	00:04	City Users complaining that response on system is slow	13	Help Desk	CITY
2	00:04	Help desk sends e-mail of complaints about response time	13	Help Desk	STATE DIS
2	00:04	DOT Users complaining that response on system is slow	13	Help Desk	STATE DOT
2	00:04	County Users complaining that response on system is slow	13	Help Desk	COUNTY
2	00:06	Traffic builds to 95%	13	Senior Network Controller	STATE DIS
2	00:06	EMD Users continue to complain system response is slow	13	Help Desk	STATE EMD
2	00:06	County Users continue to complain system response is slow	13	Help Desk	COUNTY
2	00:06	DOT Users continue to complain system response is slow	13	Help Desk	STATE DOT
2	00:06	City Users continue to complain system response is slow	13	Help Desk	CITY
2	00:07	NetAdmin of City reports that Cannot figure what is wrong with the bad host, and would like help procuring an outside expert. Don't want to just reinstall but analyze first. Can NOC find an expert?	12	Network Admin-City	CITY
2	00:07	Fish and Game complains poor response	13	Help Desk	STATE DIS

2	00:08	Help desk phones DIS to report many more complaints	13	Network Admin-State DIS	STATE DIS
2	00:08	County NetAdmin writes expressing concern that upon reviewing the logs the same Trojan (Microsoft) e-mail has gone to most other users on the system	12	Network Admin-County	COUNTY
2	00:12	Powerpoint presentation makes VNN announcement of increase in threat level from yellow to orange	13	VNN	STATE DIS
2	00:12	DIS Traffic drops down to normal 35-50%	13	Senior Network Controller	STATE DIS
2	00:12	Powerpoint presentation makes VNN announcement of increase in threat level from yellow to orange	13	VNN	STATE EMD
2	00:12	Powerpoint presentation makes VNN announcement of increase in threat level from yellow to orange	13	VNN	COUNTY
2	00:12	Powerpoint presentation makes VNN announcement of increase in threat level from yellow to orange	13	VNN	STATE DOT
2	00:12	Powerpoint presentation makes VNN announcement of increase in threat level from yellow to orange	13	VNN	CITY
2	00:14	DIS Help desk still reports complaints	13	Help Desk	STATE DIS
2	00:18	County Traffic drops down to normal 35-50%	13	Senior Network Controller	COUNTY
2	00:18	City Traffic drops down to normal 35-50%	13	Senior Network Controller	CITY
2	00:18	EMD Traffic drops down to normal 35-50%	13	Senior Network Controller	STATE EMD
2	00:18	DOT Traffic drops down to normal 35-50%	13	Senior Network Controller	STATE DOT
2	00:20	Governor's Office notifies all State department heads of change in Threat Condition to Orange	13	Governor's Office	STATE DIS
2	00:22	DOT Net Admin reports that they have shaped traffic to give lower priority to files of type .ra and .qt	1	Network Admin-State DOT	STATE DOT
2	00:22	City Net Admin reports that they have shaped traffic to give lower priority to files of type .ra and .qt	13	Network Admin-City	CITY
2	00:22	County Net Admin reports that they have shaped traffic to give lower priority to files of type .ra and .qt	1	Network Admin-County	COUNTY
2	00:24	County Help desk reports that public is writing and calling in to report several County websites are defaced with anti-American slogans	8	Help Desk	COUNTY
2	00:26	County Exec has received a media request about who is hacking the County websites. Please prepare talking points for the County Exec.	8	County Executive's Office	COUNTY
2	00:32	Governor's website defaced in call from Gov's Office	8	Help Desk	STATE DIS
2	00:33	DOT Help desk reports that public is writing and calling in to report several DOT websites are defaced with anti-American slogans	8	Help Desk	STATE DOT
2	00:33	City Help desk reports that a couple of primary web pages have been defaced with anti-American slogans	8	Help Desk	CITY
2	00:34	Labor & Industry website defaced reported in phone call	8	Help Desk	STATE DIS
2	00:34	EMD help desk reports that primary web page has been defaced (index.html)	8	Help Desk	STATE EMD
2	00:35	Mayor's office called, they have received a Media inquiry about web page defacements - please prepare talking points for the Mayor in 20 minutes	8	Mayor's Office	CITY
2	00:36	Governor's office asks for talking points to reply to media inquiry about defaced web sites	8	Governor's Office	STATE DIS
2	00:40	Director of EMD has media inquiry about website defacement - please provide talking points	8	Director of EMD	STATE EMD
2	00:53	DIS Net Admin gets really insulting e-mail from Darlene telling them to go to website and immediately download a system patch	1	Network Admin-State DIS	STATE DIS
2	00:57	DOT Net admin says all web sites are fixed	8	Network Admin-State DOT	STATE DOT
2	00:57	DIS Net admin says all web sites are fixed	8	Network Admin-State DIS	STATE DIS
2	00:57	EMD Net admin says all web sites are fixed	8	Network Admin-State EMD	STATE EMD
2	01:00	Secretary of Transportation has media inquiries about hacked DOT web sites, please provide talking points	8	Secretary of Transportation	STATE DOT

2	01:03	City NetAdmin receives e-mail from Microsoft (without PGP signature) telling of urgent security update and directing people to web site to download the patch	10	Network Admin-City	CITY
2	01:04	City traffic from a cluster to a single site on a computer off the internet grows to 85% of that site's capacity	10	Senior Network Controller	CITY
2	01:04	DIS help desk reports that a spoofed e-mail from (b)(6) (b)(6) is circulating in DIS	1	Help Desk	STATE DIS
2	01:05	DIS Help desk reports that the spoofed e-mail is popping up everywhere. Is it really her?	1	Help Desk	STATE DIS
2	01:09	Governor's office calls asking what is going on - media is asking about DIS employee who is spreading malicious software	1	Governor's Office	STATE DIS
2	01:15	City NetAdmin determines that the e-mail is not from Microsoft but is a hoax containing a Trojan	10	Network Admin-City	CITY
2	01:16	City NetAdmin writes expressing concern that upon reviewing the logs the same e-mail has gone to most other users on the system	10	Network Admin-City	CITY
2	01:22	Several Internal web servers on EMD network generate external traffic on port 80	5	Senior Network Controller	STATE EMD
2	01:22	Several Internal web servers on County network generate external traffic on port 80-saturate pipes	5	Senior Network Controller	COUNTY
2	01:23	Several Internal web servers on DOT network generate external traffic on port 80-saturate pipes	5	Senior Network Controller	STATE DOT
2	01:23	Several Internal web servers on City network generate external traffic on port 80	5	Senior Network Controller	CITY
2	01:24	State DOT help desk reports user complaints of getting out, internet is down.	5	Help Desk	STATE DOT
2	01:24	State EMD help desk reports user complaints of getting out, internet is down.	5	Help Desk	STATE EMD
2	01:24	City help desk reports user complaints of getting out, internet is down.	5	Help Desk	CITY
2	01:24	County help desk reports user complaints of getting out, internet is down.	5	Help Desk	COUNTY
2	01:25	Several Internal web servers on DIS network generate external traffic on port 80-saturate pipes	5	Senior Network Controller	STATE DIS
2	01:26	NetAdmin for City reports that the traffic coming from the web servers looks like port 80 web traffic destined for random addresses	5	Network Admin-City	CITY
2	01:27	State DIS help desk reports user complaints of getting out, internet is down.	5	Help Desk	STATE DIS
2	01:27	County Net admin says all web sites are fixed	8	Network Admin-County	COUNTY
2	01:30	All Internal web servers Scanning traffic drops abruptly from EMD networks	5	Senior NetworkController	STATE EMD
2	01:30	All Internal web servers Scanning traffic drops abruptly from City networks	5	Senior Network Controller	CITY
2	01:32	All Internal web servers Scanning traffic drops abruptly from DOT networks	5	Senior Network Controller	STATE DOT
2	01:33	All Internal web servers Scanning traffic drops abruptly on State DIS networks	5	Senior Network Controller	STATE DIS
2	01:34	All Internal web servers Scanning traffic drops abruptly from County networks	5	Senior Network Controller	COUNTY
2	01:50	Net Admin writes seeing unusual scanning on port 1433.	6	Network Admin-State EMD	STATE EMD
2	01:50	Outside sources generate traffic detectable on strip chart, port 1433	6	Senior Network Controller	STATE EMD
2	01:50	Net Admin writes seeing unusual scanning on port 1433.	6	Network Admin-County	CITY
2	01:50	Outside sources generate traffic detectable on strip chart, port 1433	6	Senior Network Controller	CITY

2	01:50	Outside sources generate traffic detectable on strip chart, port 1433	6	Senior Network Controller	COUNTY
2	01:50	Net Admin writes seeing unusual scanning on port 1433.	6	Network Admin-State DOT	STATE DOT
2	01:50	Outside sources generate traffic detectable on strip chart, port 1433	6	Senior Network Controller	STATE DIS
2	01:50	Net Admin writes seeing unusual scanning on port 1433.	6	Network Admin-City	COUNTY
2	01:50	Net Admin writes seeing unusual scanning on port 1433.	6	Network Admin-State DIS	STATE DIS
2	01:50	Outside sources generate traffic detectable on strip chart, port 1433	6	Senior Network Controller	STATE DOT
2	01:52	Inside MS-SQL servers generate traffic detectable at 100% capacity, port 1433	6	Senior Network Controller	STATE DIS
2	01:52	Inside MS-SQL servers generate traffic detectable at 100% capacity, port 1433	6	Senior Network Controller	STATE DOT
2	01:52	Inside MS-SQL servers generate traffic detectable at 100% capacity, port 1433	6	Senior Network Controller	CITY
2	01:52	Inside MS-SQL servers generate traffic detectable at 100% capacity, port 1433	6	Senior Network Controller	COUNTY
2	01:52	Inside MS-SQL servers generate traffic detectable at 100% capacity, port 1433	6	Senior Network Controller	STATE EMD
2	02:00	Outside scanning traffic on port 1433 stops.	6	Senior Network Controller	STATE DIS
2	02:00	Outside scanning traffic on port 1433 stops.	6	Senior Network Controller	CITY
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	STATE DIS
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	STATE EMD
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	COUNTY
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	COUNTY
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	STATE EMD
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	STATE DOT
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	CITY
2	02:00	Inside scanning traffic on port 1433 stops	6	Senior Network Controller	STATE DOT
2	02:03	EMD reports cannot retrieve data from contact database	6	Help Desk	STATE EMD
2	02:04	County help desk reports users complaining they cannot get to GIS data base	6	Help Desk	COUNTY
2	02:04	City help desk reports that electric utility reports they cannot get data from several databases	6	Help Desk	CITY
2	02:05	DIS help desk reports Health & Human Services Database is down	6	Help Desk	STATE DIS
2	02:05	DOT help desk reports that users complaining their data bases are not working	6	Help Desk	STATE DOT
2	02:07	County help desk reports users complaining they cannot retrieve data from their other data bases also	6	Help Desk	COUNTY
2	02:08	EMD help desk reports cannot retrieve data from Emergency Procedures database	6	Help Desk	STATE EMD
2	02:08	City help desk reports that water utility cannot retrieve data from customer database	6	Help Desk	CITY
2	02:08	DIS help desk reports State Police Database is down	6	Help Desk	STATE DIS
2	02:09	DOT help desk reports more users complaining data bases are completely non-functional	6	Help Desk	STATE DOT
2	02:10	Secretary of Transportation has media inquiries about loss of computer data bases. please provide talking points.	6	Secretary of Transportation	STATE DOT
2	02:10	Governor's office asks for talking points to reply to media inquiry about loss of state government databases	6	Governor's Office	STATE DIS
3	00:02	NetAdmin for DIS reports that NASCIO has forwarded a msg from NIPC to set Threat Condition RED	13	Network Admin-State DIS	STATE DIS

3	00:04	Traffic load from many places on internet to PNW domains.	13	Senior Network Controller	CITY
3	00:04	Traffic load from many places on internet to PNW domains.	13	Senior Network Controller	STATE EMD
3	00:04	Traffic load from many places on internet to PNW domains.	13	Senior Network Controller	STATE DOT
3	00:04	Traffic load from many places on internet to PNW domains.	13	Senior Network Controller	STATE DIS
3	00:04	Traffic load from many places on internet to PNW domains.	13	Senior Network Controller	COUNTY
3	00:05	VNN comes on to say that DHS has moved threat condition from orange to Red for the Seattle area	13	VNN	COUNTY
3	00:05	VNN comes on to say that DHS has moved threat condition from orange to Red for the Seattle area	13	VNN	STATE DOT
3	00:05	VNN comes on to say that DHS has moved threat condition from orange to Red for the Seattle area	13	VNN	STATE EMD
3	00:05	VNN comes on to say that DHS has moved threat condition from orange to Red for the Seattle area	13	VNN	CITY
3	00:05	VNN comes on to say that DHS has moved threat condition from orange to Red for the Seattle area	13	VNN	STATE DIS
3	00:06	Media has asked what the government IT department does differently when they move to condition RED	13	Mayor's Office	CITY
3	00:06	help desk complains about slow response to users	13	Help Desk	STATE EMD
3	00:06	Media has asked what the government IT department does differently when they move to condition RED	13	Governor's Office	STATE DIS
3	00:06	Media has asked what the government IT department does differently when they move to condition RED	13	Secretary of Transportation	STATE DOT
3	00:06	help desk complains about slow response to users	13	Help Desk	CITY
3	00:06	Media has asked what the government IT department does differently when they move to condition RED	13	County Executive's Office	COUNTY
3	00:06	help desk complains about slow response to users	13	Help Desk	COUNTY
3	00:06	help desk complains about slow response to users	13	Help Desk	STATE DOT
3	00:06	help desk complains about slow response to users	13	Help Desk	STATE DIS
3	00:06	Media has asked what the government IT department does differently when they move to condition RED	13	Director of EMD	STATE EMD
3	00:10	Net Admin of DIS reports that they have just received a notification from NASCIO that says that DHS has declared condition RED due to a confirmed threat to the Pacific NorthWest in the next 24-48 hours.	13	Network Admin-State DIS	STATE DIS
3	00:10	NetAdmin of State EMD reports they have just received notification of an increase in threat condition from Orange to RED due to a confirmed threat to the Pacific NorthWest in the next 24-48 hours. Was received over the National Warning System (NAWAS) and National Law Enforcement Teletype (NLETS). The Governor, TAG and Director of EMD were also briefed by Secure VTC and STU-III in a conference call from Secretary Ridge, prior to the effective time in the change in level.	13	Network Admin-State EMD	STATE EMD
3	00:10	NetAdmin for City says that heavy traffic is coming from streaming video and suggests traffic shaping to fix it	13	Network Admin-City	CITY
3	00:12	Director of EMD has media inquiry about what their IT department actions are when they go to condition RED. Please provide talking points.	13	Director of EMD	STATE EMD
3	00:12	Governor's office asks for talking points to reply to media inquiry about what of threat level RED means for state computer systems	13	Governor's Office	STATE DIS
3	00:33	DDoS starts up against City networks traffic maxes out	5	Senior Network Controller	CITY

3	00:34	DDoS starts up against State DIS networks and maxes out	5	Senior Network Controller	STATE DIS
3	00:35	Call from fire dept friend tells them that an explosion has occurred south of the city	13	Help Desk	COUNTY
3	00:35	Call from fire dept friend tells them that an explosion has occurred south of the city	13	Help Desk	STATE EMD
3	00:35	Call from fire dept friend tells them that an explosion has occurred south of the city	13	Help Desk	CITY
3	00:35	Call from fire dept friend tells them that an explosion has occurred south of the city	13	Help Desk	STATE DOT
3	00:35	Call from fire dept friend tells them that an explosion has occurred south of the city	13	Help Desk	STATE DIS
3	00:35	DDoS starts up against State DOT networks and maxes out	5	Senior Network Controller	STATE DOT
3	00:36	VNN comes on to say there has been an explosion at a warehouse south of the city	13	VNN	COUNTY
3	00:36	VNN comes on to say there has been an explosion at a warehouse south of the city	13	VNN	STATE EMD
3	00:36	VNN comes on to say there has been an explosion at a warehouse south of the city	13	VNN	CITY
3	00:36	DDoS starts up against State EMD networks and maxes out	5	Senior Network Controller	STATE EMD
3	00:36	VNN comes on to say there has been an explosion at a warehouse south of the city	13	VNN	STATE DOT
3	00:36	VNN comes on to say there has been an explosion at a warehouse south of the city	13	VNN	STATE DIS
3	00:37	DDoS starts up against County networks and maxes out	5	Senior Network Controller	COUNTY
3	00:43	VNN comes on to say that there are rumors of radioactivity in the explosion south of the city	13	VNN	CITY
3	00:43	VNN comes on to say that there are rumors of radioactivity in the explosion south of the city	13	VNN	STATE DOT
3	00:43	VNN comes on to say that there are rumors of radioactivity in the explosion south of the city	13	VNN	COUNTY
3	00:43	VNN comes on to say that there are rumors of radioactivity in the explosion south of the city	13	VNN	STATE EMD
3	00:43	VNN comes on to say that there are rumors of radioactivity in the explosion south of the city	13	VNN	STATE DIS
3	01:05	VNN shows all players their best guess of what the range of the spread of radioactivity is.	13	VNN	CITY
3	01:05	VNN shows all players their best guess of what the range of the spread of radioactivity is.	13	VNN	STATE DOT
3	01:05	VNN shows all players their best guess of what the range of the spread of radioactivity is.	13	VNN	COUNTY
3	01:05	VNN shows all players their best guess of what the range of the spread of radioactivity is.	13	VNN	STATE DIS
3	01:05	VNN shows all players their best guess of what the range of the spread of radioactivity is.	13	VNN	STATE EMD
3	01:15	DDoS stops and network traffic drops to 90% from inside the city	5	Senior Network Controller	CITY
3	01:16	DDoS against State DIS stops	5	Senior Network Controller	STATE DIS
3	01:17	DDoS against State DOT stops	5	Senior Network Controller	STATE DOT
3	01:18	DDoS against State EMD stops	5	Senior Network Controller	STATE EMD
3	01:19	DDoS against County stops	5	Senior Network Controller	COUNTY
3	01:30	City is receiving complaints that the information on the city transportation web page is telling people to evacuate town	8	Help Desk	CITY

3	01:30	DOT Help desk reports that there is confusing information on their website about how to use all traffic lanes to leave town, no inbound traffic is allowed	8	Help Desk	STATE DOT
3	01:33	City NOC employees hear from friends that the County has been ordered to evacuate the NOC	13	Network Admin-City	CITY
3	01:34	We ask the County Executive to evacuate all the people from his NOC due to danger of radioactive plume, the ventilators for the building are still on and bldg mgme has evacuated.	13	County Executive's Office	COUNTY
3	01:45	DDoS starts up against City networks traffic maxes out	5	Senior NetworkController	CITY
3	01:46	DDoS starts up against State DIS networks and maxes out	5	Senior NetworkController	STATE DIS
3	01:47	DDoS starts up against State DOT networks and maxes out	5	Senior NetworkController	STATE DOT
3	01:48	DDoS starts up against State EMD networks and maxes out	5	Senior NetworkController	STATE EMD
3	01:49	DDoS starts up against County networks and maxes out	5	Senior NetworkController	COUNTY
3	02:05	Heavy DDoS on City's e-mail servers casuses them to quit.	1	Senior NetworkController	CITY
3	02:07	load on e-mail servers goes to 100% in a prolonged DDoS, preventing outgoing mail also	5	Senior NetworkController	STATE EMD
3	02:08	With the Email servers down, we are also having problems with out of band communications. Please discuss.	1	Admin Support & runners	STATE EMD
3	02:08	With the Email servers down, we are also having problems with out of band communications. Please discuss.	1	Admin Support & runners	CITY
3	02:10	Mayor asks City NOC how their staffing is to handle the workload	13	Mayor's Office	CITY
3	02:13	Employee in bldg calls to say that they cannot get an outside line, all phones are tied up - Need to call CISCO, and worried even if they get thru, CISCO might not be able to call back	13	Help Desk	STATE EMD
3	02:20	Governer calls to ask that DIS facilitate the recall of all essential governmental employees.	13	Governor's Office	STATE DIS

APPENDIX C

SAMPLE SIMULATION COMMUNICATIONS OUTPUT

1218 20030506T13:46:34

To: netadmin.dot.control
From: dot.state.player
Subj: Email from city.player
Please apply filters to block that east coast domain.

20030506T14:53:49

To: netadmin.city.control
From: city.player@simserve1
Subj: Email from city.player
Please set egress filters at police_r to block everything other than 80, 8080 and 443 message

2991 20030507T13:58:50

To: dis.state.player
From: university.support
Subj: Email from dis.state.player Enabling such filters will greatly deminish the overall throughput of the routers as this will cuase all packets to he process-switched throught the router.

20030506T19:25:39

From :cert.support
From: city.player
How is the worm being propagated?

20030506T19:26:58

To: cert.support
From: county.player
Can you please provide us with any information on how to contact British Columbia Information Technology groups?

APPENDIX D

PRESS RELEASE

Gov. Locke Touts Success of TOPOFF2 Cyber Exercise

News Release - May 15, 2003 -- SEATTLE, Wash - - Governor Gary Locke announced the successful completion of the TOPOFF2 cyber exercise. The cyber exercise tested the response of the government's computer networks in the event it should experience a series of widespread, escalating cyber events.

The TOPOFF2 cyber exercise was part of the national TOPOFF2 exercise that began May 12 in Seattle and Chicago. The exercises featured sophisticated computer simulations, creating situations where state and local government information technology organizations had to respond in concert to a series of cyber security scenarios.

"This cyber exercise will help us be better prepared to respond to the possibility of disruptions or outages in our computer networks," Locke said. "I am proud of how our agencies performed and our ability to work across jurisdiction at the local, state and federal level."

Participants in the TOPOFF2 cyber exercise examined the actions required to limit potential damage caused by network compromise, and to minimize the impact on operations. The exercise required participants to make decisions in real-time in response to different, escalating events that slowed or stopped network operations. These events triggered management decision-making exercises about the associated business and communication functions required to recover the systems and resume providing essential public services.

"Working together in collaboration with the city of Seattle and King County, this exercise truly helped us organize a regional, coordinated response to a potential cyber event," said Stuart McKee, director of the state Department of Information Services. "The training was an excellent opportunity to test assumptions and effectively respond to a highly complex cyber incident."

Agencies involved in the cyber exercise included the state's Department of Information Services, Department of Transportation and Emergency Management Division, along with numerous agencies from the city of Seattle and King County, and the U.S. Department of Homeland Security, the U.S. Department of State, the local Joint Task Force of the FBI, the U.S. Secret Service and the U.S. Attorney's Office, as well as the private sector and Canada.

The TOPOFF2 cyber exercise is the first time an interactive, computerized network simulation has been used in public government, and was designed to create an "immersion experience" for participants. The Institute for Security Technology Studies (ISTS) at Dartmouth College created the network simulation.

This page intentionally left

Department of Homeland Security

FOR OFFICIAL USE ONLY

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "FOR OFFICIAL USE ONLY," OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.

Top Officials 3 Full Scale Exercise After-Action Report

April 4-10, 2005

Homeland Security

THIS PAGE INTENTIONALLY LEFT BLANK

ADMINISTRATIVE HANDLING INSTRUCTIONS

1. The title of this document is *Top Officials (TOPOFF) 3 (T3) After-Action Report.*

2. **WARNING:** This document is ~~FOR OFFICIAL USE ONLY (FOUO).~~ It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to ~~FOUO~~ information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

3. Reproduction of this document, in whole or part, without prior approval of National Exercise Division, DHS/FEMA, is prohibited.

4. The *T3 After-Action Report* is broken into several sections, annexes, and appendices. All of these sections remain ~~FOUO~~ when separated from the document.

5. The DHS/FEMA, National Exercise Division, is the control authority for the *T3 After-Action Report*. Ms. Sandra Santa Cosgrove, Acting Branch Chief, National Exercise Division, DHS/FEMA can be reached via e-mail at sandra.santa@dhs.gov and via telephone at 202-786-9594.

THIS PAGE INTENTIONALLY LEFT BLANK

T3 After-Action Report User Guide (A Road Map)

This After-Action Report (AAR) is a compilation of several documents, all of which are related to the design and conduct of the Top Officials (TOPOFF) 3 (T3) series of events. As a comprehensive reference guide to T3, it has been organized and sectioned to enable its users to review or access information relevant to their research interest.

The depth of detail of the report is considered sufficient to build context around core T3 issues and allow interested professionals to consider possible alternatives/improvements to address policy or procedural shortcomings within their respective Department/Agency (D/A). Requests for additional data not included in this report are to be directed through the Acting Branch Chief, National Exercise Division, DHS/FEMA, Ms. Sandra Santa Cosgrove, Sandra.Santa@dhs.gov, or 202-786-9594.

The recommendations offered in the AAR are intended to stimulate action toward improving capabilities and performance or resolving an issue or deficiency. The assessments that went into these recommendations were not intended to have the depth and granularity required to be considered on their own, fully "actionahle" prescriptions for an organization or any element within an organization.

Every attempt has been made to avoid redundancy throughout the report; however, given that several of the annexes are stand-alone documents, some redundancy is unavoidable. Two synopses, the *Executive Overview* and the *T3 AAR Summary Report*, are similar in nature; however, due to their development background, have subtle differences. Both of these abridgments provide an excellent outline of T3 issues that surfaced as a result of the Full-Scale Exercise (FSE). The *Executive Overview* is simply an overview written for senior leaders. Its content has been gleaned from a multitude of D/A input. The *T3 AAR Summary Report* is very similar in content, but has been compiled from the AAR and therefore is supported by the findings of the T3 evaluation team.

The following category descriptions supplement the content map below:

I. Exercise Overview

The Overview consists of a summary of TOPOFF series history, information on TOPOFF building block events, evaluation methodology, reconstruction data, and exercise artificialities.

A. Building Blocks

The T3 FSE is the pinnacle of a series of building block events that occurred during the 18 months leading up to the FSE. Each event preceding the FSE and the one follow-on exercise were designed to build upon the stated goals and objectives established by all participating Federal, State, and local D/As.

B. Evaluation Methodology

This section provides a description of the T3 FSE evaluation methodology, based on the approach outlined in *Homeland Security Exercise and Evaluation Program Volume II: Exercise Evaluation and Improvement* (https://odp.esportals.com/login.cfm). This approach provides participants and response agencies with information that they can use to improve their response policies and procedures to incidents of national significance. The analysis also provides information that some organizations may find useful for their internal evaluations.

C. Exercise Event Reconstruction

This section provides a fact-based, time-synchronized, de-conflicted, and meaningful account of what actually happened during the T3 FSE.

D. Exercise Artificialities

This section includes a description of T3 FSE artificialities that represent either deliberate choices made during the design of T3 or are specific to this particular exercise (as opposed to exercises in general). These choices were made with the understanding that they would have impacts on exercise findings. The T3 evaluation team believes that these impacts are accounted for in the exercise analysis.

II. Exercise Goals and Objectives

This is a one-page summary of the objectives of the T3 FSE.

III. Scenario

This section contains an overview of the T3 FSE scenario. The T3 FSE scenario provides an environment for participants—primarily top-level decision makers—to exercise against a credible terrorist adversary that plans and executes multiple attacks employing weapons of mass destruction. Although the scenario is plausible, it contains artificialities necessary to create conditions required to achieve exercise goals and objectives. The chain of events depicted in the scenario is hypothetical, and the terrorist groups and individuals portrayed in the scenario are fictional.

IV. Analysis of Mission Outcomes

This section contains identification of the ten topical areas analyzed including the four issues identified as Broad Mission Outcomes: the Homeland Security Advisory System, Joint Field Office, Resource Requesting/Coordination, and Information Sharing.

V. Analysis of Critical Task Performance

This section of the report reviews performance of critical tasks as identified by the HSEEP Volume II Exercise Evaluation Guide (EEG) including: Stafford Act Declarations, Emergency Public Information, Integrating Responses to Incident of National Significance: Public Health Emergency and the Stafford Act, the Strategic National Stockpile and Points of Distribution, Agent Confirmation and Hazard Area Definition, and Emergency Response Operations under a Unified Command.

VI. Conclusions

This section summarizes the primary issues or observations and recommended courses of action associated with each of the ten analysis topics.

VII. Annexes

- **Intelligence**
  This annex provides a For Official Use Only (~~FOUO~~) summary of the intelligence element of T3, including the 30-day pre-FSE activities and events.
- **Private Sector**
  This annex provides a summary of private sector integration and exercise play assessment. T3 reflected the first major involvement of the private sector in the TOPOFF series.
- **CT Cyber**
  This annex provides details associated with the cyber exercise in Connecticut.
- **NJ Cyber**
  This annex provides details associated with the cyber exercise in New Jersey.
- **Acronym List**
- **Executive Overview**
  This annex contains a 24-page summary of exercise issues gleaned from multiple D/A input, and was written for executive leadership review.
- **International**
  International play in T3 was primarily focused on the involvement of the United Kingdom (UK) and Canada. This annex provides integration and exercise play assessment of the UK and Canadian events and actions.

THIS PAGE INTENTIONALLY LEFT BLANK

T3 AAR Table of Contents

ANNEXES

Executive Summary

I. Introduction

This T3 Summary Report summarizes the findings/lessons of T3 After-Action Report (AAR) and provides a list of recommended remedial actions that address deficiencies and recommendations for improved performance. It is intended to provide a brief overview of key issues addressed in greater detail in the body of the AAR. Refer to the full AAR for a more extensive analysis of exercise actions based on information recorded by exercise data collectors located at key Emergency Operation Centers (EOCs) and exercise sites during the Full-Scale Exercise (FSE).

II. Background

T3 was a Congressionally mandated, national counterterrorism exercise designed to identify vulnerabilities in the nation's domestic incident management capability. It exercised the plans, policies, procedures, systems, and facilities of Federal, State, and local (FSL) response organizations against a series of integrated terrorist threats and acts in separate locations in the northeastern United States.

In coordination with T3, the United Kingdom and Canada conducted simultaneous and related exercises (Atlantic Blue in the United Kingdom and Triple Play in Canada) designed to improve mutual response and preparedness against global terrorism. The planning and execution of the three exercises provided an excellent opportunity for international cooperation, networking of key responders, and sharing of information on concepts of emergency operations.

III. Goals

The following objectives were established to direct the exercise design process for T3:

- Incident management: To test the full range of existing procedures for domestic incident management of a weapon of mass destruction (WMD) terrorist event and to improve top officials' capabilities to respond in partnership.
- Intelligence/Investigation: To test the handling and flow of operational and time-critical intelligence between agencies in response to a linked terrorist incident.
- Public information: To practice the strategic coordination of media relations and public information issues in the context of a WMD terrorist incident.
- Evaluation: To identify lessons learned and promote best practices.

With these four objectives as a guide, FSL, tribal, private sector, and other organizations created their own goals and objectives for evaluation through the exercise process. New

Jersey and Connecticut planners identified specific goals that focused the exercise design process on key issues within their respective States.

IV. Scenario Development

The T3 FSE scenario provided an environment for participants—primarily top-level decision makers—to exercise against a credible terrorist adversary that had planned and executed an attack employing WMDs. As described in Homeland Security Exercise and Evaluation Program (HSEEP) Volume III, a scenario for an objectives-based exercise should provide sufficient background and technical information to drive exercise play, yet remain at a reasonable level of complexity to avoid overwhelming the exercise players. Accordingly, the T3 FSE scenario was realistic, plausible, and designed to provide an accurate and comprehensive portrait of real-world threats related to exercise conditions described in the Homeland Security Council's Illustrative Planning Scenarios (IPSs). The T3 FSE scenario accommodated Department of Homeland Security Office of State and Local Government Coordination and Preparedness (DHS/SLGCP)-approved exercise objectives and included credible, hypothetical situations that created an internally complete and consistent world in which conditions influenced player activities and created decision-making opportunities.

Use of real-world intelligence systems to test the handling and flow of intelligence was a primary goal for the T3 FSE. To avoid the legal implications of exercising against actual terrorist groups, networks, or individuals, and to ensure that the exercise remained at the lowest possible classification level, the T3 FSE scenario employed a fictionalized threat—the Universal Adversary (UA). Although the names of UA groups and individuals were fictional, this credible, highly adaptive adversary was based on unclassified intelligence estimates describing known terrorist motivations, capabilities, intentions, organizations, strategies, operations, tactics, techniques, and procedures.

The T3 scenario contained the following elements:

- A biological attack in New Jersey
- A chemical and vehicle-borne improvised explosive device (VBIED) attack in Connecticut
- Multiple VBIED attacks in London
- A salmonella outbreak on a cruise ship in Canada

V. Exercise Artificialities

By their nature, exercises are not real events and, consequently, are influenced by constrained factors that are collectively known as artificialities. Although every attempt is made to mitigate the effects of artificialities, they will occur and can affect the outcomes of the exercise. If the nature and effects of artificialities are not taken into account, the conclusions drawn from the exercise could be incorrect. Artificialities surface in any exercise involving the response to a WMD event. The fundamental issue is that it is often impossible to exercise the full scope of a real-world event—ranging from an actual bomb

detonation to shutting down transportation infrastructure to commanding the full-time attention of top officials. The result is that many exercise events or actions must be notional or simulated, instead of actual. Despite the notional character of some events, governmental agencies and organizations played as though the events actually took place. This allowed the T3 evaluation team to examine decision-making, coordination, and communication issues. The evaluation team accounted for T3 artificialities in the analysis process to ensure proper interpretation of the exercise results.

VI. Evaluation Methodology

A. Introduction

The evaluation of the T3 FSE intended to:

- Assess and enhance FSL terrorism preparation, prevention, response, and recovery capabilities.
- Provide objective observations of complex, multifaceted interactions of FSL entities.
- Provide recommendations for improving FSL counterterrorism incident management policies and procedures.
- Provide a basis for assessing progress and improvement over time and against the backdrop of evolving policies and procedures.

The T3 FSE evaluation focused on high-level FSL coordination, support plans, policies, and procedures. In addition to the evaluation presented in this summary and in the full AAR document, organizations that participated in the exercise were encouraged to conduct their own internal evaluations based on their specific objectives, tasks, and procedures.

B. Methodology

The T3 FSE evaluation methodology is based on the approach outlined in HSEEP Volume II: Exercise Evaluation and Improvement. The overall aim of the evaluation is to document *what happened* during the exercise and explain *why*. This methodology provides participants and response agencies with information they can use to improve their response policies and procedures to Incidents of National Significance (INS). The analysis also provides information that some organizations may find useful for their internal evaluations. Evaluation consists of the following three steps:

1. Observation: collecting data
2. Reconstruction: determining what happened and when
3. Analysis: determining why specific actions or events occurred.

1. Observation

To systematically determine what happened in an exercise, dedicated observers known as data collectors must be assigned wherever exercise play occurs. The number of data

collectors at any one location depended on the scale or intensity of play, number of players, or geographic spread of the location. Analysts were available in each venue to supplement data collectors at key exercise sites, such as State EOCs or Joint Field Offices (JFOs).

Data collectors were not the only observers at the T3 FSE who provided data for analysis. T3 FSE players, controllers, simulation cell (SIMCELL) staff, and the Virtual News Network (VNN) also contributed critical data to the analysis. Players provided data by:

- Completing questionnaires (player feedback forms);
- Providing copies of logs, e-mails, and other documentation developed during the T3 FSE;
- Contributing to their organization's lessons learned; and
- Contributing to relevant Hotwashes.

This input was critical to the analysis, as it represents players' perspectives on the exercise and their actions/decisions. Exercise support personnel provided controller logs, SIMCELL logs, and VNN reports to the analysts.

In addition to data collected during the T3 FSE, a Hotwash was conducted immediately after the exercise in each venue, followed by an After-Action Conference. Data from all of these events were collected to obtain additional player feedback, ensuring a complete and comprehensive overview of the critical aspects of the exercise.

2. Reconstruction

Reconstruction produced a fact-based, time-synchronized, deconflicted, and *meaningful* account of what happened during the exercise. This laborious process is essential for conducting a meaningful analysis. Reconstruction involved the following aspects:

- Independent and parallel reconstruction of events at each location by analysts assigned to one or more locations;
- Group reconstruction of how the events at each location fit in with those at the other locations; this step typically engenders considerable revision of the individual analyst's initial reconstruction of events at his/her location; and
- Creation of a single, integrated reconstruction report.

The full AAR contains a more detailed account of the reconstruction process. Only an abridged version of the complete T3 FSE reconstruction is provided in this report.

3. Analysis

In this final step of the evaluation process, analysts used the record of events provided by the reconstruction to objectively seek patterns and develop an understanding of why certain issues emerged during the exercise. The analysis of these issues includes detailed descriptions of the issues and, when relevant, potential explanations for the behavior or

result. The T3 FSE analysis also identifies areas for improvement and recommends courses of action for strengthening the ability of FSL organizations to respond to emergencies. FSL agencies will use these results to develop improvement plans.

VII. Analysis

In an exercise as large in scope and as complex as T3, the opportunities for analysis were significant. Based on post-exercise meetings among participants, the T3 After-Action Conference, and observations by subject-matter experts during the exercise, 10 elements of the exercise were selected for in-depth analysis. These topics, listed below, are summarized in this report:

- Strategic National Stockpile (SNS) and Points of Dispensing (PODs)
- Homeland Security Advisory System (HSAS), State Threat Conditions, and Associated Protective Measures
- Stafford Act Declarations
- Integrating Responses to Incidents of National Significance: Public Health Emergency and the Stafford Act
- Emergency Response Operations Under a Unified Command (UC)
- JFO Operations
- Agent Confirmation and Hazard Area Definition
- Resource Requesting and Resource Coordination
- Information Sharing in the T3 FSE
- Emergency Public Information

The selection of these topics is not meant to indicate that other issues were not worthy of analysis. Rather, these issues reflect sequences of events that attracted great interest, involved new organizations and procedures, and revealed elements of the exercise that seemed particularly problematic or well-played. Nothing should be presumed about a topic or issue that was not selected for analysis. The brief description of each topic in this document should not be considered authoritative; a standalone section for each topic is included in the full AAR.

A. Strategic National Stockpile (SNS) and Points of Dispensing (PODs)

The release of *Yersinia pestis* (plague) in New Jersey prompted State officials to request SNS support and prompted Federal and State officials to activate nearly 400 PODs throughout the State to provide prophylaxis to all residents. Analysis of the T3 FSE data suggests that this plan was not executable. Distribution of prophylaxis was hampered by the short incubation period of plague, a fragmented Federal and State planning process, and resource management issues.

Comparatively, few problems were observed during the delivery and distribution of the SNS. There was some initial uncertainty about the SNS request and problems integrating Federal plans for SNS deployment with the State; however, the T3 participants successfully resolved these issues.

Throughout the year-long development process for the T3 New Jersey pneumonic plague scenario, a dedicated team from the AMTI prime contractor and the CDC painstakingly developed an epidemiologically sound progression model for the spread of the Plague in New Jersey. Based on this model, New Jersey scheduled a highly ambitious exercise play for its entire state hospital and local health organization infrastructure for the mass distribution of medications to combat the Plague. Based on real life resource constraints, every organization that could play did so and more robust participation was simulated. Had the Master Scenario Events List progression of spreading Plague been allowed to play out as designed, a more orderly medical response would have been anticipated

1. Observations

- The throughput of the PODs fell short of the goal of processing 1,000 persons per hour, which was established in the New Jersey Mass Prophylaxis Manual. The average rate achieved among the 22 New Jersey PODs was approximately 500 people per hour. Reasons for the discrepancy should be identified.
- The plan to conduct prophylaxis on this scale evolved during the course of the exercise and did not appear to reflect a preplanned and carefully integrated Federal and State response.
- It is not clear that the Federal government has a strategy or plan for implementing its own system of PODs or for rapidly identifying and supplying staff to support State efforts in the event of a large-scale requirement.

2. Recommendations

- States need to work with the Federal government to develop scalable prophylaxis plans that address the need to reach very large numbers of people. T3 indicates the difficulty of doing this while an event is unfolding.
- Integrate Federal and State planning processes to ensure that mass prophylaxis plans will be executable if needed.
- The Federal government should decide whether it will be in the business of establishing and operating its own PODs in the event of a major public health emergency as occurred during T3.

B. Homeland Security Advisory System (HSAS), State Threat Conditions, and Associated Protective Measures

The Homeland Security Presidential Directive (HSPD)-3 created the HSAS to improve coordination and communication in the event of terrorist attacks. First, the HSAS informs FSL governments and the public of the perceived credibility and imminence of threats. Second, it directs a systematic, coordinated governmental response to such threats to "reduce vulnerability or increase response capability." To date, elevations of the HSAS threat condition to Red have only occurred in response to notional attacks during exercises. The HSAS level has never been elevated to Red in an exercise or real-world setting on a preattack basis.

Implementation of the HSAS, and specifically the Red threat condition, has been closely examined and critiqued in three previous exercises—the T2 FSE, T3 Command Post Exercise (CPX), and SOE FY04-4 *Crimson Dawn*. The T3 FSE demonstrated that the HSAS is still not used in a systematic manner, and therefore it is not effectively achieving the objectives listed in HSPD-3.

1. Observations

- Real-world and exercise elevations of the HSAS level to Orange and Red reveal that implementation of the HSAS is not systematic.
- There does not appear to be a formal mechanism for coordinating, reporting, and tracking changes to HSAS and State threat levels and implementation of associated FSL and private sector protective measures.
- The absence of a mechanism for coordinating the implementation of protective measures under changing HSAS levels contributed to an uncoordinated response.
- Unintended consequences of implementing HSAS Red protective measures were not well-understood.
- Officials in the T3 FSE used the HSAS and State homeland security advisory systems as a means to facilitate emergency response operations more than as threat advisory systems.
- Inconsistent messages and little specific public guidance limited the value of the HSAS as a warning/advisory system.

2. Recommendations

- Develop a formal process for coordinating and tracking implementation of severe (Red-level) protective measures across FSL governmental agencies and the private sector.
- Provide more specific guidance regarding the color-coded threat conditions than the general guidance currently provided in HSPD-3, and link the levels to specific protective measures.
- Re-examine and refine the desired purposes of the HSAS: public warning/advisory, attack prevention, and/or emergency response.

C. Stafford Act Declarations

There were several declarations and proclamations of emergencies and disasters during the T3 FSE. State and local jurisdictions in both exercise venues invoked their authorities to declare emergencies and also requested Federal assistance under the Stafford Act. These requests led to presidential declarations of a major disaster in Connecticut and an emergency in New Jersey.

As in the T2 FSE, participants discussed the applicability of a major disaster declaration under the Stafford Act to terrorist attacks, especially to attacks that feature nonexplosive

biological weapons. Although the governor of New Jersey requested a major disaster declaration, New Jersey received an emergency declaration.

1. Observations

- It remains unclear whether an incident with a non-explosive biological, chemical or radiological weapon would fit the definition of a major disaster under the Stafford Act.
- Other Federal programs may provide assistance in lieu of a major disaster declaration; however, the pursuit of these programs diverts State and local resources from other response and recovery activity.
- Provisions within the Stafford Act provide for the possibility of exceeding the $5 million limit in assistance funding that would most likely be invoked after a terrorist incident.
- Lack of feedback to agency staffs on verbal approvals of presidential declarations caused initial uncertainty regarding the type of declaration and assistance approved.

2. Recommendations

- Determine the applicability of a Stafford Act major declaration to non-explosive incidents involving WMD, particularly those involving a large-scale bioterrorism incident.
- If these types of incidents do not fit the definition of a major disaster declaration, determine whether exemptions within the Stafford Act for emergency declarations and other Federal programs can result in an equivalent level of assistance and are made aware to the States.
- Consider legislation to ensure the Stafford Act major disaster declaration covers all hazards and is applicable to terrorist events.

- Until legislation is passed, that would allow these types of incidents to receive the full range of Federal assistance provided under a major disaster declaration, identify other Federal programs that may be able to provide assistance.

D. Integrating Responses to Incidents of National Significance: Public Health Emergency and the Stafford Act

The Secretary of the Department of Health and Human Services (HHS) declared a public health emergency in New Jersey under the authorities of the Public Health Service Act. As discussed earlier, the president approved Stafford Act declarations for the incidents in New Jersey and Connecticut. Additionally, the T3 FSE tested the recently released National Response Plan (NRP). It was the first opportunity to examine the guidance the NRP provides in coordinating incidents of national significance (INSs).

The T3 FSE revealed that the NRP does not provide adequate guidance for coordination of Federal operations and support under a public health emergency when a Stafford Act

declaration is in effect. Specifically, the processes were unclear regarding the process required to request and coordinate Federal assistance under other Federal authorities in conjunction with a Stafford Act declaration. The relationship between the public health emergency and the Stafford Act declarations was further clouded by HHS' lack of an established process for coordinating Federal-to-Federal support. Additionally, the funding responsibilities of State and local governments under a public health emergency were not clearly defined.

1. Observations

- Neither the NRP nor the HHS concept of operations (CONOPS) provides sufficient guidance for coordinating assistance for incidents covered under a Stafford Act declaration in conjunction with a public health emergency (or other Federal authorities). In some cases, the information conflicts.
- HHS does not have a detailed process for requesting and coordinating Federal-to-Federal assistance.
- Funding capabilities and responsibilities under a public health emergency are unclear.

2. Recommendations

- Clarify the process for Federal-to-Federal support for non-Stafford Act assistance in conjunction with a Stafford Act declaration.
- Develop a transition plan for coordinating incidents that start under non-Stafford Act authorities but later grow to include a Stafford Act declaration.
- Develop a process for Federal-to-Federal support under a public health emergency.
- Clarify the funding capabilities and responsibilities of the State, HHS, and other Federal agencies under a public health emergency.

E. Emergency Response Operations under a Unified Command

The National Incident Management System is the federally-mandated system for managing emergency responses. NIMS uses the Incident Command System (ICS) to integrate an organizational structure that can scale up or down to effectively meet the demands of an incident. It allows for an integrated organizational structure that can scale up or down to effectively meet the demands of an incident. When multiple organizations or jurisdictions have responsibility over aspects of the tactical response, a UC may be formed to link organizations or municipalities together, provide a forum for integrated decision making, and allow a coordinated approach to incident response.

The T3 FSE provided an opportunity to exercise the integrated ICS approach in Connecticut with the formation of a UC.

1. Observations

- There was inadequate integration between the off-site Unified Command Post (UCP) and activities at the incident scene.
- Integration of the UCP with other emergency response organizations and EOCs remains a challenge.
- Concern exists regarding the alignment between the National Oil and Hazardous Substances Pollution Contingency Plan (NCP) and NRP, which plays out most significantly at the UC.

2. Recommendations

- Rework the information flow processes involving the UC to include local and State EOCs, even when using direct Federal support or NCP authorities.
- Discuss the development of a National IMAT with interagency membership, as opposed to a Coast Guard-only IMAT
- Expand the NRP to include discussion of the UC—its scope of responsibilities and interactions with other emergency response centers.
- Develop criteria for an IC to use to determine the circumstances under which it is appropriate to stand-up a UC.

F. JFO Operations

The T3 FSE provided an opportunity to exercise the recently codified JFO concept and identify issues that could impede the JFO's ability to support emergency response operations. The events in Connecticut and New Jersey prompted Federal officials to activate JFOs and select PFOs for both States. During the exercise, the JFO and PFO staffs focused their efforts on integrating the Federal and State response efforts by arranging resource support, coordinating response policies and operations, and sharing information.

Observations made during the exercise indicate that JFO operations were problematic in both States. The JFO staff encountered problems coordinating their activities and support with State officials. More prominently, the JFO staff also had trouble coordinating the activities among the JFO staff elements.

1. Observations

- The lines of authority and coordination inside the JFO were unclear.
- The presence of the PFO cell complicated JFO operations.
- The JFO did not always follow standard processes for sharing information internally.
- Resolving these internal structural and process issues would ultimately strengthen the JFO's ability to coordinate Federal and State response efforts (i.e., address the JFO's external coordination efforts).

2. Recommendations

- Clarify the lines of authority for the PFO, FCO, and JFO cell.
- Document the role and responsibilities of the PFO cell in the NRP and JFO standard operating procedures (SOP).
- Develop and implement processes and procedures that JFO staffs can use to share information internally.

G. Agent Confirmation and Hazard Area Definition

In a chemical, biological, or radiological attack, early identification of the agent combined with clear definition of the hazard area and the potentially exposed population can save lives, speed effective treatment of symptoms, and prevent injury to medical responders. Until recently, there was no single Federal source for collecting data and producing the modeling products used by decision makers. The T3 FSE provided the opportunity to observe the progress made in creating a single authoritative Federal source for plume modeling. It also highlighted issues regarding the coordination of data and information to confirm the agent and define the hazard area.

The T3 FSE highlighted the potential for tension when many organizations participate in the sampling process and when information about the agent is not systematically distributed among response organizations. In Connecticut, the Interagency Modeling and Atmospheric Analysis Center (IMAAC) was the sole Federal source of plume modeling. Observations indicate that this single-source approach resolved much of the confusion about plume models noted during previous exercises. IMAAC products provided authoritative plume predictions that were used by all the response organizations to define the hazard area and make associated decisions; however, problems with version control as well as lack of consolidation and confirmation of model inputs were evident.

1. Observations

- Specialized incident site response units did not exhibit a clear understanding of each other's roles, authorities, and SOPs.
- The lack of a formally defined information flow process from the incident site resulted in premature public messages and decisions regarding the identity of the chemical agent.
- The IMAAC did not appear to have adequate procedures to deal with discrepancies or contradictions in inputs or modeling requests from various agencies.

2. Recommendations

- Clarify response organizations' roles and responsibilities at the incident site, including the timing of those responsibilities and their value to the larger response operation.

- Continue to develop IMAAC processes for receipt and review of other modeling products and establish a protocol for other modeling agencies to distribute to their product and their guidelines for use.
- Clarify the responsibilities, authorities, and mechanisms for the IMAAC to formally disseminate critical information learned through its scientific analysis of the incident.

H. Resource Reqnests and Resonrce Coordination

The T3 FSE provided an opportunity to exercise the process of providing Federal support to States that have been overwhelmed by a significant terrorist attack involving WMDs. After the releases of *Y. pestis* and mustard agent, officials in New Jersey and Connecticut, respectively, requested a variety of resources from the Federal government, including medical supplies, healthcare professionals, transportation support, security personnel, mortuary affairs teams, and decontamination units. In addition to these State requests, Federal agencies pushed assets to support the State responses.

Observations indicate that the process of resource allocation was problematic in both States. State and Federal officials were uncertain about what had been requested, who had requested it, and what was being provided. These issues and the delays they caused encumbered the allocation of resource process in the T3 FSE and frustrated participants. Resolving these issues would strengthen the ability of State and Federal officials to match the resource needs of responders with available assets.

1. Observations

- Participants used three different processes for allocation of resources that were not well coordinated.
- Federal and State officials struggled with the implementation of these processes to allocate resources.
- Reliable information about resources was not readily available.

2. Recommendations

- Develop a unified Federal emergency process for the allocation of resources.
- Provide States with a team of subject-matter experts on the allocation of resources.
- Document the mission assignment process within the NRP.
- Clarify the role of the Secretary's Emergency Response Team (SERT) during emergencies that also involve a JFO.

I. Information Sharing in the T3 FSE

Accurate and timely sharing of information and the resulting development of a Common Operational Picture (COP) are critical for the success of an integrated FSL response to domestic emergencies. Despite efforts to improve communications and information

sharing across response organizations, the lack of shared situational awareness and the dissemination of incorrect information remain significant roadblocks to a coordinated emergency response.

Other sections of the AAR touch on information sharing and the coordination problems associated with resource requests and coordination, agent identification, status of advisory levels, and integration of operations centers into the response, among others.

1. Observations

- Information systems used in T3 were largely stove-piped within agencies and/or response communities.
- The vast number of operating centers activated during T3 negatively affected information sharing by increasing the scope and complexity of the problem.
- The use of informal or alternate channels for sharing information caused problems by enabling circular reporting and bypassing authoritative sources.
- The T3 FSE revealed a lack of uniform reporting guidelines and procedures for validating information received from secondary or tertiary sources.
- Agencies and operations centers acted and made decisions on different information.
- Situational awareness was not effectively shared across operating centers and agencies.

2. Recommendations

- Support the development of interoperable information systems and/or a suite of emergency response/management applications that can be used across response communities.
- Assess the role and responsibilities of each EOC and consider reducing their number, consolidating them, or collocating personnel.
- Require that all casualty numbers are attached to a clear description of the information included in the report.
- Identify key terms that are likely to appear during a WMD response, standardize their definitions, and then disseminate the information across the entire response network.
- Establish mechanisms to update and disseminate new definitions during response operations.
- Consider the development of a DHS field operations guide that lists radio frequencies/preferences of federal, state and local responders to expedite the development of communications plans.

- To build an accurate and effective common operating picture, the response network needs to:
  - Identify and define the overlapping critical information required by all the responding communities.
  - Establish specific reporting protocols and guidelines for all levels of government.
  - Identify the authoritative sources for EEIs and which EEIs should he included.
  - Identify an operating center at each level of the response to act as "keeper of the critical information."
  - Develop protocols for horizontal and vertical coordination (i.e., horizontally across one level of government and vertically between levels) to align the operational pictures developed and maintained by different operating centers.

J. Emergency Public Information

The term "emergency public information" reflects an understanding that public information during an emergency might differ from normal, day-to-day public information provided to citizens by the government. In the event of a major disaster or emergency, this often means the coordination, development, and delivery of time-critical, lifesaving information to potentially affected people. In a climate of heightened uncertainty and concern, the timing and content of official statements can save lives. The media and general public are likely to scrutinize these statements, and some statements could incur heightened legal or political liabilities.

The policies, procedures, and mechanisms employed by participating FSL departments and agencies and/or nongovernmental organizations to communicate with the public were aggressively stressed during the T3 FSE. Governmental interaction with media outlets was tested through *VNN Live*; VNN.com; and notional radio, print, and other media outlets (press releases). Other means of reaching the public with official lifesaving information included the use of hotlines, call centers, agency website postings, e-mails, blast faxes, flyers, and reverse 911 to phones of citizens. NRP-related coordination structures and mechanisms used by FSL departments and agencies to develop and deliver messages to the public were examined.

1. Observations

- DHS demonstrated numerous tools that were implemented based on lessons learned from the T2 FSE and were designed to help coordinate a consistent message, including its Ready Room, National Incident Communications Conference Line (NICCL), and Public Affairs Guidance.
- FSL departments and agencies may still not be prepared to provide swift, accurate, consistent lifesaving protective action guidance to the public.
- The operations of multiple Joint Information Centers (JICs) were not always well coordinated, and a Joint Information System (JIS) was not used.

- DHS' preexercise coordination with international participants may offer a model for international public affairs coordination in a terrorist attack.

2. Recommendations

Develop a supporting JIS CONOPS to complement emergency support function (ESF)-15 and Public Affairs Annexes of the NRP and Incident Communications Emergency Response (ICER) to provide more specific operational implementation guidance for executing public affairs in the context of the NRP and NIMS.

- Consider using future exercises to further test and refine protocols and educate stakeholder organizations on how mechanisms for public affairs coordination (e.g., NICCL) can be used to promote a COP and coordinate message content.
- Establish primary information sources early in the incident, such as the State hotlines and websites activated in New Jersey and Connecticut.

VIII. Additional Issues

A. State of New Jersey T3 Cyber Exercise

The New Jersey T3 Cyber Exercise, a one-day interactive tabletop exercise, was conducted on March 30, 2005, at the Office of the Attorney General complex in Trenton, New Jersey. This exercise examined the integration of inter- and intragovernmental actions related to a large-scale cyber attack and synchronized with a terrorist WMD attack in an operational context. The exercise examined disruptions to networks, the consequences of those disruptions, responses, and the implications for protective measures. It was divided into the following three sessions:

- Session 1 exercised a variety of communications paths and explored complex policy questions. New Jersey and Hudson County incident response capabilities and practices were examined.
- Session 2 exercised the players' ability to correlate information to determine complex attack vectors. Players examined their capability to identify remediation actions and potential unauthorized information exposure.
- Session 3 exercised force multiplier effects and assessed their consequences. It included a major WMD event for State agencies and a power failure involving key county facilities and networks.

1. Issues/Recommendations

- Develop a leadership mechanism to provide oversight for New Jersey State cyber security and continuity of operations.
- Develop a service agreement to define obligations and expectations of the provider and users, even though an Internet Service Provider resides within the broader State organization.
- Conduct a statewide risk assessment of all IT-related capabilities.

- Create and distribute best practice documentation in areas such as configuration management, acceptable use, and incident response.
- Draft a recovery plan to address the process, priorities, and any exceptions that may be required in the event of a takedown of the entire State network.
- Establish and document a clearly defined threshold for reporting criminal intent or behavior to law enforcement.

B. State of Connecticut T3 Cyber Exercise

The Connecticut T3 Cyber Exercise was conducted on March 22–23, 2005, at the Connecticut Department of Information Technology headquarters in East Hartford, Connecticut. There were approximately 80 participants, including top officials and network operation centers (NOCs) from the Connecticut State Department of Information Technology, Connecticut Department of Transportation, Connecticut State Police, Connecticut Education Network, and City of New Haven.

The NOCs used a simulated network developed by the Institute for Security Technology Studies (ISTS) as the primary source of exercise-related stimuli. The network replicated elements of regional, wide-area networks and an intergovernmental network. The exercise encompassed three cyber attack scenarios, each associated with different aspects of the cyber security problem:

- Scenario 1, *Disjointed Attacks*, featured an "above normal" level of network disruptions. Players reviewed both the internal and external communication flows of their NOCs and discussed relevant cyber security issues.
- Scenario 2, *Coordinated Attack*, was a low-level, coordinated cyber attack against stakeholder organizations. Players addressed response issues and identified the actions necessary to respond to these attacks in a combined manner and resume network operations.
- Scenario 3, *WMD Force Multiplier*, was an overwhelming, coordinated cyber attack acting as a "force multiplier" for a combined terrorist WMD attack. NOCs addressed the necessary actions to reestablish or maintain network operations to permit crisis and consequence management.

1. Issues/Recommendations

- Connecticut or DHS needs to develop cyber-related plans and procedures associated with HSAS levels.
- Network organizations and their functions, with regard to plans, policies, and procedures regarding cyber-terrorism within Connecticut, need to be identified.
- Doctrine needs to reflect the importance of radio communications and non-voiceover Internet protocol (VoIP).

C. Intelligence Play

DHS made *information sharing* one of four key objectives in the T3 FSE. To ensure that information sharing was appropriately exercised, an Intelligence Working Group (IWG) was formed. The IWG defined and charted the real-world information-sharing channels that presently exist. This enabled T3 planners to create "preventable acts" that could be put into play through streams of intelligence for analysts to evaluate and intercede if the assessment dictated.

The real-world intelligence issues noted during the exercise were primarily related to intelligence channels, disconnects, and other contentious or undefined areas in the intelligence community and information-sharing arena.

1. Issues/Recommendations

- Improve systems used to contribute to and create a common intelligence picture.
- Develop further the validation of interagency processes for information sharing.
- Create and maintain an Interagency Handbook for Information Sharing to enhance interoperability.
- DHS should develop a detailed plan for the intelligence component and information flow under the NRP.
- DDNI/Collection should form a Request for Information (RFI) working group to review processes, review systems, and provide recommendations for enhancing the visibility of RFIs and responses to RFIs between departments and agencies.
    - The establishment of an RFI fusion center at the National Counterterrorism Center (NCTC) should be considered.
- Promote analysts' awareness of and access to the span of interagency tools to "pull" intelligence.

D. Private Sector Integration

The National Strategy for Homeland Security states that the Federal government is responsible for fostering "unprecedented levels of cooperation" between the private sector and all levels of government. HSPD-5 emphasizes "the role that the private and nongovernmental sectors play in preventing, preparing for, responding to, and recovering from terrorist attacks, major disasters, and other emergencies."

Exercise design constraints were a limiting factor in private sector integration for T3. In addition to the stringent requirements placed on participating organizations, initial apprehension at the development of the private sector piece created a need for different levels of participation and a number of artificialities. The following issues were raised in the private sector portion of the exercise:

- **Prototype private sector coordination mechanisms:** Two private sector coordinating mechanisms were prototyped during the T3 FSE: a Private Sector Liaison at the New Jersey and Connecticut Office of Emergency Management

(OEM), and a Private Sector Cell at the National Infrastructure Coordinating Center (NICC). As a result of the success of both models, players requested that the models be institutionalized for real-world incidents.

- **Public/private coordination and communication:** The issues arising from the communication between the government and the private sector dominated the feedback from the private sector players. The issues surrounding the interfacing of public and private fell into three categories: (1) lines of communication, (2) method of communication, and (3) coordination.
- **Testing internal emergency response/business continuity plans:** For the employees of many private sector organizations, T3 raised the level of awareness of the critical roles of business functions during an event. The cascading effects of absenteeism, especially of critical employees, can shut down organizations and subsectors. T3 also provided a useful, realistic opportunity for private sector organizations to test their internal response and business continuity plans.
- **Cross-sector coordination and communication:** The T3 FSE illustrated that the current level of coordination and communication between various subsectors of the private sector is indispensable to an effective response, but also generally insufficient to respond effectively and efficiently to an event of this magnitude. The issue of creating an industry analog to the IIMG was offered, particularly as it relates to improving cross-sector integration for planning and evaluation.

IX. Conclusion

The T3 FSE was an innovative, challenging, and highly productive exercise designed to stress the system and the agencies responsible for responding to a terrorist attack. The observations, assessments, and recommendations in this summary were garnered from a number of forums and were validated from a practitioner's standpoint.

As the largest and most complex counterterrorism exercise ever attempted, the T3 FSE provided a tremendous opportunity for private sector and FSL governmental participants to test their procedures and push their agencies to their limits. Many departments and agencies were successful in stressing their policies and procedures and identifying potential shortfalls. In addition, the exercise provided many important lessons regarding FSL interagency procedures for communications and the integration of support measures.

Because of the extensive data collection process and the effort to make T3 FSE findings well documented and traceable through a detailed reconstruction of the exercise events, the full AAR provides a baseline on which subsequent TOPOFF and other counterterrorism exercises can build and be rigorously compared.

Part 1: Exercise Overview

Exercise Name:

Top Officials (TOPOFF) 3 (T3) Full-Scale Exercise (FSE)

Duration:

T3 Planning and Relevant Events: June 2003–October 2005

Exercise Date:

April 4–10, 2005 - Full-Scale Exercise

Sponsor:

Department of Homeland Security

Federal Exercise Project Officer:

DHS, Office of Grants and Training, Program Manager - Butch Colvin

Type of Exercise:

Full-Scale Exercise

Funding Source:

Department of Homeland Security
Department of State

Program:

Homeland Security Exercise and Evaluation Program

Focus:

_X_ Response _X_ Recovery _X_ Prevention

Classification:

~~For Official Use Only (FOUO)~~

Scenario:

Biological and Chemical Release

Location:

Washington, DC, New Jersey, Connecticut, Canada, and the United Kingdom

Participating Organizations:

Canadian Agencies
Agriculture and Agri-Food Canada
Canadian Border Services Agency
Canadian Food Inspection Agency
Canadian Security and Intelligence Service
Citizenship and Immigration Canada
Communications Security Establishment
Department of National Defense
Department of Justice
Environment Canada
Foreign Affairs Canada
Fisheries and Oceans
Health Canada/Public Health Agency of Canada
Industry Canada
Natural Resources Canada
Public Safety and Emergency Preparedness Canada
Royal Canadian Mounted Police
Social Development Canada/Human Resources and Skills Development Canada
Transport Canada
Canadian Red Cross
United Kingdom Agencies
Cabinet Office
Department for the Environment, Food and Rural Affairs
Department of Health

Department for Transport (and TRANSEC)
Foreign and Commonwealth Office
Government Communications Headquarters
Health Protection Agency
Health and Safety Executive
HM Treasury
Home Office
Joint Terrorism Analysis Centre
National Health Service
Ministry of Defense
Office of the Deputy Prime Minister
Office of Science and Technology
Secret Intelligence Service
Security Service
Association of Chief Police Officers
City of London Police
Metropolitan Police
United States Federal Agencies and Organizations
American Red Cross (ARC)
Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)
Centers for Disease Control and Prevention (CDC)
Central Intelligence Agency (CIA)
Department of Agriculture (USDA)
Department of Commerce
Department of Defense (DoD) Office of the Secretary of Defense U.S. Army Corps of Engineers USNORTHCOM National Security Agency (NSA)
Department of Education
Department of Energy (DOE)
Department of Health and Human Services (HHS)
Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA)
Department of Housing and Urban Development (HUD)
Department of Justice (DOJ)
Department of Labor (DOL)
Department of State (DOS)
Department of the Interior (DOI)

Department of Transportation (DOT)
Department of Treasury
Department of Veteran's Affairs (VA)
Environmental Protection Agency (EPA)
Federal Bureau of Investigation (FBI)
Federal Aviation Administration (FAA)
Food and Drug Administration (FDA)
General Services Administration (GSA)
Homeland Security Council (HSC)
National Aeronautics & Space Administration (NASA)
National Oceanic & Atmospheric Administration (NOAA)
Nuclear Regulatory Commission
Occupational Safety and Health Administration (OSHA)
Office of Management and Budget (OMB)
Small Business Administration (SBA)
U.S. Postal Service (USPS)
U.S. Marshals Service
Non-Governmental Organizations
American Red Cross of Central New Jersey Emergency Services
The Salvation Army
State and Local Agencies
Kean University
Middlesex County Office of Emergency Management - Emergency Services Center
Middlesex County Office of the Fire Marshal - Emergency Services Center
Middlesex County Prosecutor's Office
New Jersey Board of Public Utilities - Bureau of Emergency Management
New Jersey Department of Banking and Insurance
New Jersey Department of Community Affairs
New Jersey Department of Corrections
New Jersey Department of Health and Senior Services
New Jersey Department of Health and Senior Services - Emergency Medical Services
New Jersey Department of Health and Senior Services - Emergency Preparedness & Response
New Jersey Department of Health and Senior

Services - Communications and Risk Information
New Jersey Department of Human Services
New Jersey Department of Labor
New Jersey Department of Laws & Public Safety - Attorney General's Office
New Jersey Department of Laws & Public Safety - Office of Counter-Terrorism
New Jersey Department of Laws & Public Safety - Public Information
New Jersey Department of Military and Veterans Affairs
New Jersey Department of Transportation
New Jersey Department of Treasury
New Jersey Department of Environmental Protection
New Jersey Division of Mental Health Services
New Jersey National Guard
New Jersey Network (NJN)
New Jersey Office of Recovery and Victims Assistance (ORVA)
New Jersey State Fire Coordinator
New Jersey State Medical Examiner
New Jersey Office of Emergency Management
New Jersey State Police - Emergency Management Section
New Jersey State Police - Homeland Security Branch
New Jersey Transit
Port Authority of New York and New Jersey
Rutgers University
Union County Division of Emergency Management
Union County Health Department
Union County Prosecutor's Office
City of Groton Fire/Police
City of New Haven Fire/Police
City of Norwich Fire Department
Connecticut Children's Medical Center
Connecticut Civil Air Patrol (CAP)
Connecticut CT-1 Disaster Medical Assistance Team (DMAT)
Connecticut Department of Corrections (DOC)
Connecticut Department of Emergency

Management and Homeland Security (DEMHS)
Connecticut Department of Environmental Protection (DEP)
Connecticut Department of Mental Health and Addiction Services (DMHAS)
Connecticut Department of Public Safety (DPS)/Connecticut State Police (CSP)
Connecticut Department of Public Safety State Fire Marshall
Connecticut Department of Transportation
Connecticut DHS Immigration and Customs
Connecticut Federal Bureau of Investigation (FBI)
Connecticut Ledge Light Health District
Connecticut National Guard
Connecticut Occupational Safety and Health Administration (OSHA)
Connecticut State Fire and Rescue Plan
Connecticut Sub Base Fire Department
Connecticut United States Coast Guard (USCG)
Connecticut Urban Search and Rescue (US&R)
Connecticut U.S. Customs and Border Protection
Connecticut U.S. Department of Homeland Security Transportation Security Administration
Mashantucket Pequot Tribal Nation Fire
Mohegan Tribal Government Fire/Police
Montville
Mystic Fire Department
New London Fire/Police
New London Health Department
New London OEM
Northern/Southern Tier Hospitals
Pequonnock Bridge Fire Department
Town of East Lyme Fire/Police
Town of Groton ECC
Town of Groton Police
Town of Ledyard
Town of Waterford Fire/Police
UNCAS Health District
University of Connecticut (UCONN)

Number of Participants:

- Participants 22,000+
- Controllers/Evaluators 1,700+
- Observers 600+

I. Exercise Overview

A. T3 Authorization

The Top Officials (TOPOFF) series of exercises is a Congressionally mandated, national counterterrorism progression of exercises designed to identify vulnerabilities in the nation's domestic incident management capabilities. It actively exercises the plans, policies, procedures, systems, and facilities of Federal, State, and local (FSL) response organizations against a series of integrated terrorist threats and acts in separate locations in the United States.

The TOPOFF exercise series' authorization is anchored in Public Law 106-553. Senate Report 106-404 outlines the program conceptually. TOPOFF events also fulfill a requirement of the National Security Council's Policy Coordinating Committee on Counterterrorism and National Preparedness Exercise Sub-group for the conduct of a large-scale, national-level, counterterrorism exercise.

Whereas TOPOFF 3 (T3) planning began under earlier Presidential Directives, the Homeland Security Presidential Directive (HSPD)-5 articulates the current Federal incident management policy that ultimately provided focus for the exercise event and gave national impetus to the recently adopted and unrehearsed National Response Plan (NRP) and National Incident Management System (NIMS). In conjunction, HSPD-8 provides for the adoption of the following, all of which were incorporated into the T3 series of events:

- National Preparedness Goal, National Planning Scenarios
- Universal Task List
- Target Capabilities List
- Homeland Security Grant Program Guidance
- National Preparedness Guidance

All participating FSL, tribal, private sector, and international (United Kingdom and Canada) authorities were asked to submit exercise objectives to planners at the beginning of the T3 design cycle to ensure that the exercise would support specific participant objectives while also addressing national priorities.

B. Design and Concept

The first TOPOFF exercise (TOPOFF 2000) was a single, no-notice, full-scale exercise (FSE) co-chaired by the Department of Justice (DOJ) and the Federal Emergency Management Agency (FEMA) in May 2000. TOPOFF 2 (T2) was designed as an open exercise in which participants were introduced to the scenario prior to the FSE through a cycle of activities of increasing complexity. T3 (co-chaired by DHS and DOS) was similar to T2 in architecture, although with a less scripted scenario.

T3 was the largest and most comprehensive terrorism response exercise ever conducted in the United States. The exercise scenario, which was played out from April 4–8, 2005, depicted a fictitious, foreign terrorist organization that conducted a simulated chemical (mustard) attack and detonation of a vehicle-borne improvised explosive device (VBIED) in New London, Connecticut, and a release of pneumonic plague (*Yersinia pestis*) in Union and Middlesex Counties in New Jersey. There was also significant 30-day-intelligence play over real-world channels, two cyber exercises, and related terrorist exercise activities in the United Kingdom and Canada.

The United Kingdom (ATLANTIC BLUE) and Canada (TRIPLE PLAY) conducted simultaneous, related exercises with overarching international exercise objectives to improve mutual response and preparedness against global terrorism. The three domestic scenarios were enhanced by incorporating events from the other two countries. The planning and execution of the three national exercises provided an excellent opportunity for international cooperation, networking of key responders, and sharing of information regarding each country's concepts of emergency operations.

T3 included the following seminars and exercises:

- Command Post Exercise (CPX);
- a series of planning conferences including: the Initial Planning Conference, Midterm Planning Conference, Final Planning Conference, and After-Action Conference (AAC);
- a series of national seminars on chemical terrorism, biological terrorism, and public affairs;
- an Advanced Distance Learning Exercise (ADLE);
- a Senior Officials Exercise (SOE) Series (tabletops at the Deputy Secretary level); and
- a Large-Scale Game (LSG) that focused on recovery and remediation requirements (tabletop three-day event series).

Exercise design, exercise play, and exercise review—the three major components of T3—were all cast in deference to the four major objectives of the FSE:

- Incident Management: To test the full range of existing procedures for domestic incident management of a weapons of mass destruction (WMD) terrorist event and to improve top officials' capabilities to respond in partnership.
- Intelligence/Investigation: To test the handling and flow of operational and time-critical intelligence between agencies in response to a linked terrorist incident.
- Public Information: To practice the strategic coordination of media relations and public information issues in the context of a WMD terrorist incident.
- Evaluation: To identify lessons learned and promote best practices.

The purpose of designing an open and unscripted exercise was to enhance its learning and preparedness value through a building block approach, and to enable participants to develop and strengthen relationships in the national response community. Participants at the FSL levels endorsed this methodology as being very beneficial to the validation and coordination of their domestic preparedness strategies.

C. Building Blocks

The T3 FSE was the pinnacle of a series of building block events that occurred over the course of 18 months. Each event preceding the FSE and the one follow-on exercise were designed to build upon the stated goals and objectives established by all participating FSL departments and agencies. During each of these events, key leaders were brought together to identify and address issues pertaining to terrorism preparedness, response, and recovery.

The relevant building blocks began with the National Seminar on Chemical Terrorism, conducted in Mystic, Connecticut, August 25–26, 2004. The seminar was designed to identify critical issues facing FSL, private sector, and international officials following a chemical terrorism attack. The seminar explored preparation strategies for the unique problems created by a chemical terrorism scenario and the best approaches to resolve these issues. The participants included representatives from domestic FSL governments, Canadian and United Kingdom governmental agencies, as well as State and local emergency response agencies from Connecticut and New Jersey.

The National Seminar on Public Affairs was the second T3 national-level seminar, held in Silver Spring, Maryland, October 5–6, 2004. The seminar focused on the ability of the Federal government to coordinate messages across agencies through the NRP. Additional objectives of the seminar included:

- balancing real-world and exercise media demands during the T3 FSE;

- maximizing the rehearsal value for participants of T3; and
- examining/developing strategies to effectively communicate with the media and the public during a WMD event.

This seminar was designed to reach Federal-level public affairs and public information professionals.

The third seminar was held in the Meadowlands, New Jersey, December 1–2, 2004. The T3 National Seminar on Biological Terrorism brought together homeland security leaders from FSL departments and agencies, as well as the Canadian and United Kingdom governments. The seminar offered the opportunity to discuss issues regarding the response to a bioterrorism attack. The event was designed to improve relationships and enhance networking between the FSL levels of government, the private sector, and international partners.

The first local or venue-specific seminar was conducted in Union County, New Jersey, December 9, 2004. The New Jersey Seminar on Public Affairs explored the ability of New Jersey's State public information officers (PIOs) to provide pertinent/timely information to the media and the general public during a large-scale health disaster. The one-day seminar provided New Jersey PIOs effective insight into risk communication management and recommended concepts necessary to prepare "public information" responses to a terrorist incident. The audience and program presenters were comprised of FSL government officials and public information professionals.

The Connecticut Seminar on Public Affairs was the second locally-executed venue-specific seminar. It was conducted in Mystic, Connecticut, December 16, 2004. This seminar enabled Connecticut State PIOs an opportunity to discuss the policies, plans, and procedures in place to manage information and effectively communicate in the event of a major health incident. The seminar also addressed the issue of FSL partners working together to manage information during a major incident. The seminar was conducted over one day and included a public affairs training program designed by the U.S. Coast Guard (USCG) and a program comprised of a series of presentations on the different perspectives of risk communications.

The third local seminar was held in Gloucester County, New Jersey, January 21, 2005, and dealt with chemical terrorism. This program explored the specific issues of response and recovery facing New Jersey in the event of a chemical terrorist attack. The goal of the seminar was to enable the target audience to make appropriate decisions during a chemical WMD attack utilizing NIMS principles. The seminar also provided education and training on information and intelligence sharing and increased awareness of the threat assessment process. During the one-day seminar, participants observed briefings and presentations and engaged in a facilitated scenario-based discussion. The participants included Federal government officials and New Jersey State and local emergency response agencies.

The final local seminar was held in New Haven, Connecticut, February 23, 2005, and dealt with "terrorism threat awareness." The program provided background on the terrorist threat facing the United States and, more specifically, the State of Connecticut. The seminar also facilitated the exchange of information regarding the nature of the threat among the State and local agencies represented. One of the program's principal aims was to enhance the knowledge and understanding of the current global terrorist threat, who the terrorists are, and how this background could be applied to homeland security training, exercises, and mission areas. Participants included representatives from Connecticut law enforcement, first responders, and private sector agencies.

A Command and Control Seminar was conducted by means of the ADLE network, which aired via satellite broadcast, January 25–27, 2005. The seminar provided a forum for discussing control and consequence management of complex chemical or biological terrorist events. The ADLE was available to viewers after the satellite broadcast through the Lessons Learned Information Sharing website, as well as CD-ROM.

The final T3 building block event was the T3 LSG. The LSG was conducted four weeks after completion of the FSE and addressed the nation's ability to recover and manage the long-term consequences of a terrorist attack. The T3 LSG was designed based on the scenario, goals and objectives, and actual outcomes of the T3 FSE. The LSG focused on the most pressing recovery issues, ranging from time periods of 30, 90, and 180 days post-incident. Representatives from all FSL government agencies and the private sector who participated in the FSE were included.

To expose the Interagency with challenges they were likely to encounter during the FSE, two SOEs (tabletop exercises) were conducted. The principal objectives for the two SOEs included:

- exercising the implementation of the Homeland Security Advisory System (HSAS), while identifying related protective measures for implementation and
- identification of outstanding issues affecting the readiness posture of the U.S. government to manage complex WMD events.

In addition, these exercises enabled participants to assess information and intelligence-sharing mechanisms and to identify the actions required to assure cohesive and appropriate domestic and international public notification. Both SOEs exercised top official decision making relative to an operational response in the context of the NRP and NIMS at a SECRET classification level.

The first exercise, SOE 05-2, *Fierce Squall,* was held February 15, 2005, in Washington, D.C. *Fierce Squall* focused on the issues that senior-level officials would face in the wake of a biological terrorist attack. Participants were presented with the latest information and intelligence pertaining to biological WMD events and provided the opportunity to engage in discussion and decision making around this issue.

SOE 05-3, *Roaring Tempest*, was held March 10, 2005, in Washington, D.C. *Roaring Tempest* was conducted in three moves and addressed new intelligence, VBIEDs and chemical attacks, and expanding response/law enforcement security.

II. Exercise Evaluation

A. Evaluation Methodology

The evaluation of the T3 FSE aims to:

- assess and enhance FSL terrorism preparation, prevention, and response capabilities;
- provide objective observations of complex, multifaceted interactions of FSL entities;
- provide recommendations for improving FSL counterterrorism incident management policies and procedures; and
- provide a basis for assessing progress and improvement over time and against the backdrop of evolving policies and procedures.

The T3 FSE evaluation focuses on high-level FSL coordination, support plans, policies, and procedures. In addition to the evaluation presented in this document, organizations that participated in the exercise were encouraged to conduct their own internal evaluations based on their specific objectives, tasks, and procedures.

The following people and elements collected data for the T3 FSE evaluation:

- Data collectors: Data collectors were provided by participating agencies to record what happened in a particular place or among a particular group of participants. They were knowledgeable about the activities of the players they observed (e.g., firefighter data collectors observed firefighter players). In many instances, the participating agencies also used these data to conduct their own internal evaluations.
- Analysts: Analysts were provided by the exercise support team and were responsible for the oversight and coordination of all aspects of data collection and evaluation. After the exercise, the analysts conducted the reconstruction and analysis in accordance with the evaluation methodology discussed in this document.
- Lead Analyst: The lead analyst reconstructed and analyzed the T3 FSE and wrote the reconstruction and analysis sections of the T3 FSE After-Action Report (AAR).
- Players: Players were FSL agency and department personnel who had active roles in the response. They performed their assigned roles and functions in response to the situations in the exercise. Players initiated actions that managed and mitigated the simulated emergencies.

- Controllers: Controllers, using procedures identified in the control staff instructions (COSIN), managed the conduct of the exercise; directed the pace and intensity of exercise play; assured the safety of participants, the public, and the environment; and maintained the security of exercise participants, equipment, and resources. Controllers monitored the sequence of exercise events and the pace of activity. In many cases, controllers were drawn from the trusted agents who planned the exercise.
- Simulators: Simulators, including actors and role players, were control staff personnel who simulated nonparticipating organizations or role-played key nonparticipating individuals.
- Master Scenario Events List (MSEL): The T3 FSE MSEL was the primary exercise control document. It is the chronological list of exercise injects and event implementers that was used to stimulate and guide player action. Each MSEL inject or implementer specified when, by whom, to whom, and what was injected.
- Virtual News Network (VNN): VNN was a mock media production group that supplemented the MSEL. As would be expected during an actual terrorist event, players received public media injects and interactions over VNN.

B. T3 Evaluation Methodology

The T3 FSE evaluation methodology is based on the approach outlined in HSEEP Volume II: Exercise Evaluation and Improvement. The overall aim of the evaluation is to document *what happened* during the exercise and explain *why*. This methodology provides participants and response agencies with information they can use to improve their response policies and procedures regarding incidents of national significance. The analysis also provides information for organizations conducting their internal evaluations. Evaluation consists of the following three steps:

1. Observation: Collecting data
2. Reconstruction: Determining what happened and when
3. Analysis: Determining why specific actions or events occurred

1. Observation

To record what happened in the exercise, dedicated observers known as data collectors were assigned to sites of exercise play. The scale or intensity of play, number of players, and geographic spread of the location determined how many data collectors were present at a given site. Analysts supplemented data collectors at key exercise sites, such as State emergency operations centers or Joint Field Offices (JFOs).

Data collectors were not the only observers who provided data for analysis. Players, controllers, simulation cell (SIMCELL) staff, and VNN also contributed critical data to the analysis. Players provided data by:

- Completing questionnaires (player feedback forms);
- Providing copies of logs, e-mails, and other documentation developed during the T3 FSE;
- Contributing to their organization's lessons learned; and
- Contributing to Hotwashes.

This input was critical to the analysis, as it represents players' perspectives on the exercise and their actions/decisions. Exercise support personnel provided controller logs, SIMCELL logs, and VNN reports to the analysts.

In addition to data collected during the T3 FSE, a Hotwash and AAC results were collected to obtain additional player feedback and the most complete understanding of the critical aspects of the exercise.

2. Reconstruction

Reconstruction produces a fact-based, time-synchronized, de-conflicted, and *meaningful* account of what happened in the exercise. This laborious process is essential for conducting a meaningful analysis. Reconstruction involves the following:

- independent and parallel reconstruction of events at each location by analysts assigned to one or more locations;
- group reconstruction of how the events at each location fit in with those at the other locations (this step typically engenders considerable revision of the individual analyst's initial reconstruction of events at his/her location); and
- creation of a single reconstruction report.

The T3 FSE reconstruction report was completed before this AAR. An abridged version of the complete T3 FSE reconstruction is provided in this report.

3. Analysis

In this final step of the evaluation process, the analysts use the record of events provided by the reconstruction to objectively seek patterns and develop an understanding of why certain issues emerged during the exercise. The analysis of these issues includes detailed descriptions of the issues and, when relevant, potential explanations for the behavior or result. The T3 FSE analysis also identifies areas for improvement and recommends courses of action that are intended to strengthen the ability of FSL organizations to respond to emergencies. FSL agencies should take these results and use them to develop improvement plans.

III. Exercise Reconstruction

The reconstruction provides a timeline of the T3 FSE. The timeline is an overview of the events and activities that took place during the exercise. The T3 FSE reconstruction product is the result of reviewing the observations in nearly 400 data collector logbooks. These observations were augmented with controller observations and chat logs from the Master Control Cell (MCC) and Venue Control Cells (VCCs). Player-generated data, including more than 2,000 e-mails, briefs, website postings, and notes, were also used. These data sources were compiled into a database with more than 10,000 data entries. The database was then sorted by time, taking into account each venue's specific time zone. Decisions and events were identified and filtered for redundancy.

It is important to distinguish between events that were physically executed and those that were notional. The physical activities involved the participation of:

- top officials and representatives of top officials;
- participating agencies' personnel numbering in the thousands;
- more than 400 "injured" persons in Connecticut, represented by role players and augmented by a few mannequins and on-paper patients;
- thousands of role players acting as NJ patients augmented by on-paper patients and the public at the points of distribution (PODs); and
- VNN broadcasts.

Although these parties' actions were affected to some degree by exercise artificialities, they were real in the exercise sense that somebody physically participated and performed the action, thereby encountering some semblance of realistic time delays, possibility of errors, and the issues that real operations entail.

All other actions—the closures of highways, airports, and ferry systems; orders to the population to shelter-in-place; elevations of the HSAS threat condition; spread of pneumonic plague outside New Jersey, etc.—were done in a notional sense. Also, all requests for emergency powers, changes of alert status, and so on were granted only on an exercise basis.

What follows is a reconstruction summary in a tabular format to lend context to the analysis. The table enables the reader to compare the events of one venue with the events of the other venues. Specific times are indicated based upon the data. They are provided not for the purpose of pinning events or decisions down to the exact minute, because the vast volume of data and multiple observer/participant accounts do not allow for such precision. These times illustrate the overall sequence of key events and decisions. The definitions of acronyms are provided in the Acronym List in this AAR.

A more complete, searchable full reconstruction product is provided separately. The full reconstruction enables readers to understand exactly what happened during the T3 FSE and, more importantly, what types of activities and decisions one could expect to

encounter in a chemical weapon or bioterrorism attack. It takes into account the various perspectives of participants and all government levels.

Table 1. T3 FSE Summary Reconstruction

D-Day, Monday, April 4

TIME	NEW JERSEY	CONNECTICUT	INTERAGENCY AND FOREIGN
08:00-09:00 EDT	Symptomatic patients presented to hospitals in NJ. SUV discovered at Kean University.		
09:00-10:00 EDT	Scene around SUV at Kean University was secured by law enforcement officials.		UK considered raising its assessment of the threat in the U.S. from "severe" to "critical."
10:00-11:00 EDT	Cases of presumptive diagnoses of plague were reported.		CDC put out a heightened epidemiological alert. USCG boarding of M/V Red Thunder was completed.
11:00-12:00 EDT	FBI received preliminary results of positive plague test on SUV.	Airborne chemical was released over New London Pier in CT.	Interagency Incident Management Group (IIMG) Director convened an emergency Counterterrorism Security Group (CSG) teleconference. Homeland Security Operations Center (HSOC) Public Affairs Office (PAO) activated the NICCL. UK increased its assessment of the threat level in the U.S. to "critical."
	VNN reported a large number of patients with "flu-like" symptoms reporting to NJ hospitals.		
12:00-13:00 EDT	NJ Governor declared a state of emergency, initiated the activation of the Emergency Operations Center (EOC), and raised the State's threat condition level to Orange.		Secretary of Homeland Security activated the IIMG.
13:00-14:00 EDT		VBIED attack occurred in New London, CT. New London Fire Chief arrived on scene and assumed Incident Command.	Interagency Modeling and Atmospheric Assessment Center (IMAAC) was activated by HSOC.

TIME	NEW JERSEY	CONNECTICUT	INTERAGENCY AND FOREIGN
14:00-15:00 EDT		CT Governor declared a state of emergency, activated the State EOC, and raised the State's threat condition level to Orange. FBI Special Agent-in-Charge (SAC) requested support from the Domestic Emergency Support Team (DEST). CT State Police advised the public to shelter-in-place. FBI reported that a private citizen observed a suspicious airplane land at a private airstrip one mile from Deblois, ME. Four unknown subjects left the airfield in a blue late-model Ford 500.	The Secretary of Homeland Security declared the events in New Jersey to be an Incident of National Significance (INS) and designated a Principal Federal Official (PFO). NICC was activated via Emergency Notification System.
15:00-16:00 EDT	Epidemiological Team from U.S. Public Health Service arrived at NJ DHSS.	There was a presumptive confirmation of mustard gas. DMAT was assembled at Camp Rell. Fisher's Island Sound Ferry informed USCG that ferry services were shut down and residents of Fisher's Island Sound were sheltering-in-place. CT Governor requested a declaration under the Stafford Act.	Secretary of HHS authorized the deployment of Strategic National Stockpile (SNS) to NJ. Secretary of Homeland Security declared the incidents in CT to be an INS and designated a PFO. Driver of a suspicious vehicle was detained by the Canadian Border Services Agency. Three men escaped.
16:00-17:00 EDT	NJ requested DMATs, Disaster Mortuary Operational Response Teams (DMORTs), and CDC epidemiologists.	FBI reported that the Joint Operations Center (JOC) designated the New London incidents as terrorist attacks. Unified Command (UC) formally stood up. The CT National Guard (NG) arrived at the Waterford Police Department (PD) for assignment to the Millstone Nuclear Power Plant.	UK issued travel advisory for the U.S.
	Secretary of Homeland Security raised HSAS level to Orange for the nation and to Red in Middlesex and Union Counties, NJ. The President verbally issued Stafford Act declarations for CT and NJ.		

TIME	NEW JERSEY	CONNECTICUT	INTERAGENCY AND FOREIGN
17:00-18:00 EDT	PFO requested 10 DMATs and 3 DMORTS on alert in support of NJ. CDC-SNS Technical Advisory Response Unit (TARU) was deployed to NJ.	CT Department of Public Health (DPH) requested the CDC Rapid Response Registry. Federal Coordinating Officer (FCO) arrived at the JFO. JFO is activated. CT State DMAT arrived at the incident site.	Secretary of HHS declared a public health emergency in NJ. Royal Canadian Mounted Police (RCMP) stopped vehicle with four suspects; one was in custody, and three remained at-large. Suspect admitted involvement in CT incident.
	AMTRAK closed passenger rail service between Washington, D.C. and Boston.		
18:00-19:00 EDT	Elizabethtown Water Company advised consumers to boil water before use. All county EOCs in NJ are asked to activate. Preliminary case definitions for plague were issued.	EPA requested TAGA. HHS SERT arrived at the JFO.	National Response Coordination Center (NRCC) received CT and NJ Governor's requests for Stafford Act declarations.
19:00-20:00 EDT	NJ EOC informed that SNS is arriving and needs an escort. ARC stopped all blood collections in NJ. All blood collected in NJ and PA within the past three weeks was quarantined.	ATF National Response Team (NRT) was activated for response to the New London incident.	HHS requested 1,000 ventilators for New London incident site.
20:00-24:00 EDT	NJ State Medical Examiner reported 92 deaths to the NJ State EOC. SNS MI arrived at NJ Receipt, Staging, and Storage (RSS) site.	UC turned over incident site to FBI and moved to UCP. CT NG Civil Support Team (CST) field tests showed positive results for mustard. Unified Command (UC) held planning meeting for Incident Action Plan (IAP).	NRCC confirmed a major disaster declaration in CT and an emergency declaration in NJ.

D+1, Tuesday, April 5

TIME	NEW JERSEY	CONNECTICUT	INTERAGENCY AND FOREIGN
24:00-03:00 EDT	SNS push package arrived at NJ RSS site. FEMA informed NJ State EOC that DMORT will arrive in state at 06:00.	SNS ventilators (1,000) and burn/blast kits (1,000) arrived at USCG Station in New London.	CDC reported a total of 36 suspected plague cases in 16 states and Washington, D.C. IMAAC reported that, based on a comparison of field tests with models, sulfur mustard dispersal was both via VBIED and airborne.
03:00-06:00 EDT	NJ NG activated.		VBC News reported multiple patients in UK hospitals with flu-like symptoms. UK Foreign and Commonwealth Office asked if consular officials could access sites in NJ and CT.
06:00-08:00 EDT		UC approved the IAP. PFO and JFO approved incident site sampling plan.	USCG raised Maritime Security (MARSEC) level in Port of NY/NJ to MARSEC II.
08:00-09:00 EDT	First request for medical support to a POD was received by the RSS warehouse lead.	FBI reported that chemical precursors to mustard gas were found on M/V Red Thunder. ECA laboratory confirmed presence of mustard.	
09:00-10:00 EDT	FEMA Region II submitted formal request for Defense Coordinating Officer (DCO) to DoD. State RSS shipped medications to Union and Monmouth Counties.	CT State EOC requested DoD Quick Reaction Force (QRF) to replace CT NG at Millstone Nuclear Power Plant. CT Department of Public Health (DPH) reported 195 fatalities, 4,130 sick/injured, and 8,987 worried well.	FBI requested to conduct interviews of the three arrested by RCMP. UK Cabinet Office Briefing Room (COBR) decided to go to "critical" in the UK.
10:00-11:00 EDT	Union and Middlesex Counties schools were closed.	FBI Hazardous Materials Response Team (HMRT) conducted chemical analysis of 55-gallon drum found on small aircraft. Tests were positive for mustard gas.	HHS contacted World Health Organization (WHO) to discuss implications of the plague outbreak.
11:00-12:00 EDT	State RSS shipped medications to Mercer County.	The highway Information Sharing and Analysis Center (ISAC) issued an advisory to all carriers who have been in CT within the past 36 hours.	HHS asked VA to alert all hospitals and clinics in NJ and CT to be prepared to take in patients and to use VA facilities as staging areas for Federal assets.
	VNN reported that the President had issued a Statement of Concern.		

TIME	NEW JERSEY	CONNECTICUT	INTERAGENCY AND FOREIGN
12:00-13:00 EDT	First real POD opened (Union County).	ARC opened a temporary shelter in Groton, CT.	VNN reports that cruise ship passengers from NJ were not screened for plague as they disembarked at Port St. John. FBI reported that a source reports that a shipment of weapons and ammunition is hidden in a car being shipped to the U.S. onboard the M/V Black Cloud.
13:00-14:00 EDT		New London City Manager closed the New London EOC.	FAA announced that international flights inbound to JFK and EWR would be diverted to BOS, BWI, and PHL airports.
14:00-15:00 EDT	NJ Governor raised threat condition to Red for entire State.	EPA and CT Department of Environmental Protection (DEP) implemented sampling and monitoring plan.	NRCC received request from HHS to set up 2 alternative care facilities, one in each state. C/S Comet Atlantic arrived in Halifax and was quarantined by Public Health Canada.
15:00-16:00 EDT			DOS reported that British consular officials granted permission to visit NJ and CT.
16:00-17:00 EDT			Report of first case of *Y. pestis* in Fredericton, New Brunswick, Canada.
17:00-18:00 EDT	NJ Governor announced plan for distribution of prophylaxis to all State residents. Administrative Order issued closing all schools and colleges in the State FBI identified the location of a safehouse and laboratory related to NJ biological attack.	CT OEM requested ARC feeding and mental health support for 10,000-bed ACF. FBI reported USCG tracking M/V Black Cloud off Nantucket, which may have mustard gas onboard.	DHS and HHS requested ESF-13 to identify security requirements for ACF in NJ and CT.
18:00-19:00 EDT			Secretary of Homeland Security raised HSAS level to Red for entire State of NJ.

TIME	NEW JERSEY	CONNECTICUT	INTERAGENCY AND FOREIGN
19:00-24:00 EDT		FBI turned incident site over to EPA. CT Governor asked President for QRF.	Secretary of HHS approved Emergency Use Authorization (EUA) for ciprofloxacin, and FDA approved the protocol. HHS announced combined Federal and State POD plan.

D+2, Wednesday, April 6

TIME	NEW JERSEY	CONNECTICUT	INTERAGENCY AND FOREIGN
01:00-09:00 EDT	Expanded NJ State PODs (notional) and Federal PODs (notional) opened (08:00). New Jersey State Police (NJSP) and FBI teams initiated assault on safehouse and bio lab.	QRF arrived at Groton airport to conduct relief-in-place with CT NG at Millstone Power Plant.	Bomb exploded in London, UK financial district. Blister and nerve agents potentially involved (09:00 BST).
09:00-11:00 EDT	VNN reported that a temporary morgue planned for 5,000 to 10,000 deaths.		HHS confirmed plague deaths in 26 states, mostly near NJ. This report was consistent with a single POD. DOS reported 120 injured and 58 deaths in the UK (18 U.S. citizens injured and 4 U.S. citizens dead). RCMP located a safehouse. Situation was escalated to an armed encounter with three hostages being taken.
11:00-13:00 EDT	Officials in State EOC decided to lift travel restrictions.	Sampling results confirmed no further contamination to the west and significant degradation due to rain overnight. NRT agreed to provide a panel of technical experts to advise the UC on a plan to decontaminate facilities.	
13:00-15:00 EDT	NJDA submitted request for 2 Veterinarian Medical Assistance Teams (VMATs). NJ State EOC advised NJSP of decision to lift travel restrictions and to dissolve checkpoints at the State borders.	DOJ approved a search warrant for M/V Black Cloud. EPA and CT DEP concluded sampling efforts at the incident site.	UK Prime Minister made public statement that another attack on UK was imminent.

TIME	NEW JERSEY	CONNECTICUT	INTERAGENCY AND FOREIGN
15:00-17:00 EDT	SERT reported a notional POD throughput of 1,044,750. VNN reported 6,508 dead in NJ. Money allotted for refrigerated trucks changes from $500,000 to $5 million. Trucks cannot be rented because once they are contaminated they cannot be used for food again. Notional Federal POD prophylaxis throughput is estimated at 1,194,000.	CT Governor lifted shelter-in-place order. FBI conducted raid on suspected safehouse in CT. Two subjects were taken into custody.	DHS Science and Technology (S&T) reviewed recommendations for deployment of BioWatch detectors to new additional jurisdictions. RCMP prepared to board M/V Castle Maine, which is suspected to have mustard gas onboard. VA responded to requests from HHS to locate 7 VA clinic sites for PODs and provide RNs, LPNs, and physicians for ACF.
17:00-20:00 EDT	NJ State EOC reported that 456 notional PODs were in operation.	CT Secretary of State sent a letter to HHS Secretary's Operation Center (SOC) declining 5,000-bed ACF.	
20:00-24:00 EDT	Law enforcement reported the theft of four ambulances from four hospitals.	FBI Hostage Rescue Team (HRT) assaulted the M/V Black Cloud.	

D+3, Thursday, April 7

TIME	NEW JERSEY	CONNECTICUT	INTERAGENCY AND FOREIGN
24:00-08:00 EDT	Total number of deaths reported as 8,070. Emergency Medical Services (EMS) units arrived at two staging areas, the Meadowlands Sport Complex and the PNC Arts Center for Operation Exodus.		
08:00-10:00 EDT	JFO received the Emergency Declaration amended to include 10 additional counties. A total of 66 EMS/ambulances units were dispatched to hospitals.		
10:00-12:00 EDT	C130 for Operation Exodus arrived at Newark Liberty International Airport (NLIA). Patients were transported from hospitals to NLIA.		
12:00-15:00 EDT	Federal PODs closed. The transfer of patients from ambulances to the C-130 begins. Operation Exodus concludes. NJ Governor announced opening of 20 notional family assistance centers.		Bomb exploded at Waterloo Station, London, UK. HHS, Immigration and Customs Enforcement (ICE), and FBI worked to locate and transport injured UK citizens out of the country.
15:00-18:00 EDT	NJ requested that individual assistance be added to the emergency declaration.		CDC reported 4,600 plague cases and 2,000 deaths in states outside NJ. One American is dead and two were injured in Waterloo explosion.
18:00-21:00 EDT	FEMA Region II Regional Response Coordination Center (RRCC) received letter from NJ Governor requesting the emergency declaration to be changed to a major disaster declaration.		

TIME	NEW JERSEY	CONNECTICUT	INTERAGENCY AND FOREIGN
21:00-24:00 EDT	NJ State PODs closed (23:00).		Copy of FDA EUA for ciprofloxacin was signed and sent to SERT in NJ.

D+4, Friday, April 8

TIME	NEW JERSEY	CONNECTICUT	INTERAGENCY AND FOREIGN
24:00-09:00 EDT			UK reported nine confirmed plague cases (three dead). RCMP boarded M/V Castle Maine.
09:00-ENDEX EDT	VNN reported 8.8 million NJ residents received prophylaxis.		CDC reported 600 deaths from reactions to doxycycline, 200 deaths from reactions to ciprofloxacin.
	Transition back to HSAS Orange level in NJ. Remainder of country remains at Orange.		

IV. Exercise Artificialities

By their nature, exercises are not real events, and no exercise can duplicate the scope and richness of real-world emergencies. Although every attempt is made to mitigate their effects, artificialities will occur and can affect the outcomes of the exercise. If the nature and effects of artificialities are not taken into account, the conclusions drawn from the exercise could be incorrect. This section focuses on the key artificialities noted during the exercise. These artificialities can be placed into the following broad categories:

- those that are inherent to the exercise design process;
- those specifically related to the T3 exercise design; and
- those that arose during actual exercise play.

The net impact of artificialities can be difficult to assess. For example, considerations must be taken into account for questions such as the following:

- Did an artificiality make the response decisions or actions easier than they might have been?
- Did an artificiality unnecessarily complicate the response relative to a real-world operation?

For their part, the T3 exercise designers tried to strike a balance, compensating for one artificiality (e.g., a response team's need, absent a real-world emergency, to take a commercial flight) with another (e.g., the same team's seemingly premature departure).

The two questions to ask when assessing the impact of an exercise artificiality are:

- What difference, if any, did it make to the play of the participants?
- What difference, if any, did it make to the play of top officials?

A. Artificialities Inherent in Exercise Design

There will be artificialities in any exercise involving the response to a WMD event. The fundamental issue is that it is often impossible to exercise the full scope of a real-world event—ranging from an actual bomb detonation to shutting down transportation infrastructure to commanding the full-time attention of top officials. Many exercise events or actions must be notional or simulated, instead of actual. Despite the notional character of some events, governmental agencies and organizations played as though the events actually took place. This allowed the T3 evaluation team to examine decision-making, coordination, and communication issues. As long as they are understood and accounted for in the analysis process, the T3 FSE artificialities should not have a significant impact on interpreting the results of the exercise.

1. Top Officials' Play

The involvement of top officials in T3 was extensive but in real-world emergencies of the magnitude portrayed in this exercise they would be immersed in coping with the emergency, almost to the exclusion of all other activities. In T3, top officials were present only intermittently and largely on a schedule; however, they devoted considerable personal time to the exercise. Some also designated individuals (e.g., a deputy) to play their parts in the exercise when they were not available. The T3 evaluation team believes that top official play during the exercise was relatively unaffected by the artificialities of scheduling, availability, and substitution.

2. Limited Scope of Play

Many effects associated with the intentional release of *Yersinia pestis* and a sulfur mustard agent were not designed into or played in the exercise. Some of the most important include the following:

- exercise play was expanded to include the effects of the releases on states other than Connecticut and New Jersey and
- the potential for population disruption, movement, anxiety, and fear.

3. Notional Actions

Because of limits on the scope of play, the most apparent artificialities were those in which notional (or constructive) actions replaced real ones. Examples include the notional closure of New Jersey borders and roads and the activation of hundreds of notional PODs.

4. Limited Public Involvement

In a real-world event, the public reaction can include clamor for more information, crowds of people fleeing their homes, traffic jams, and disruptive reactions during the public appearances of top officials. Although T3 involved role players acting as patients in New Jersey hospitals and PODs and as persons injured by victims of the blast in Connecticut, the general public was minimally represented. There was no reaction to the emergency from the general public. These reactions could have impacted top officials' decision making and the actions of emergency personnel at the scene; however, precluding their existence was a necessary artificiality.

Many important considerations would include, but not be limited to, those regarding public information, heightened public anxiety, and other psychosocial factors. Such issues would expand beyond the immediate affected communities. For example, other cities in America that were not coping with the ongoing emergency would look for guidance regarding what might later happen in their cities. The lack of involvement from 48 non-affected states and hundreds of non-affected cities is an artificiality that must be taken into account when considering the play of national top officials.

B. Artificialities Specific to the T3 Design Process

The artificialities in this section represent deliberate choices made during the design of T3 or they are specific to this particular exercise. These choices were made with the understanding that they would impact exercise findings. The T3 evaluation team believes that these impacts are accounted for in the exercise analysis.

1. Knowledge of the Scenario

T3 was designed as a building-block process wherein the general exercise scenario was explored in a series of seminars, an LSG, and SOEs. This process was designed to promote learning among the agencies and organizations involved in T3. Indeed, participants felt that they had learned a great deal even before participating in the FSE. It is important to note, however, that while the scenario was widely known, participants did not have access to the MSEL, which drove FSE play.

2. Scope of Participation

A number of important organizations and governments were simulated. Notable examples included the governments of France, Singapore, and Thailand, as well as the real-world media. Additionally, private sector participation was limited. The governments of Canada and the United Kingdom did participate in the T3 FSE; however, their participation was based upon Command Post Exercises (CPXs).

3. Spread of the Pneumonic Plague

During the planning of the exercise, the decision was made not to address the spread of plague outside the borders of New Jersey. Although numbers of plague victims were reported in other states, officials from those states did not simulate the action of requesting assistance (e.g., access to the Strategic National Stockpile (SNS)). In a real-world outbreak of plague, the Federal government would have taken the needs of these states into account when deciding how to support New Jersey's needs, potentially limiting New Jersey's access to Federal resources.

4. Lack of 24-Hour Play

In a real-world emergency, activity would have continued around the clock. During the T3 FSE, some activities functioned around the clock, but others did not. As a result, some participants were occasionally stymied when other participants were not playing at the same time. For example, "overtime" costs limited play commitment from some participants.

5. Prepositioning of Responders

Various assets, such as teams from the DHHS, DoD, FEMA, and the FBI were prepositioned in the venues for reasons of safety, logistics, and cost. The T3 evaluation accounted for advance deployments and ensured that they were accounted for in the subsequent analysis. *6. Varying Participation Schedules*

Numerous city, county, and State agencies participated in the T3 FSE at different times during exercise play. For example, the 90+ hospitals participating in New Jersey operated during different time periods. As a result, some activities that would usually occur in a coordinated fashion were disjointed. This resulted in organizations operating under different conditions (e.g., some during the early phase of the disease outbreak and others later), thereby creating some degree of confusion.

Similarly, the PODs that distributed prophylaxis in New Jersey operated on a staggered schedule. Each POD operated for approximately four hours on different days during the exercises.

C. Artificialities Arising during Exercise Play

A number of artificialities arose during the execution of the exercise. In an exercise as large and complex as T3, this is not an unexpected event. These artificialities were properly accounted for in the analysis of the exercise.

1. Flooding in New Jersey

In the days prior to the exercise, New Jersey experienced heavy rains that caused significant flooding. At times, participants had to suspend their participation in the exercise to respond to the real-world flooding emergency. The flooding also impacted the location of some of the State facilities in Trenton, causing minor disruptions. These incidents are accounted for in the analysis.

2. Issues with Control

During the T3 FSE, there were several minor incidents in which controllers took it upon themselves to modify the scenario. There were also instances in which other exercises or unrelated events were briefly believed to be part of T3 play.

In other instances, controllers provided players with information that the players should have been required to obtain through their participation in the exercise. Many players in the infrastructure that support top officials and their PIO staff were uncertain about how to interact in the exercise. In some cases, they requested information from controllers that they were not able to easily obtain through their formal channels. This contributed to a number of conflicting information threads which were fed to top officials, spokespersons, and press releases and were challenged by the *VNN Live* anchors during interviews. Again, these instances were documented and accounted for in the analysis.

3. Notional Play

There is evidence that some participants did not understand the concept of "notional" play. These participants confused their FSE play schedules with real-world constraints. In an exercise, the play schedule of an organization can be quite different from the decision realm—an organization is bound by certain constraints in an exercise environment (such as availability of personnel and costs) that may limit its ability to physically play. However, it can make "notional" decisions that reflect what it would do in real life, even though the organization may not physically play the decision. In the T3 FSE, some organizations made public announcements that some officials interpreted as incorrect because that organization was not physically playing for another 24 hours. For example, a health organization could decide to open a POD on Day 1 even though it may not be physically exercising the POD until Day 2 (if at all). On Day 2, the organization would play as though the POD had already been open for a full day and was in its "second" day of operation.

In the T3 FSE, an announcement on the opening of a POD in Middlesex County led to significant confusion among decision makers who knew that the POD would not really activate until the following day. This led to inconsistent messages by officials that were picked up and challenged by VNN reporters. The inconsistent messages were largely a result of a lack of coordination and understanding of the difference between notional and actual play, rather than any coordination problems that may have existed among the participants in making and publicizing the decision.

4. Choosing Not to Follow Procedures

Some first responders at the incident site in New London, Connecticut chose to forgo some of their normal response procedures, causing widespread confusion regarding protective action guidance. For example, some of the HAZMAT responders at the site of the chemical explosion did not wear personal protective equipment (PPE); meanwhile, the Governor of Connecticut was implementing and emphasizing a strict shelter-in-place order across the city. *VNN Live* footage of responders not wearing PPE led VNN viewers and reporters to question the rationale for the governor's policy decision. This contributed to some apparent conflicts between FSL government emergency public policy decisions, such as whether the shelter-in-place order was still required.

5. VNN

Many of the top officials and spokespeople had never participated in an exercise like the T3 FSE. Many players appeared to not understand that they were to behave as though they were responding to a real-world event. Late-breaking news which was generated as a result of player actions (rather than being pre-scripted as injects) required spokespeople to be knowledgeable on the unfolding incident and the actions of their agencies, as though they were responding to real-world events. A lack of familiarity among spokespersons about the nature of exercise play led to variances in the quality of preparation and interview effectiveness. Of important note, in the State of New Jersey, some public information exercise play was impacted by real-world ongoing flood responsibilities.

Some informational segments on VNN were pretaped and inserted between live coverage. For example, VNN aired footage of frightened citizens using duct tape to seal off their homes, supposedly in Connecticut in response to the shelter-in-place order. At the time the footage aired, the use of duct tape had not yet been specifically recommended by any official. For this reason, it was an artificiality. However, to the extent that it could have represented an undesired response to a public message (which could and does happen in real life), it could have prompted officials to respond with clarifying messages.

THIS PAGE INTENTIONALLY LEFT BLANK

Part 2: Exercise Goals and Objectives

The following four overarching objectives were established to direct the exercise design process for T3:

- Incident Management: To test the full range of existing procedures for domestic incident management of a WMD terrorist event and to improve top officials' capabilities to respond in partnership.
- Intelligence/Investigation: To test the handling and flow of operational and time-critical intelligence between agencies in response to a linked terrorist incident.
- Public Information: To practice the strategic coordination of media relations and public information issues in the context of a WMD terrorist incident.
- Evaluation: To identify lessons learned and promote best practices.

With these four objectives for a framework, FSL and tribal organizations created their own goals and objectives for evaluation through the exercise process. New Jersey and Connecticut planners identified specific goals that focused the exercise design process on key issues within their respective States.

THIS PAGE INTENTIONALLY LEFT BLANK

Part 3: Exercise Events Synopsis

I. Purpose

This part of the report provides a synopsis of the Top Officials (TOPOFF) 3 (T3) Full-Scale Exercise (FSE) scenario.

II. General

The T3 FSE scenario provided an environment for participants—primarily top-level decision makers—to exercise against a credible terrorist adversary that plans and executes an attack employing weapons of mass destruction (WMD). Although the scenario is plausible, it contains artificialities necessary to create conditions required to achieve exercise goals and objectives. The chain of events depicted in the scenario is hypothetical, and the terrorist groups and individuals portrayed in the scenario are fictional.

A. Prelude to the Attack

1. The Point of Friction

After the terrorist attacks of September 11, 2001 (9-11), oil supply disruptions in Venezuela in 2002 and 2003, and the United States (U.S.) armed intervention in Iraq in 2003, U.S. policy has increasingly emphasized diversification of U.S. energy supplies, especially from sources outside of the Persian Gulf. According to Cambridge Energy Research Associates, between 2004 and 2010, West and Central Africa (far closer to U.S. refining centers than the Middle East) will add 2 to 3 million barrels per day to world production. This will account for one in five new barrels of oil (i.e., 20 percent of new production capacity worldwide). This oil will be the low sculpture, light product that U.S. refiners require. To meet projected rising U.S. demand for natural gas, ample new and reliable external sources will also be required. If projects currently under evaluation and development in Nigeria, Angola, and Equatorial Guinea are brought to fruition in the next decade, they will increase West Africa's annual liquefaction capacity from 9 million to 30–40 million tons. (Current worldwide capacity is 115 million tons annually.) The United States will also increasingly rely on imports of refined products, such as gasoline, as U.S. refinery capacity fails to meet growing demand. West and Central African refiners can help to fulfill these needs.[1]

Since 9-11, U.S. counterterrorism concerns in West and Central Africa have increased significantly, resulting in heightened and evolving engagement in the region by U.S. intelligence and military personnel. This shift has dramatically reversed the calculation that was born in the immediate aftermath of the Cold War in the early 1990s, in which

[1] Goldwyn, David L., and Morrison, J. Stephen, "*Promoting Transparency in the African Oil Sector: A Report of the CSIS Task Force on Rising U.S. Energy Stakes in Africa,*" Center for Strategic and International Studies, March 2004, p 4.

West and Central Africa mattered minimally to U.S. global security interests. Indeed, West and Central Africa venues are becoming priority zones in global counterterrorism efforts, evidenced most overtly by the recent, sudden projection south of the U.S. European Command. Current threats and vulnerabilities in this region include:

- indigenous militant Islamic groups that are concentrated in Nigeria and neighboring states and are linked to externally supported local madrassas;
- the southern migration from Algeria and other North African venues of terrorist movements, most notably the Algerian Salafist Movement, which reportedly has established training bases in Mali and Niger;
- increase in the number of Lebanese trading communities, long-standing support networks for Hezbollah, some of which are reportedly engaged in illicit diamond trafficking, money laundering, and the movement of lethal material; and
- a rising number of minimally protected economic installations, especially in the energy sector, that are overtly tied to Western corporate interests.[2]

Just as it does in the Middle East, oil may eventually form the bedrock of the politics of West Africa over the next few decades as the United States develops the region as an alternative source to the Gulf. A key objective of a global insurgency inspired by the radical Islamist group, el-Zahir, is to deny the United States secure supplies of energy, thereby posing a risk to the U.S. economy.

The expanding threat of international terrorism continues to affect U.S. foreign and domestic security. Both timing and target selection hy terrorists can affect U.S. interests in areas ranging from preservation of commerce to nuclear non-proliferation to the Middle East peace process. Complex terrorist networks have developed their own sources of financing, which range from nongovernmental organizations and charities to illegal enterprises such as narcotics, extortion, and kidnapping. In an attempt to challenge the West's conventional military superiority, there is an inexorable trend toward proliferation of WMD or the means to make them. Policy makers are concerned that states designated by the U.S. State Department as sponsors of terrorism—Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria—may have supplied terrorists with WMD capahility. Although there is a degree of uncertainty, the possibility of covert transfers or leakages clearly exists.[3]

2. The Emerging Threat – Universal Adversary (UA)

El-Zahir, first designated as a foreign terrorist organization (FTO) by the U.S. Department of State in October 1999, is the inspiration for an increasingly violent global insurgency. El-Zahir was established by Yemen-born Alim Badi Al Zaman in the late 1980s. Al Zaman's worldview was influenced by several renowned radical Islamist scholars who taught in the Gulf States. His worldview was also significantly shaped by

[2] Ibid., p 14.
[3] Perl, Raphael, Congressional Research Service, "Terrorism and National Security: Issues and Trends," Updated July 6, 2004.

his experiences in Afghanistan at the end of the Soviet Afghan campaign. Al Zaman returned to Afghanistan in the 1990s to manipulate civil disorder and establish a string of militant training camps.

The infrastructure that el-Zahir established during this time, which was primarily to recruit Muslims to create Islamist states throughout the world, resulted in the growth of a global movement that currently extends directly and indirectly into various countries including: Algeria, Egypt, Turkey, Syria, Pakistan, Malaysia, Indonesia, Saudi Arabia, Yemen, Chechnya, Somalia, Kashmir, Sudan, and Eritrea.

In addition to its core membership, el-Zahir has successfully attracted the support of three other groups of militant Islamists, including groups fighting Islamic rulers believed to have compromised Islamic ideals and interests, groups fighting against oppression and repression of the Muslim population, and groups fighting regimes to establish their own Islamic state. This wide-ranging support structure has enabled el-Zahir to execute a terrorist campaign on several fronts or inspire other militants to execute a terrorist campaign. Furthermore, it allows the "network of networks" to employ a wide range of tactics, from kidnapping and conventional attacks using improvised explosive devices (IEDs) and suicide bombers to unconventional attacks using chemical and biological weapons.

In response to increased U.S. military presence in Central and West Africa, el-Zahir and several of its African-based affiliated and inspired groups have developed a plan to retaliate against the United States and its allies with a series of coordinated strikes against the U.S. homeland and the United Kingdom (UK).

The scale of the attacks is planned to surpass that of the 9-11 attacks. El-Zahir will provide mission support that will include limited financial capital for weaponry, support networks in place in the West, access to front companies, and the recruitment of skilled weapons technicians.

The Fronte Salafiste pour la Liberation de Terre Etrangere (FSLTE), an Algerian-based terrorist organization loosely affiliated with el-Zahir, will provide tactical forces and weapons expertise for this operation. Under the leadership of Ahmed Abdul Aziz (aka "Al Jundi"), the group aims to overthrow the secular government of Algeria and establish an Islamist caliphate that adheres to the Salafist interpretation of Islam. Although the group has denied issuing statements threatening attacks on U.S. assets in Algeria, they are opposed to the U.S. presence in North and West Africa. FSLTE was first designated an FTO by the U.S. Department of State in March 2002.

FSLTE has recruited from the disenfranchised and the embittered. FSLTE has particularly concentrated on recruiting from the criminal fraternity in prisons who have turned to Islam through the work of radical Muslim clerics not necessarily associated with FSLTE or any other noted militant group. Most of the funding for the group's activities is acquired via criminal activities.

To successfully conduct clandestine operations in the West, el-Zahir and FSLTE will rely on two additional organizations. In Europe, they will rely on Nasamaah-At, translated as "active individuals." This movement was established in Egypt in the 1970s by Amir Haleeb. The group began as a highly disciplined movement that was divided into action cells, recruiting groups, and logistic units, and worked toward re-educating the Egyptian population to accept a new community governed by Shari'ah law.

Originally, Nasamaab-At was apolitical and nonviolent. However, after facing growing repression by the authorities, the group was radicalized and ultimately resorted to the use of violence to initiate change within society. Instead of focusing their efforts in the Middle East, Nasamaah-At sent personnel throughout Western Europe to begin their own radical cells deep within Western society. Here, the group has focused on recruiting first- and second-generation Europeans. Thus, Nasamaah-At has evolved into an unstructured entity that is largely ad hoc by nature, but radicalized to the extent that individual cells established throughout Europe have sought to build direct and indirect ties to el-Zahir. Although the group is well-established throughout Western Europe, the United Kingdom is considered the principle transit point for new recruits and a distribution point for the "revolutionary message of jihad."

The movement has attracted a number of well-educated, unemployed youth who are second-generation immigrants from Algeria, Egypt, and Syria who have found themselves alienated from the mainstream culture of their respective European countries. As a result, they have devoted themselves to radical Islam and the global insurgency inspired by el-Zahir.

In the United States, el-Zahir and FSLTE will rely on Mutaki'oun, a loose network of American Islamic radical converts. These operatives were largely recruited from the U.S. prison population through the work of radical clerics. These individuals were almost all born in the United States, but many have traveled extensively throughout the Middle East and Caucasus. Although they maintain a Western lifestyle, they attend mosques where they have developed close relationships with other militant Islamists. Most have undergone paramilitary training either at camps overseas or at "warrior training" camps in the United States.

Mutaki'oun operational cells—called Sutra teams—are oriented around protecting radical clerics at the mosques frequented by these converts. Their training has made them highly capable facilitators of terrorist operations through activities such as intelligence collection, countersurveillance expertise, weapons acquisition, money laundering, and credit card fraud. However, their tactical skills are largely unproven.

3. The Contemporary Operating Environment

a. International

- Anti-U.S. sentiment continues to simmer across the globe.
- U.S. troops continue to be stationed and active in Afghanistan and Iraq, as well as other countries throughout the Middle East, Central Asia, and Africa.
- El-Zahir has released several statements through al-Jazeera and through key Islamist websites that contain general threats against the United States and its allies (particularly the United Kingdom, Canada, Italy, and Australia).
- Canada and the United States are exploring new approaches to border security and monitoring under the watchful eye of Canada's new Prime Minister.

b. National

- The nation is in a post-presidential election period, with the administration attempting to address key national concerns, including homeland security, the economy, and foreign policy.
- The U.S. intelligence community has detected an increasing level of "chatter" among known and suspected radical Islamists both inside and outside the continental United States.
- The Homeland Security Advisory System (HSAS) threat level is currently set to Yellow (ELEVATED – Significant Risk of Terrorist Attacks).

c. Regional

- In the northeastern United States, State and local law enforcement officials have been engaging with Joint Terrorism Task Forces throughout the region regarding growing concerns over the increasing activities of the Mutaki'oun.
- During the holiday season, ongoing concerns over port and transportation security, combined with a significant spike in Islamist "chatter" noted by the intelligence community, led the DHS to issue an elevation of the HSAS level to Orange (HIGH – High Risk of Terrorist Attacks) for the New York, NY; Boston, MA; and Washington, D.C. metropolitan areas. The rest of the nation remains at HSAS level Yellow.

d. Local

- Throughout these areas, including northern New Jersey, State and local governments were forced to address the economic impact of an elevation in the HSAS level over the holidays, leading to increased concerns over how to pay for the fluctuating costs of supporting homeland security measures.

B. The Attack Plan

1. UA Targeting Priorities (Posted on a Radical Islamist Website)

The following is a translation of *The Battar Training Camp (Mu'askar Al-Battar), The 7th Edition, March 2004*. The text below is exactly as it was released. Inaccuracies were not corrected for publication of the T3 FSE scenario.

2. Targets Inside Cities[4]

Attacks inside cities are considered a kind of militant diplomacy; this kind diplomacy usually is written with blood and decorated with body parts and gunpowder.

These attacks carry a political meaning related to ideological struggle; it is considered a message to several parties. Therefore it is very important to be detailed in selecting targets. A good example of this is the attacks by our brothers, those attacks by the heroes (Khalid Al-Sa'id, Riyad Al-Hajri, Abd-al-Aziz Al-mi'shim and Muslih Al-Shamrani) was the beginning. Their choice for a target was a great success. The building belonged to the CIA. This was the spark that ignited our Jihadi youth and opened the eyes of the nation to the Zionist presence in the land of Mohammad.

Also the attack in east Riyadh in 2003 was a message to the enemy, telling them that here we are, we have attacked you before and we can attack you now, you cannot hide because we are after you and you cannot get comfortable in the land of Mohammad.

Also the attacks by our brothers; Ali Al-Ma'badi and Nasir Al-Sayyari that targeted Al-Muhaya on the Intelligence Center were successful too. This proves that the attacks are diplomatic messages written with blood and decorated with body parts and gunpowder.

3. Religious Targets

It is not advisable to do any attacks against religious targets at the beginning of a Jihadi movement unless one of the following situations applies:

- When groups are involved in converting Muslims to Christianity like what happened in Yemen and what is happening in Iraq. Also in Saudi Arabia where Christians are trying to distribute bibles. In these cases they should be hunted down.
- Intelligence Activity hiding under a religious cover. In the case when it is a Muslim that is under cover he should not be attacked because Jihad movement can get a bad reaction from the public and it can backfire.

[4] From a translation of Abu Hajir Abd-al-Aziz Al-Manun's *The Battar Training Camp (Mu'askar Al-Battar), The 7th Edition, March 2004*. (http://tides.carebridge.org/Translations/TWPR-Al-Battar-7.htm).

- In the case when some priests and rabbis and religious figures attack Muslims or Islam like that American priest that cursed the prophet Mohammad, we ask God to bring our swords closer to his neck. Also when Sayid Nsair killed Kahana who cursed the prophet.
- In the cases where Christian and Jewish figures are conducting financial, moral, and militant campaigns against the Muslims like the previous crusades.

4. Financial Targets

The goal for attacking these kinds of targets is to shake the security and the environment for financial growth like attacking the oil pipelines in Iraq that prevented foreign companies from joining in stealing the Muslims fortunes. Also one of the goals is to get foreign investors to get out of the local market. Also, the affect of these attacks on the financial powers like the attacks in Madrid that damaged the crusaders economy. Here are some practical examples of these financial targets:

- Jewish and Crusaders investment in the lands of the Muslims.
- International companies.
- International Economical experts.
- Attacking imports from crusaders' countries or boycotting them.
- Attacking the crude materials stolen from the lands of the Muslims like oil carriers or pipelines.
- Assassinating Jewish people that work in financial field and teaching those that work with them a lesson.

5. Human Targets

We have to kill the Jews and the Christians. We have to tell everyone that fights Muslims that we are coming to kill you. We should not be divided by geographical borders. The land of the Muslims is our land. We have to turn the countries of the enemies to hell the way they turned our lands to hell. All the cells, where ever they are should be active and disregard any borders that were drawn by the enemy.

- In this case, priority is for Jewish and Christian officials in the land of the Muslims and the goal is not to let them get comfortable. We advise you to target easy targets at the heginning and priority goes to the infidels that directly support the local rejecters of Islam. For example, the targets in Saudi Arabia should be the Americans first and the English second; in Iraq, the Americans; in Afghanistan, the Americans; in Algeria, the French; in Indonesia, the Australians.

- The Human targets are in these categories:
    - Jews, and they are divided in categories, for example The Jews of America and Israel and the Jews of the UK and France.

- Christians are ranked in the following order:
  - Americans
  - UK
  - Spanish
  - Australians
  - Canadians
  - Italians

- These will also be divided into the following categories:
  - Finance and businessmen, for money is important in this day and age.
  - Diplomats, politicians, intellectuals and political delegations.
  - Military leaders and soldiers.
  - Tourists and all those that were warned by the Mujahidin.

- Collaborators are good targets and are ranked as follows:
  - Those with close ties to the Christian and Jewish governments like Husni Mubarak of Egypt and the rulers of Arabian Peninsula and their advisors.
  - The liberals and the seculars who have harassed the faith.
  - Spies and Intelligence, they are shielding and protecting the Jews and the strong-arm of the collaborators rulers.

6. The Goals of Targeting Humans

- To provide clarification of the nature of the conflict. By targeting Christians and Jews it shows that this is a religious struggle.
- To show the main enemy.
- To cleanse the earth of these people and to deter others.
- To spread fear in the enemy and this is a requirement documented in Koran.
- To raise the morale of the Islamic Nation.
- To destroy the image of the government that was targeted. After the 9/11 attacks, America's nose was in the dirt.
- To disrupt the plans of the infidels, like the time when Italy refused to send troops to Iraq. Also like what happened in Spain where the challenger of the prime minister promised to pull the troops out the Iraq after the attacks in Madrid.
- To punish them for killing the Muslims.

7. The Pros of Attacks in Cities

- Raising the morale of the nation and of the Mujahidin.
- Confirming the credibility of the Jihadi group in the society. People will be able to see and the media cannot lie to the public.
- Forcing the regime not to cross red lines.
- Testifying that there is no God but Allah and Mohammad is his prophet and for achieving unity.
- The governments will lose their effective symbols.

- Influencing the economies of those countries.
- The Mujahidin gain experience and qualification that will make them leaders of the nation in the future.
- Study and analysis of mistakes that need to be avoided in the future.
- Preparing the nation and the brothers for future wars and confrontations.
- Winning sympathizers and increasing the popularity of the Mujahidin with every successful operation.
- Forcing the regime to change their policies.
- Shaking the trust and the confidence of the members of the regime. It could also cause clashes between the military and political powers in the country and cause disagreement among the political parties.

8. The Cons of Attacks in Cities

- The killing of Jihad leaders and members once these attacks are discovered.
- Lots of human and material damage.
- Lowers the morale of Mujahidin in cases of failure. This is why a good leader raises the morale of his people in any case.
- Gives the regime a chance to take advantage of the situation and harm innocents.
- Raises the morale of the members of the regime when they win the battles.
- Some members of the Jihad can be captured and secrets could be uncovered.
- Weakening in the trust between the Jihadi groups and the society in case of repeated failures.

9. UA Specified And Implied Mission Tasks

a. Specified Tasks

- El-Zahir will provide access to weapons material and technical expertise, ideological justification and inspiration, and limited direction and financial support.
- FSLTE will plan and conduct compartmented tactical planning, preparations, rehearsals and execute attacks against New York City and Boston employing a combination of large vehicle bombs, chemical and biological weapons.
- FSLTE will coordinate support activities and train operatives from Mutaki'oun to assist with the execution of Vehicle Borne Improvised Explosive Device (VBIED) and chemical/biological weapons attacks against New York City and Boston.
- FSLTE will conduct compartmented tactical planning, preparations, rehearsals and execution of a chemical attack at specified targets in London, UK.
- Nasamaah-At will conduct a series of attacks against specified targets in London, UK.

b. Implied Tasks

- Operational security will be strictly observed:
  - Tactical elements will remain unaware of each others activities.
  - Communication with tactical elements will kept to a minimum.
- Individual targets will be selected by FSLTE cell leaders to achieve desired outcomes. Selection criteria will be based on anticipated weapons effects, analysis of security measures, and on the results of reconnaissance and surveillance.

10. Desired Outcomes

- Demonstrate our resolve to fight the United States and their allies with all means available by doing the unthinkable—releasing biological and chemical agents against the general population in the United States and United Kingdom.
- Create mass casualty events to demoralize the general population and create an atmosphere for them to challenge their governments' foreign policies toward Islam.
- Cripple the U.S. economy by disrupting commerce and forcing an increase in security measures nationwide.
- Drive a wedge between the U.S./UK alliance.
- Force the United States to deploy additional forces to Central and West Africa to ensure access to oil supplies, further stretching military resources and relieving pressure on mujahideen in Afghanistan and Iraq.
- Destabilize the governments of Central and West Africa to facilitate conditions favorable to an expansion of the global Salafist insurgency.

C. Attack Execution Timeline

1. Concept of Operations

Universal Adversary elements are planning to conduct a coordinated strike using WMD on Boston, Massachusetts; New York, New York; and London, United Kingdom. Their concept of operations includes the following:

2. Premission activities

- Infiltrate command and control elements and CW/BW agents into the United States and the United Kingdom.
- Establish safe houses/laboratories in the United States and the United Kingdom. The Boston attack will be staged from Connecticut, and the New York City attack will be staged from New Jersey.
- Produce and weaponize CW/BW agents.
- Construct vehicle-borne IEDs (VBIEDs).
- Organize support within Mutaki'oun (U.S.) and Nasarnaah-At (UK).
- Conduct reconnaissance and surveillance of possible targets.

- Select targets.
- Conduct mission rehearsals.

3. Mission execution

- April 2, 2005: Under the operational control of FSLTE, Mutaki'oun operatives conduct a BW attack against New York City.
- July 4, 2005: FSLTE and Mutaki'oun operatives conduct combined VBIED/CW attacks against Boston.
- July 4, 2005: FSLTE and Nasamaah-At conduct multiple CW and IED attacks against London.

4. Post-mission activities

- FSLTE (U.S.) command and control element exfiltrates through Canada to Algeria.
- Mutaki'oun and Nasamaah-At operatives go underground in the United States and the United Kingdom.

D-400 TO D+7

D-400 (February 29, 2004)
Tribal Areas, Pakistan
El-Zahir releases a statement via their propaganda channels (including the magazine Al Battar) that receive wide distribution in North Africa and Western Europe. The statement discusses the need to bring jihad to the door of coalition members of the U.S.-led Global War on Terrorism as retribution for their continued abuses against Islam.

D-380 (March 20, 2004)
Mauritania, Africa
FSLTE command conducts initial attack planning with Faisal Diya Amid "Al Hakam" (FSLTE Chief of Operations) present. Faced with increased counterterrorism activity in Algeria, the command group meets in Mauritania.

D-375 (March 25, 2004)
Mauritania, Africa
FSLTE uses el-Zahir communications channels to request operational support. Khatib 'Adli (the el-Zahir Operations Coordinator) returns a secure message to FSLTE to meet for further discussion. In anticipation of receiving support from el-Zahir to procure chemical and biological agents, Al Hakam uses secure internal group communications to activate Ismail Husam al Din (FSLTE Chemical Weapons Expert) and Fatima Barakah (FSLTE Biological Weapons Expert).

D-370 (March 30, 2004)
Johannesburg, South Africa
Khatib 'Adli and Al Hakam discuss operational details and how el-Zahir could support the FSLTE-initiated attacks. El-Zahir agrees to facilitate access to biological and chemical agents.

D-362 (April 7, 2004)
Algiers, Algeria
FSLTE releases a statement via their new globally distributed Internet publication. The statement discusses the need to bring jihad to the doorsteps of the coalition members as retribution for their continued abuses against Muslims.

D-355 (April 14, 2004)
Mauritania, Africa (Wahhabi Madrassa)
FSLTE decides to activate U.S.- and UK-based support cells to conduct local target surveys. An FSLTE messenger begins travel to Frankfurt to deliver an activation message to a French-based FSLTE operative, who is to deliver the message to Bilal Id Habib (FSLTE Tactical Leader, United Kingdom) in London. Using an encrypted message, each cell is given a timeline of operations and details for secure communications channels to be used for this operation.

D-350 (April 19, 2004)
Boston, Massachusetts
The FSLTE cell in the United States is activated via human courier by Al Hakam, who will also serve as the U.S. FSLTE Tactical Leader.

Frankfurt International Airport, Germany
The FSLTE UK cell is activated.

Karachi, Pakistan
Fatima Barakah receives *Yersinia pestis* (*Y. pestis*) seed stock from Europe and South America via airmail and begins production.

D-340 (April 29, 2004)
Boston, Massachusetts and New York, New York
Al Hakam activates Mutaki'oun support cells located in Boston and New York City. Al Hakam has established a relationship with radical imams who preach at closed study groups in New Jersey and Connecticut. Al Hakam asks Ismail Al Muhaat (a local imam) to deliver a message to Ali Waddab Bishr (Mutaki'oun Communications, New Jersey). Al Hakam also asks Hanouf Khan (a local imam) to deliver a similar message to Aqil Azhar Kutaiba (Mutaki'oun Security, Connecticut). Mutaki'oun support cells are given limited information apart from the type of support that is needed (e.g., to rent a house, obtain specific supplies, etc.).

Al Hakam also directly activates the New York City operational cell of Mutaki'oun through his personal ties to Zafir Hamal (Mutaki'oun Tactical Leader, New Jersey). The

operational cell is given a targeting package but no dates. Dates will be provided to Mutaki'oun closer to D-Day.

London, United Kingdom
Bilal Id Habib activates Nasamaah-At through an established operational relationship with Basir Imad Rahman (Nasamaah-At Tactical Cell Bravo Leader). The Nasamaah-At operational cell is given an attack timeline and access to an FSLTE secure communications channel. The communications channel will ensure that Rahman's cell has access to all required support necessary to fulfill its mission objectives.

Habib further activates "Tactical Cell Alpha" and the UK Nasamaah-At support cell through Fawzi (FSLTE Spiritual Guide and Commander). Fawzi is given a secure message that he delivers to Alima Durrah Hafa (Nasamaah-At Communications) and Marid Fouad Bakri (Nasamaah-At Tactical Cell Alpha Leader).

D-310 (May 29, 2004)
Boston, Massachusetts
Falih al Hakam Hadi (FSLTE Intelligence and Security, Connecticut) conducts target reconnaissance and surveillance and relays target intelligence to the cell commander, Al Hakam. Hadi also coordinates remote targeting for New York City and builds a targeting package that is to be forwarded to Zafir Hamal by Al Hakam.

New York, New York
Al Hakam forwards the targeting package to Zafir Hamal by posting it to a covert website. After receiving the targeting package, Hamal is ordered to conduct more detailed reconnaissance and surveillance in New York City and choose the most vulnerable symbolic targets. The final list is to be reposted on the covert website for Al Hakam to retrieve.

London, United Kingdom
Marid Fouad Bakri and Basir Imar Rahman conduct target reconnaissance and surveillance and attack planning.

D-280 (June 28, 2004)
Karachi, Pakistan
Fatima Barakah completes production of the *Y. pestis* and departs Karachi for Beirut, Lebanon, where she undergoes plastic surgery to alter her appearance.

D-275 (July 3, 2004)
Algiers, Algeria
Ismail Husam al Din begins the first phase of sulfur mustard (HD) precursor production with chemicals acquired through the el-Zahir network.

D-225 (August 22, 2004)
Algiers, Algeria
Ismail Husam al Din ships HD precursor chemicals to London via Rotterdam for a second phase of processing and prepares to travel to the United Kingdom to oversee final production.

D-212 (September 4, 2004)
Beirut, Lebanon
After successful plastic surgery, Fatima Barakah departs Beirut for New York's Kennedy Airport, via Madrid, Spain, using commercial air.

D-210 (September 6, 2004)
New York, New York
Fatima Barakah arrives at John F. Kennedy International Airport, where she is met by Shihad bin Zaki (Mutaki'oun Security, New Jersey). Barakah is escorted to a safe house south of Iselin, New Jersey.

D-207 (September 9, 2004)
Newark, New Jersey
An FSLTE messenger arrives at the international airport in Newark, New Jersey from Karachi, Pakistan via Madrid, Spain, where he is met by Shihad bin Zaki. The messenger delivers 50 percent of the *Y. pestis* seed stock concealed in the battery compartment of a cellular telephone.

D-200 (September 16, 2004)
London, United Kingdom
Bilal Id Habih relocates to the safe house to oversee equipment procurement and receipt of transshipment of the HD precursor and to prepare for the arrival of Ismail Husam al Din from Algiers.

Middlesex County, New Jersey
Yasir Raja Abdul (Mutaki'oun Logistics, New Jersey) and Fatima Barakah coordinate acquisition of her lab equipment needs.

D-195 (September 21, 2004)
London, United Kingdom
Al Hakam arrives at the FSLTE safe house from Algiers to oversee operational preparations.

D-190 (September 26, 2004)
London, United Kingdom
Ismail Husam al Din arrives at the FSLTE safe house to conduct the second phase of HD production.

D-182 (October 4, 2004)
Newark, New Jersey
An FSLTE messenger arrives at the international airport in Newark, New Jersey from Karachi, Pakistan via Athens, Greece, where he is met by Shihad bin Zaki. The messenger delivers the remaining 50 percent of the *Y. pestis* seed stock concealed in the battery compartment of a second cellular telephone.

D-181 (October 5, 2004)
Middlesex County, New Jersey
Fatima Barakah begins full-scale production of the *Y. pestis* agent.

D-180 (October 6, 2004)
Newark, New Jersey
Al Hakam arrives in the United States from London to oversee final production of *Y. pestis*, synthesis of HD, and other operational preparations.

D-172 (October 14, 2004)
New London, Connecticut
Al Hakam tasks two FSLTE cell members who are licensed pilots (Jamil Abu al Khayr [FSLTE Communications, Connecticut] and Falih al Hakam Hadi) to develop air routes over populated areas in Boston for aerial dispersal of the HD agent.

D-121 (December 4, 2004)
New London, Connecticut
Rafi' Dhak-wan Aziz (Mutaki'oun Finance and Logistics, Connecticut) procures the agent dispersal equipment.

Middlesex County, New Jersey
Yasir Raja Abdul orders agricultural sprayers.

D-60 (February 3, 2005)
London, United Kingdom
Ismail Husam al Din begins sending the HD precursor material (TDG) to New Haven, Connecticut in four separate shipments.

D-49 (February 14, 2005)
Middlesex County, New Jersey
Yasir Raja Abdul purchases three used sport utility vehicles (SUVs) from private citizens, with cash, at three different northern New Jersey locations for use in the attacks on New York City. They are stored in a warehouse until the agent is ready.

D-45 (February 18, 2005)
London, United Kingdom
Ismail Husam al Din completes weaponization of HD for use on UK targets and boards an aircraft for Hartford, Connecticut via New York, New York.

D-30 (March 5, 2005)
New London, Connecticut
The first shipment of TDG arrives in the United States from the United Kingdom. It is retrieved by Aqil Azhar Kutaiba (Mutaki'oun Security, Connecticut) and transported to a safe house.

Union and Middlesex Counties, New Jersey
Mutaki'oun operatives begin rehearsing driving routes from New Jersey to New York City in their personal vehicles.

D-20 (March 15, 2005)
New London, Connecticut
Jamil Abu al Khayr and Falih al Hakam Hadi begin rehearsing a flight plan in their time-share twin-engine Beechcraft Baron (model B-58) over Boston, Massachusetts.

D-13 (March 22, 2005)
Middlesex County, New Jersey
Fatima Barakah completes production of *Y. pestis*, and weaponization begins.

D-6 (March 29, 2005)
New London, Connecticut
Ismail Husam al Din completes aerial dissemination device.

D-4 (March 31, 2005)
New Haven, Connecticut
0900
Law enforcement and intelligence agencies identify the ship carrying the second shipment of TDG 1,200 nautical miles from the U.S. coast. The subject vessel is identified as Liberian-registered with a foreign crew.

D-3 (April 1, 2005)
Newark, New Jersey
0800
Fatima Barakah boards a commercial flight to Miami, Florida. Her plan is to leave Miami for Brazil on a connecting flight.

Middlesex County, New Jersey
2300
Mutaki'oun operatives load the *Y. pestis* agent into the sprayers and prepare for deployment as planned.

D-2 (April 2, 2005)

Union and Middlesex Counties, New Jersey

0200

Zafir Hamal, Fatih Yaman Ihsan, and Jibran Al Mash'al drive three SUVs outfitted with biological weapon (BW) dissemination devices toward New York City to execute their mission. As the vehicles are making their way toward the city, a confrontation with an off-duty police officer at a New Jersey Turnpike rest stop, followed by a call to authorities, causes one of the drivers to panic. He believes that the mission is compromised and communicates this to the other drivers while fleeing the scene of the incident. The operatives make the decision to avoid New York City and disseminate as much agent as possible in New Jersey on the Garden State Parkway, US 1/9, and NJ-18/New Jersey Turnpike.

By pure coincidence, April 1 was the final day of an international financial services industry conference held at the Sheraton at Woodbridge Place Hotel in Iselin, New Jersey. Many delegates from the United Kingdom and Canada remained overnight.

Union and Middlesex Counties, New Jersey

0600

The New Jersey tactical team abandons their vehicles. Using a one-use emergency mobile phone provided to him, Zafir Hamal quickly communicates the belief that their mission was compromised to Al Hakam. Hamal describes their hasty actions to avoid capture, and Al Hakam makes the decision to accelerate the Connecticut cell's attack timeline due to the potential for immediate police involvement. He believes that the compromised New Jersey operation will lead the police to the Connecticut cell prior to their planned July attack on Boston, Massachusetts.

New London, Connecticut

0800

Al Hakam requests that the UK-based Nasaamah-At accelerate their timeline as well.

Newark, New Jersey

0900

Fifteen UK nationals who attended the financial industry trade conference at the Woodbridge site board an airplane for Gatwick International Airport. Approximately half of them have been infected, but they are still asymptomatic.

New London, Connecticut

1200

Al Hakam and his accomplices devise their hasty attack plan. After discussions with Ismail Husam al Din, it has been decided that they are incapable of mounting any attack using HD for at least two days. They are not prepared to mount an attack on Boston due to a lack of scheduled public gatherings in the immediate timeframe and incomplete reconnaissance and surveillance. Additionally, they only have one VBIED that is close to completion, and the *Y. pestis* incubation period will likely result in casualties beginning April 4. There is a local festival occurring at the New London City Pier on April 4 that

will present an opportunity for them to use their HD on as many as 10,000 people. Al Hakam makes the decision to attack this festival. The single completed VBIED will be used in conjunction with the aerial contamination to maximize casualties.

Bayonne, New Jersey
1300
A cruise ship departs for St. John, New Brunswick, Canada with six infected, but still asymptomatic, victims on board. The victims were attendees at the financial industry convention at the Sheraton Woodbridge in Iselin, New Jersey. Four are Canadian citizens, and two are UK citizens.

D-1 (April 3, 2005)
New Brunswick, New Jersey
0930
The first victim of the biological attack, a 14-month-old girl, is admitted to Robert Wood Johnson University Hospital.

STARTEX

D-Day (April 4, 2005)
London, United Kingdom
0200 (0700 GMT)
The infected UK attendees of the financial conference in New Jersey go to work at their respective firms as usual.

Union and Middlesex Counties, New Jersey
0800
Three victims are admitted to Union, Trinitas, and Raritan Bay Hospitals. The victim admitted to Union Hospital arrives by Emergency Medical Services and is coughing up blood.

Union County, New Jersey
0900
One of the abandoned SUVs is discovered by local security in a parking lot at Kean University and is reported to police. The agricultural sprayer is still in the SUV. The police quickly determine that this vehicle is the same one involved in the incident on April 2 and send investigators to the scene.

St. John, New Brunswick, Canada
1000
The cruise liner arrives from Bayonne, New Jersey. Four of the six infected passengers, who are now becoming symptomatic, disembark.

New London, Connecticut
1100
Preparations are complete, and Al Hakam orders the operation to be executed immediately. Al Hakam, Ismail Husam al Din, and Jamil Abu Al Khayr bring their weapon to the Groton-New London airport, install it in their aircraft, and take off en route to the target.

New London, Connecticut
1120
As the aircraft approaches New London City Pier, the aircraft disperses its entire HD payload over the area, contaminating the west bank of the Thames River and the downtown riverfront area. Approximately 8,000 people are contaminated with HD. This is a covert release, and people begin departing the area approximately 10 minutes later without knowing that they have been contaminated.

Upon completion of the attack, the plane turns north toward Canada. The operatives' plan is to land the aircraft at a remote airfield in Deblois, Maine, and make their way on land to Canada via the border at Calais, Maine – St. Stephen, New Brunswick.

New London, Connecticut
1300
Victims of the HD attack are becoming symptomatic and are seeking medical attention at the first aid tent on the pier.

Deblois, Maine
1310
As planned, the aircraft carrying Al Hakam, Ismail Husam al Din, and Jamil Abu al Khayr lands at a remote airstrip. The operatives abandon the aircraft and head for the border at Calais, Maine – St. Stephen, New Brunswick with a Canadian accomplice who has crossed into the United States to provide them with transportation to Canada.

New London, Connecticut
1320
As victims of the HD attack begin to form a crowd at the first aid tent on the pier, Falih Al Hakam Hadi detonates his VBIED, martyring himself and destroying the first aid tent at the festival. The VBIED contains the remaining HD that was not used in the aerial attack. The VBIED attack causes the collapse of several structures and results in approximately 200 casualties.

New London, Connecticut
1415
HAZMAT field screening indicates presumptive identification of HD agent.

New London, Connecticut
1430
911 calls begin coming in from around the greater New London area reporting symptoms of HD contamination.

Calais, Maine
1450
Al Hakam, Ismail Husam al Din, Jamil Abu Al Khayr, and their Canadian accomplice cross the Canadian border.

St. Stephen, New Brunswick
1500
The Canadian driver is detained by Canadian authorities, and Al Hakam, Ismail Husam al Din, and Jamil Abu Al Khayr flee the scene in the vehicle.

St. John, New Brunswick, Canada
1600
The cruise liner continues to Halifax with two of the six original victims.

Union County, New Jersey
2000
A presumptive diagnosis of *Y. pestis* is established based on patient epidemiology, laboratory results, and a swab taken from the abandoned SUV at Kean University. This information is communicated to the United Kingdom and Canada via the World Health Authority.

St. John, New Brunswick, Canada
2230
The first victim of the New Jersey biological attack who went ashore in St. John is admitted to a local hospital.

D+1 (April 5, 2005)
New London, Connecticut
0645
Dozens of trucks loaded with food, blankets, medical supplies, and so forth arrive at the blast site, escorted by hundreds of volunteers who want to help. People are milling around the site, and the investigators and first responders are having difficulties containing the eager volunteers and the supplies that they are bringing. People who have already shown up say that many more volunteers and supply trucks are on their way.

Middlesex County, New Jersey
1400
Investigation of the SUV leads to the discovery of the location of the biological weapons production facility used by FSLTE and the Mutaki'oun.

Halifax, Nova Scotia, Canada
1415
The second, third, and fourth cruise ship passengers who are victims of the biological attack in New Jersey present at St. John Hospital.

Middlesex County, New Jersey
1500
Investigation of the SUV leads to the discovery of the location of the Mutaki'oun safe house.

Halifax, Nova Scotia, Canada
1500
The cruise ship arrives in the Halifax area. No victims disembark.

Newark, New Jersey
1800
A second SUV is discovered abandoned on Avenue "C" near the airport.

New London, Connecticut
2300
Law enforcement and intelligence agencies identify the ship carrying the third shipment of TDG in U.S. waters. The subject vessel is identified as Liberian-registered with a foreign crew.

D+2 (April 6, 2005)
New London, Connecticut
0900
An investigation leads to the discovery of the chemical staging facility used by FSLTE and the Mutaki'oun. Evidence discovered in this facility confirms connections to the United Kingdom and suggests an imminent threat there.

London, United Kingdom
1200
The discovery of a VBIED similar in design to the one detonated by the FSLTE in New London, Connecticut, marks the beginning of a series of terrorist attacks in London targeted against the transportation infrastructure.

Deblois, Maine
1800
The abandoned aircraft used in the Connecticut attack is discovered.

D+3 (April 7, 2005)
London, United Kingdom
TBD
An investigation leads to the discovery of the chemical weapons production facility, which contains some of the precursor chemicals previously shipped to the United States.

London, United Kingdom
1200
Chemical devices are activated on mainline trains arriving at Waterloo International Rail Terminal, the station concourse, and the adjacent Underground station. Casualties include U.S. citizens.

D+4 (April 8, 2005)
Yarmouth, Nova Scotia, Canada
1000
The fourth and final shipment of TDG is identified on a vessel currently located in the Atlantic en route from London, United Kingdom to Yarmouth, Nova Scotia.

ENDEX

Part 4: Analysis of Mission Outcomes

In an exercise as large in scope and depth as T3, the opportunities for analysis are significant. Based on post-exercise meetings among participants, the T3 After-Action Conference (AAC), and observations by subject matter experts during the exercise, 10 elements of the operation were selected for in-depth analysis. The topics discussed in this report include the following:

Broad Mission Outcomes	• The Homeland Security Advisory System (HSAS) • Joint Field Office (JFO) Operations • Resource Requesting and Resource Coordination • Information Sharing
Critical Tasks	• Stafford Act Declarations • Emergency Public Information • Integrating Responses to Incidents of National Significance (INSs): Public Health Emergency and the Stafford Act • The Strategic National Stockpile (SNS) and Points of Dispensing (PODs) • Agent Confirmation and Hazard Area Definition • Emergency Response Operations under a Unified Command (UC)

The selection of these 10 topics in no way suggests that other issues were not worthy of analysis. Rather, these issues involve sequences of events that attracted great interest; new or developing organizations and procedures; and elements of the exercise that seemed problematic or well-played. Nothing should be presumed about a topic or issue that was not selected for analysis.

This section of the report provides an analysis of the four issues identified as Broad Mission Outcomes and addresses how well the participating agencies/jurisdictions dealt with these significant issues. Mission outcomes are those broad areas of service or functions that the public expects from its officials and agencies. As defined in the Office for Domestic Preparedness' Homeland Security Exercise and Evaluation Program (HSEEP) – Volume II: Exercise Evaluation and Improvement, the mission outcomes include: prevention/deterrence, emergency assessment, emergency management, hazard mitigation, public protection, victim care, investigation/apprehension, and recovery/remediation. Analysis of the more specific issues, identified as Critical Tasks, and the activities and processes that contributed to their results are found in Part 5.

I. The Homeland Security Advisory System (HSAS), State Threat Couditious, and Associated Protective Measures

A. Introduction

President George W. Bush signed Homeland Security Presidential Directive (HSPD)-3, which created the HSAS to improve coordination and communication in the event of a threat of terrorist attacks. The HSAS is meant to "disseminate information regarding the risk of terrorist acts to Federal, State, and local (FSL) authorities and to the American people.[1]" The HSAS has two stated purposes: first, it informs Federal, State, and local governments and the public of the perceived credibility and imminence of threats; second, it directs a systematic, coordinated governmental response to such threats to "reduce vulnerability or increase response capability."

The system uses colors (from Green to Red) to define threat conditions from low to severe. Since its creation on March 11, 2002, the HSAS threat condition has been increased from Yellow (Elevated) to Orange (High) seven times,[2] most recently in July 2005. The threat condition has never been lower than Yellow or higher than Orange. The first full-scale test of an elevation to Red (notional) occurred in the T2 FSE (May 2003). To date, the HSAS has only been elevated to Red during exercises. All such elevations to Red have been in response to attacks rather than being based on preattack threats.

Implementation of the HSAS, and specifically the Red threat condition, has been closely examined in three previous exercises—the T2 FSE, T3 CPX, and Senior Officials Exercise (SOE) 04-4, *Crimson Dawn*. The T3 FSE demonstrated that previously identified issues still persist and underscored some questions regarding the protective value of HSPD-3 as currently implemented through the HSAS. The core issue demonstrated in the exercises that have

SUMMARY OF CONCLUSIONS: HOMELAND SECURITY ADVISORY SYSTEM

- Real-world and exercise elevations of the HSAS to Orange and Red indicate that implementation of the HSAS was not systematic.
- There did not appear to be a formal mechanism for coordinating, reporting, and tracking HSAS and State threat level changes and implementation of associated Federal, State, local, and private sector protective measures.
- The absence of a mechanism for coordinating the implementation of protective measures contributed to an uncoordinated response.
- Unintended consequences of implementing HSAS Red protective measures were not well understood.
- Officials in the T3 FSE used the HSAS and State threat conditions more as a means of facilitating emergency response operations than as a threat advisory system.
- Inconsistent messages and little specific public guidance limited the value of the HSAS as a warning/advisory system.

[1] President George Bush, Homeland Security Presidential Directive-3, March 11, 2002.

[2] September 10–24, 2003; February 7–27, 2003; March 17–April 16, 2003; May 20–30, 2003; December 21, 2003–January 9, 2004; August 1–November 10, 2004 (Banking/Financial sector only for NY, NJ, and Washington, DC); July 7, 2005–present (mass transit only).

examined the HSAS—most recently the T3 FSE—is that the HSAS is still not used in a systematic manner and therefore is not effectively achieving the objectives detailed in HSPD-3.

B. Background

The HSAS is "intended to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response." Whereas the HSAS defines the general threat conditions across a risk spectrum, HSPD-3 directs Federal agencies and departments to develop and implement protective measures appropriate to each threat condition.

The general HSAS guidelines for protective measures that Federal departments and agencies should consider under condition Orange, or "High Risk of Terrorist Attacks," include the following:

- coordinate necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations;
- take additional precautions at public events and consider alternative venues or cancellation if necessary;
- prepare to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and
- restrict threatened facility access to essential personnel only.

The general HSAS guidelines for protective measures that Federal agencies should consider under condition Red, or "Severe Risk of Terrorist Attacks" include the following:

- increase or redirect personnel to address critical emergency needs;
- assign emergency response personnel and preposition and mobilize specially trained teams or resources;
- monitor, redirect, or constrain transportation systems; and
- close public and government facilities.

The HSAS is only binding for the executive branch of the Federal government. HSPD-3 does, however, encourage governors, mayors, and other leaders to review their organizations and assign protective measures to the threat conditions in a manner consistent with that of the Federal government. Some State and local governments have adopted threat advisory systems based on the HSAS, with specific security measures to be implemented under each of the color codes. Both Connecticut and New Jersey have a threat alert system that is coordinated with the

HSAS.[3,4] State and local governments can raise their threat conditions independent of the Federal government.

C. Reconstruction

The T3 FSE did not have scripted elevations of the HSAS or State threat conditions. The exercise began with the HSAS and participating State (New Jersey and Connecticut) advisory systems at Yellow (elevated). At 12:14 on Monday, April 4, 2005, the New Jersey governor, in consultation with the Department of Homeland Security (DHS) Secretary, raised the New Jersey State threat condition to Orange following a presumptive diagnosis of pneumonic plague and the discovery of a suspected *Yersinia pestis* dispersal mechanism. Later that day the governor enacted travel restrictions in Middlesex and Union counties, the suspected origins of the attacks.

At 14:12 the Connecticut governor, in consultation with the DHS Secretary, raised the Connecticut State threat condition to Orange in response to the vehicle-borne improvised explosive device (VBIED) and chemical mustard attacks in New London.. At 17:00, the DHS Secretary announced the elevation of the HSAS to Orange nationwide and to Red in Middlesex and Union Counties, New Jersey.

At 14:05 on April 5, 2005, tbe New Jersey governor announced that he was raising the New Jersey State threat condition to Red for the entire State. He issued an order restricting travel to "persons seeking essential medical care, residents traveling to prophylaxis Points of Dispensing (PODs), and essential public and private sector personnel and those people returning home," in part to facilitate movement of emergency responders. The order and accompanying press release stated:

> *Essential personnel for the purposes of this emergency shall include, but not be limited to the following: State employees bearing State identification designating them as essential employees for the purpose of traveling during this emergency, New Jersey Transit employees, utility contractors, hospital and nursing home personnel, and others providing emergency services or support to those adversely affected by this emergency.*

On the evening of April 5, the DHS Secretary raised the HSAS to Red for the State of New Jersey. He considered raising the HSAS to Red for the State of Connecticut as well, but the Connecticut governor convinced him that it might only hinder response efforts.

Over the next two days (April 6 and 7), DHS, IIMG, and New Jersey officials discussed removing the travel restrictions and lowering the HSAS and the State threat conditions for New Jersey. The New Jersey State Emergency Operations Center (EOC) announced that the travel

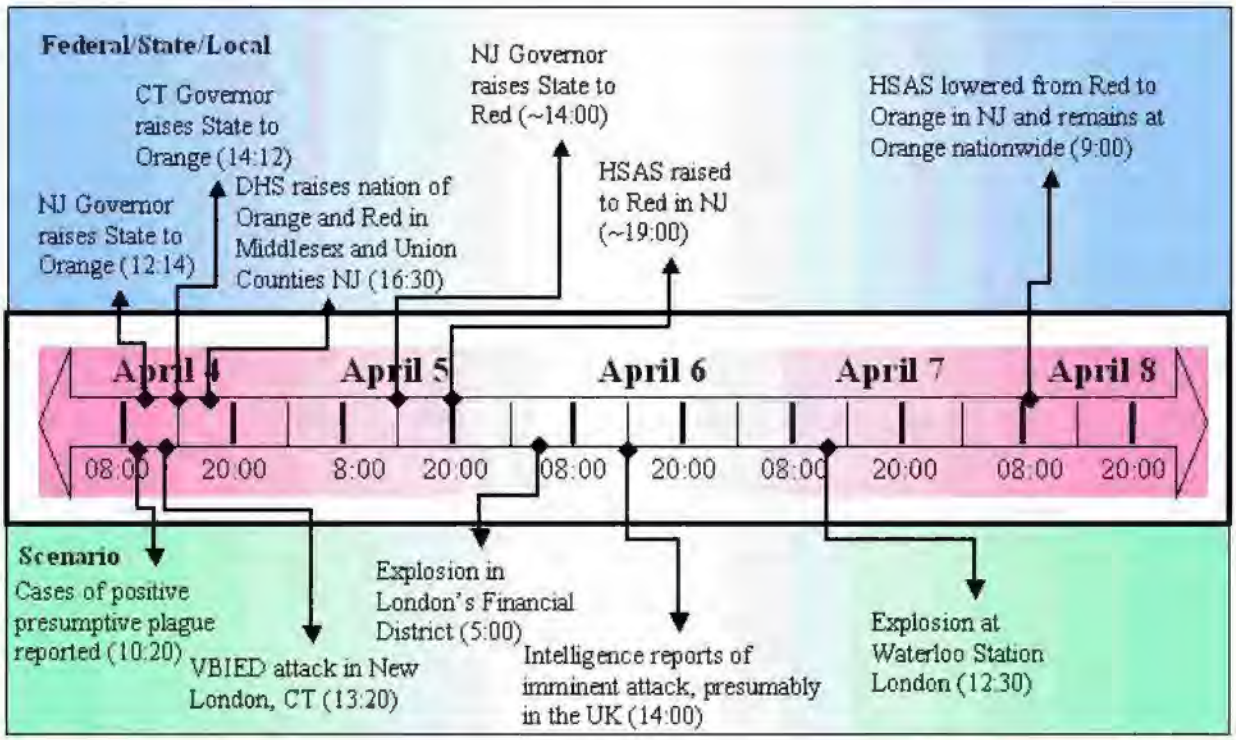
---

[3] New Jersey website http://www.njhomelandsecurity.com/.

[4]Connecticut website http://www.ct.gov/hls/cwp/view.asp?a=1030&q=255220#Yellow

restrictions were lifted at 10:30 on April 6. However, many Federal agencies remained unclear for several hours about whether the restrictions were still in effect. Late on April 7, DHS and the State of New Jersey began coordinating a joint press release announcing reduction of the State threat condition and the HSAS from Red to Orange. This press release was issued on April 8. When the T3 FSE concluded midday on April 8, both Connecticut and New Jersey were at State and Federal HSAS levels Orange. The remainder of the country also stayed at Orange. Figure I-1 shows the HSAS threat condition timeline.

Figure I-1. HSAS Threat Condition Timeline



D. Analysis

HSPD-3 states that the HSAS was created to serve two primary purposes. First, it is intended to inform Federal, State, and local governments and the public of the perceived credibility and imminence of threats. Second, it is intended to direct a systematic, coordinated governmental response to such threats to "reduce vulnerability or increase response capability." For example, HSPD-3 states that Federal departments/agencies should consider "monitoring, redirecting, or constraining transportation systems" under a Red threat condition (which could reduce vulnerability) and consider "prepositioning and mobilizing specially trained teams or resources" (which would increase response capability).

Although implementation of the HSAS has evolved and become more nuanced, it does not necessarily serve either of these purposes effectively, as evidenced by the issues observed in the

T3 FSE. Further, these purposes could be in conflict at times, as was observed in SOE 04-4, *Crimson Dawn,* as well as during the T3 FSE. In the nearly three years since it was created, FSL government agencies and the public have become accustomed to the system, but implementation of the HSAS and associated protective measures is still not systematic. Issues/observations from the T3 FSE are discussed below.

1. Lack of Systematic Implementation of the HSAS

An examination of the conditions under which, and how, the Orange and Red HSAS threat conditions have been used in real-world and exercise elevations reveals that although some patterns in its usage are emerging, its implementation is still not systematic. This may contribute to varying perceptions and interpretations of the threat levels.

DHS has varied in its approach to the HSAS Red threat condition in response to mock chemical/radiological attacks. In the T2 FSE, the first FSE after the creation of the HSAS, the DHS Secretary notionally elevated it to Red for the city of Seattle in response to the radiological dispersal device (RDD) blast. In the T3 CPX, DHS elevated the HSAS to Red for the States that were affected by chemical attacks. During the T3 FSE, the Secretary proposed elevating the State of Connecticut to Red in response to the notional VBIED blasts and chemical attacks; however, he did not do so in deference to the governor's request.

There has been more commonality in usage of the HSAS in response to biological attacks. In the T2 FSE, the level was elevated to Red for the city of Chicago in response to the mock biological attack, along with six other high-risk (based on the mock intelligence) cities in the second day of the exercise, but no State was elevated to Red. On Day One of the T3 FSE, the Secretary of DHS elevated the HSAS to Red for the two counties most directly affected by the biological attack in New Jersey and extended it the next day to the entire State.

In the T2 FSE, the Secretary ultimately elevated the nation's threat level to Red for a period of two days to prevent additional terrorist attacks. In contrast to each of these past exercises, participants in the four SOEs that preceded the FSE—one of which (SOE 04-4, *Crimson Dawn*) was dedicated to examining the HSAS—indicated they would not recommend raising the HSAS to Red even after two coordinated terrorist attacks.[5] One pattern across these exercises suggests that DHS would not likely elevate the HSAS to Red on a preattack basis.

Some of the inconsistencies in these exercises are due to changing leadership and relative newness of the system (despite growing real-world experience with Orange elevations, many recent ones have taken different, tailored forms and the exercise-oriented Red elevations have been experimental in nature). Even the former Deputy Secretary of DHS, Admiral James Loy observed in congressional testimony that the HSAS has evolved to the point where "today's Yellow is yesterday's Orange." As discussed later in this section, some of this may also be due to

[5] SOE 04-4, 05-3 and 2

the fact that protective measures for the Red threat condition have not yet been fully defined and their implications are not fully understood.[6]

Interpretation of the very general HSAS guidelines has been evolving with experience. Further consideration regarding the purpose and desired implications (beyond symbolic) of the HSAS is needed. Policymakers should examine the growing body of data on officials' perceptions of the HSAS and how it is applied to inform any changes to HSPD-3.

2. Lack of Formal Mechanism for HSAS

Over the course of seven real-world elevations of the HSAS to Orange, DHS has enhanced its high-level protocols for coordinating changes to HSAS threat conditions with State and local governments. A March 2004 General Accounting Office (GAO) report highlighted the various means by which DHS communicates threat level changes to Federal, State, and local government and private sector leaders, including conference calls from the Secretary of DHS to governors, mayors, and CEOs; e-mails; and coordination through the Homeland Security Operations Center (HSOC) and DHS Office of State and Local Government Coordination and Preparedness (SLGCP).[7]

In the T3 FSE, DHS coordinated directly with top officials from State and local governments on HSAS threat level changes. When DHS raised the HSAS threat condition to Orange, SLGCP contacted State homeland security advisors regarding the Federal HSAS change approximately 20 minutes prior to the change taking effect and approximately 40 minutes before the Secretary's press announcement. The elevation of the HSAS threat condition was widely disseminated within the Federal government and State EOCs prior to the announcement on VNN. When DHS raised the Federal HSAS threat condition to Red for the State of New Jersey, top officials coordinated with the New Jersey governor and the New Jersey State homeland security advisor. DHS and State top officials held conference calls to discuss lowering the HSAS and State threat conditions in New Jersey to Orange, and many agencies over several days reported discussing the changes and their potential effects.[8]

Coordination of the threat condition changes at the highest levels of the State and Federal government did not always translate to smooth coordination and understanding at the staff levels. There appeared to be no uniform method or process for transmitting the decisions on the HSAS and State threat levels to State and Federal agencies (and the private sector). In the T3 FSE, this caused some organizations to be unaware that the HSAS had changed, uncertain as to whether associated State threat conditions had also changed, and/or uncertain as to the status of either

---

[6] See also SOE 04-4 After-Action Report.

[7] U.S. General Accounting Office, Risk Communication Principles May Assist in Refinement of the Homeland Security Advisory System, (Washington, D.C.: Mar 16, 2005), http://www.gao.gov/new.items/d04538t.pdf.

[8] Data did not provide insight into specific effects of threat level changes that agencies discussed.

threat condition. For example, different agencies in New Jersey reported different threat conditions at the same time or incorrectly reported that the entire State had been elevated to Red, though it was only Middlesex and Union Counties. T3 FSE data have similar examples of incorrect notification or reporting of threat conditions among Federal agencies, between Federal and State agencies, and within States among State agencies.

Some of the misunderstandings may have been due to the similarities between State systems and the HSAS. The participating States in the T3 FSE use terminology similar to the HSAS: Connecticut's system is referred to as the "Homeland Security Threat Level," and New Jersey's language and color-coded levels are identical to the HSAS. This further underscores the importance of formal notifications that clearly identify which threat condition (HSAS, State, or local) is being elevated and by whom. Formal notification is especially important with the more tailored elevations of the HSAS threat condition to a specific region or sector. Also, without a formal notification process, it can be difficult to distinguish between authoritative decisions and unconfirmed advance notices, further contributing to misunderstandings.

Misunderstandings on the status of HSAS and State threat conditions due to the absence of formal notification procedures were observed in the T2 FSE (May 2003) and the T3 CPX (May 2004). In a February 2004 GAO report that examined real-world elevations to Orange, it was noted that DHS had not formally documented notification protocols for alerting FSL government departments/agencies of changes to HSAS threat levels[9]. Although notification protocols have improved considerably over the past two years, more detailed notification protocols at FSL levels regarding the status and implications of the various threat advisories could be helpful.

> **"The cornerstone of the HSAS is the protective measures that are implemented at each Threat Condition."**
>
> *Testimony of DHS Deputy Secretary James Loy, ADM, USCG (RET), Before the House Select Committee on Homeland Security, "The HSAS: Improving Preparedness through Effective Warning," February 4, 2004*

The T3 FSE data suggest that the protective measures that were implemented (notionally) under the HSAS and State threat conditions of Red were not uniformly tracked. Some Federal agencies generally reported implementing protective measures at HSAS threat conditions of Orange and Red, but most did not provide a list of specific protective measures. The Interagency Incident Management Group (IIMG) reviewed candidate Federal protective measures in their deliberations related to the HSAS, but the data do not identify which were implemented, with the exception of the transportation sector.

The DHS Protective Security Division developed a set of recommended protective measures for the private sector[10] and passed them to the IIMG. But no listing could be found as to which, if

[9] U.S. General Accounting Office, *Homeland Security Advisory System: Preliminary Observations Regarding Threat Level Increases from Yellow to Orange*, GAO-04-453R (Washington, D.C.: Feb. 26, 2004).

[10] For critical infrastructure for specific sectors (e.g., energy).

any, were implemented in elevations of the HSAS threat condition. Also, there was no evidence from the data collected at the National Infrastructure Coordinating Center (NICC) that the private sector participants received these recommended protective measures prior to or during the FSE. Although there were instances of collaboration on individual protective measures (such as travel restrictions), there did not appear to be an overarching mechanism for coordinating implementation of FSL and private sector measures.

The transportation sector provided the most comprehensive record of which protective measures were implemented. For example, the Federal Aviation Administration (FAA) implemented Temporary Flight Restrictions (TFRs) for the airports in the incident regions. The U.S. Coast Guard (USCG) elevated their Maritime Security (MARSEC)[11] levels in the affected areas consistent with HSAS elevations. The State of New Jersey also provided data on its highway/roadway travel restrictions.

At the local level, Union County, NJ[12] initiated the following protective measures in response to the elevation of the HSAS and State threat conditions to Red:

- closed all schools;
- closed all government offices;
- announced that only essential personnel needed to respond to threat;
- cancelled all major events;
- closed businesses (except for grocery stores);
- initiated Buffer Zone Protection Plans;
- maintained contact with hospital and health officials; and
- initiated travel restrictions.

But even those protective measures that were widely communicated were often incorrectly reported or misunderstood due to the absence of a formal mechanism for coordinating and tracking implementation. For example, the USCG implemented MARSEC II[13] in Boston, New York/New Jersey, Trenton, and Philadelphia, and MARSEC III in Bridgeport, New London,

---

[11] http://www.uscg.mil/d17/msojuneau/facsec/facility_security_requirements.htm. There are three MARSEC levels that are aligned with the HSAS threat condition color codes. MARSEC I aligns with HSAS Green, Blue, and Yellow with normal security measures to minimize vulnerability to incidents. MARSEC II has additional protective measures that are expected to be sustained for substantial periods of time and aligns with Orange. MARSEC III aligns with Red with even more protective measures; however, these protective measures, and therefore MARSEC III, are not intended to be sustained for substantial periods.

[12] Similar measures were reported for Middlesex County. However, the reports of those measures associated them with a state of emergency instead of an elevation in the threat condition.

[13] Under MARSEC II, access to port facilities is controlled and 25 percent of pedestrians, baggage, and personnel effects are screened. MARSEC III includes the protective measures under MARSEC II, 50 percent of vehicles are screened, and 100 percent of large vehicles are screened. MARSEC III does not mean automatic closure of the port, but can include port closure.

New Haven, and Long Island Sound in Connecticut.[14] Some agencies erroneously reported the "ports" of New York and New Jersey as closed when they were not.[15]

Similar misunderstandings occurred with airports. The Department of Transportation (USDOT) reported the airports in New York and New Jersey as open and operating throughout the exercise. It asked air carriers to voluntarily cancel flights into affected airports, and many international flights were redirected to other airports primarily in Philadelphia, Boston, and Baltimore. Yet, many FSL agencies were confused regarding the status of the airports and repeatedly asked if the airports were closed, or mistakenly reported them as closed.

3. Lack of Formal Coordination Mechanism

In the T3 FSE, there did not appear to be a formal mechanism for coordinating and tracking the implementation of FSL and private sector protective measures. This may have contributed to the inconsistent application of some measures in the T3 FSE. For example, when New Jersey elevated the State threat level to Red, highway travel in and around the State was restricted to essential emergency personnel and supplies to facilitate response and prevent the spread of plague. However, even after DHS elevated the HSAS threat level to Red for the State, the airports and ports in New Jersey remained open. This could have been problematic for a number of reasons. Under this arrangement, passengers and cargo were permitted to arrive in New Jersey by ship or plane, but not permitted to leave the airport or port facility. It could also have resulted in conflicting messages to the public.

In addition, little guidance was provided regarding what constituted "essential" in these cases. Some EOC personnel in New Jersey expressed concern that the restrictions might apply to their personnel, and that they would therefore be unable to report to the EOC. There is no evidence that instructions were provided to New Jersey State Troopers or local police on how to identify authorized travelers. Further, there is also no evidence that essential medical or other personnel outside the State of New Jersey were provided with instructions regarding the credentialing they would need to cross the State border and travel unimpeded while the travel restrictions were in effect.

The Lead Sector Coordinator for the Healthcare Sector in the DHS Infrastructure Coordination Division believed implementation of movement restrictions could apply to transport of food and water, which could have had an immediate and significant impact on healthcare operations in New Jersey by delaying deliveries.[16] Additionally, the restrictions on interstate road travel could

---

[14] Long Island Sound is located north of Long Island and south of Connecticut and Rhode Island. The entrances to the Port Authority of New York/New Jersey are south of Long Island.

[15] No further details were provided.

[16] Dale Brown Lead Sector Coordinator, Healthcare and Public Health Infrastructure Coordination Division, DHS, *Impacts of the shift to RED on the Public Health and Healthcare Sector*, memo written during T3 and posted on JFONET, Undated.

have caused severe traffic congestion along the entire East Coast as traffic was diverted around the State of New Jersey, a major passenger and freight thoroughfare. Without more comprehensive and coordinated implementation planning, these restrictions, which were intended to facilitate response efforts, could have severely hampered movement of necessities into the State.

4. Unintended Consequences of HSAS Red

The T3 FSE revealed differing views on whether an HSAS and/or State Red threat condition would help or hinder response. In the SOEs that preceded the T3 FSE, officials who were reluctant to elevate the HSAS to Red mentioned these concerns frequently. As mentioned earlier, the New Jersey governor believed an elevation of the HSAS and State threat conditions to Red would help response efforts, whereas the Connecticut governor was concerned that this threat condition would hinder response efforts. The DHS Lead Sector Coordinator for the Healthcare Sector (Infrastructure Coordination Division) was concerned that the increased security checks and patrols implemented under the elevation of the HSAS and State threat conditions to Red could hinder response. For example, healthcare facilities (such as in-patient care sites other than hospitals) are encouraged to escort contract personnel, increase security patrols, and place guards at entries under an HSAS Red threat condition. But these requirements could necessitate additional security personnel who are already overburdened by other response needs. The data from the T3 FSE did not indicate whether these security measures were even notionally implemented. However, even if they were implemented notionally, the personnel requirements of these security measures were not likely fully recognized. DHS and FAA staff expressed concern that the TFRs imposed over New London, CT, and New Jersey would hamper relief efforts, though the data did not provide insights into their specific concerns.

Discussions by officials at the IIMG expressed concern that extended periods of time with Red protective measures implemented could have negative economic and psychological impacts on the northeast region, and ultimately hamper response efforts. DHS officials worked with the State of New Jersey to reduce and eliminate travel restrictions that would negatively affect the response efforts. Later, the IIMG reviewed Federal Red protective measures and determined that it was not Federal measures that were hindering response activities. They determined that lowering the threat advisory to Orange, while maintaining certain Red protective measures, would not increase the vulnerability to attack.[17]

Because few of the HSAS Red protective measures that would be implemented were shared across FSL government agencies, and the private sector and implementation of all of the Red protective measures were notional, it is not possible to assess their full impact on the response efforts. But, the T3 FSE demonstrated that some protective measures intended to facilitate response could potentially hamper response and that more implementation planning and

[17] The data did not provide insight into what specific Red protective measures the IIMG felt could be maintained to enhance security and which could be terminated.

coordination for any extreme protective measures—especially those related to passenger or freight transportation—would be critical to minimizing unintended (and unanticipated) consequences. The T3 FSE also demonstrated that a better understanding of the ripple effects of extreme protective measures is needed. SOE 04-4, *Crimson Dawn*, made similar recommendations to better understand the consequences of extreme protective measures.

5. HSAS Used as a Means to Facilitate Emergency Response Operations

There was a notable difference in the use of the HSAS and State homeland security advisory systems in the T3 FSE from previous exercises. This difference involved the conscious use of Red threat conditions by top officials to facilitate emergency response operations, both in terms of operational coordination and movement. Most of the discussions regarding elevating the HSAS and/or State threat conditions to Red—or downgrading to Orange from Red—focused primarily on these aspects and less on the threat of an imminent attack. This focus is not inconsistent with HSPD-3, which states that the purpose of the HSAS is "to reduce vulnerability or increase response capability." But, it is noteworthy because in other exercises and in real-world applications of the HSAS to date, the focus has been primarily on the threat alert and prevention aspects.

6. Inconsistent Messages and Little Specific Guidance

In the T3 FSE, the elevated HSAS and State threat conditions did not serve as a particularly informative warning or risk communication tool for the public. By elevating the threat conditions after the attacks (even to Orange), the use of the HSAS as a warning tool communicated little to the public that it didn't already know (that the United States had been attacked and was possibly at higher risk for additional attacks). Little information was provided to the public in terms of protective action guidance specifically related to the HSAS and State Threat Level elevations. Also, the HSAS was elevated to Red in New Jersey as a response to the presumed biological attacks, but only to Orange in Connecticut after the VBIED- and covert-airplane-dispersed chemical attacks on New London.[18] No explanation was provided as to why residents in Connecticut were at less risk than those in New Jersey.

Other authorities, granted by such declarations as the State of Emergency and the Federal disaster declaration, as well as a Public Health Emergency in New Jersey, allowed the flow of resources and implementation of protective measures to facilitate response. These activities would have likely conveyed the message that FSL government agencies were actively coordinating response measures. Further, the protective action guidance that was issued in both venues (In New London, CT, residents were instructed to shelter in place to prevent/minimize exposure to the chemical attacks and New Jersey residents were advised to seek prophylaxis treatment in response to the plague outbreak) was not directly related to the HSAS. For these

[18] The DHS Secretary wanted to elevate the State of Connecticut to Red, as well as New Jersey, but was persuaded not to take this action by the governor who was opposed to it out of concern that it would hinder response.

reasons, the use of the HSAS in the T3 FSE appeared redundant. This, coupled with some of the misunderstandings by officials and the media regarding the status of various threat conditions, could have complicated rather than simplified the public message.

The DHS Secretary did provide some examples of specific protective measures that the Federal government was taking in the initial elevation of the HSAS to Red in New Jersey. This was in contrast to the T2 FSE, in which little to no information was provided to the public on the HSAS elevations to Red. He also referenced "hundreds" of measures routinely taken at Orange, which, although nonspecific, would have likely fostered a perception that the Federal government is acting in a proactive and focused manner to protect the public. This introduction of the Red threat condition to the public represented a marked improvement from previous exercises in which very little information had been given regarding the definition of the "Severe" threat condition. Efforts have also been made to increase the guidance available to the public regarding the HSAS. For example, DHS, with input from the American Red Cross (ARC), has developed "Citizen Guidance on the Homeland Security Advisory System" and has sponsored Ready.gov, among other public awareness initiatives.[19] But, public guidance related to specific HSAS elevations still remains rather general for a variety of reasons, including national security concerns (not wanting to tip off the terrorists) and the lack of uniform procedures for coordinating and tracking implementation of specific protective measures.

Discussions among Federal and State top officials during the T3 FSE regarding elevating the HSAS to Red suggested that the public warning/advisory aspect of the HSAS is heavily considered in decisions to elevate the HSAS, but that the possible effects of a Red threat condition are not well, or at least not consistently, understood. For example, the HSAS and State threat conditions in New Jersey were elevated to Red and highway/roadway travel restrictions were implemented into, within, and out of the State of New Jersey in the belief (at least in part) they would help facilitate response to the biological attack.[20] In contrast, the Connecticut governor requested that DHS not elevate the HSAS to Red for any part of Connecticut out of concern that some of the protective measures could hinder response efforts.[21] The Connecticut governor expressed concern that negative consequences of elevating the HSAS to Red would outweigh the benefits. The Secretary of DHS expressed his belief that elevating the HSAS to Red in response to the attacks was important from a "public perception" standpoint, but deferred to the Connecticut governor's wishes to leave the State's HSAS at Orange.[22]

When New Jersey and DHS officials discussed lowering the HSAS and State threat conditions from Red to Orange before prophylaxis operations were completed, the New Jersey governor

---

[19] http://www.dhs.gov/interweb/assetlibrary/CitizenGuidanceHSAS2.pdf

[20] New Jersey Governor Press Release, 20:46, April 5, 2005.

[21] The data did not provide insight on the governor's specific concerns.

[22] No additional or amplifying information was provided.

expressed concern that lowering the threat conditions would send the wrong message to the public. He feared that the public would believe that the threat was over and those who had not yet been prophylaxed would not report to the PODs. Recent SOEs, particularly SOE 04-4, revealed a similar emphasis on the (positive or negative) public perception of an HSAS Red threat condition and that the implications of a Red threat condition are not well understood.

7. Issues from Previous Exercises

Table I-1 depicts the significant exercise decisions and issues/observations since the T2 FSE that are related to the HSAS and State threat advisory systems, with special focus on elevations of the threat condition to Red.[23]

Table I-1. Comparison of T3 FSE with Previous Exercises

T2 FSE	T3 CPX	SOEs 05-2 and 05-3	T3 FSE
SIGNIFICANT DECISIONS			
• Affected local jurisdictions in, Washington State elevated their threat conditions to Red immediately after RDD blast. • DHS elevated the HSAS to Red for Seattle that afternoon. • DHS elevated the HSAS to Red for seven cities late that evening. • DHS elevated the HSAS to Red nationwide the next day in response to both the RDD and biological attacks.	• DHS instituted a regional elevation of the HSAS to Orange from Boston, MA, to Norfolk, VA, in response to intelligence suggesting an imminent attack. • DHS elevated the HSAS to Orange nationwide and Red in selected states after simultaneous chemical attacks in CT and NJ. • DHS lowered the selected Red States to Orange and nation remained at Orange after all suspects were in custody.	• Interagency decision makers expressed consistent reluctance to elevate the HSAS to Red, even in the aftermath of attacks—primarily due to concerns regarding unintended consequences. • Some State participants expected their State threat advisory system might be elevated to Red in the event of a compelling threat of, or in response to, an attack.	• Affected governors elevated their State threat conditions to Orange shortly after the biological (NJ) and chemical (CT) attacks, and after coordinating the elevation with DHS. • DHS elevated the HSAS to Orange for the nation and Red for the two counties in NJ suspected of being the epicenters of the biological attacks. • On afternoon of D+1, NJ governor elevated State threat condition to Red for all counties. • In the evening of D+1, DHS elevated HSAS to Red for all of NJ. • On D+3, DHS lowered HSAS in NJ to Orange.
ISSUES/OBSERVATIONS			
• Agencies do not have or share consistent understanding of formal notification approaches for HSAS status changes. • There was widespread uncertainty as to the HSAS status until the nationwide alert on D+1.		• The IIMG, SLGCP, and personal phone calls from the Secretary of DHS to governors/mayors are three mechanisms by which HSAS threat changes would be coordinated with State/local governments.	• Coordination of HSAS status changes occurred at the highest levels. *This did not translate into smooth coordination among operations centers.*
• The absence of a mechanism for coordinating the implementation of protective measures			• There did not appear to be a formal mechanism for coordinating, reporting, and tracking HSAS and State threat

[23] Issues are depicted in red font; observations in black, and improvements/good practices in green.

T2 FSE	T3 CPX	SOEs 05-2 and 05-3	T3 FSE
across Federal, State, and local governments and private sector can contribute to an uncoordinated response.			level changes and implementation of associated Federal, State, local, and private sector protective measures. • The absence of a mechanism for coordinating the implementation of protective measures contributed to an uncoordinated response.
• Increased coordination is needed between DHS and States/localities on nature of threats in order to minimize unintended consequences and cost-effectively increase the overall protective posture.		• Consequences of HSAS and State Red-level threat conditions are not well understood.	• Unintended consequences of implementing HSAS Red protective measures were not well understood.
• Public information messages regarding HSAS elevations should be clear, consistent, and explain comprehensive Federal, State, and local response actions, as well as recommended actions for the general public.		• Public Affairs participants emphasized the need for consistent messaging and specific guidance.	• Inconsistent messages and little specific public guidance limited the value of the HSAS as a warning/advisory system.
			• Observation of real-world and exercise elevations of the HSAS revealed that its implementation was not systematic. • Officials used the HSAS and State homeland security advisory systems to facilitate emergency response operations more than as threat advisory systems.
	• Decision makers experimented with "Orange Plus" terminology in CPX to refer to a level of Orange with selected Red protective measures but have since abandoned this language.	• Decision makers expressed concern over how to define the conditions under which it would be acceptable to lower the HSAS from Red and the mechanics for doing this.	

E. Conclusions

There was a notable difference in the use of the HSAS and State homeland security advisory systems in the T3 FSE from previous exercises. This difference involved the conscious use of Red threat conditions by top officials to facilitate emergency response operations, both in terms of operational coordination and movement. Most of the discussions regarding elevating the HSAS and/or State threat conditions to Red—or downgrading to Orange from Red—focused primarily on these aspects and less on the threat of an imminent attack. The effects on response efforts of raising the HSAS to Red after an attack are unknown, and are tied directly to the specific protective measures that are implemented, as well as how they are implemented. Improved protocols for coordinating and tracking implementation of protective measures—particularly severe protective measures—are needed.

A noteworthy element of the exercise was the increased emphasis on, and influence of, the public warning/advisory element of the HSAS in decisions to elevate or lower the threat condition. More consistent and clear messages are needed to fulfill this purpose of the HSAS. Citing other authorities, such as declarations of states of emergencies, in messages related to emergency response actions—rather than the HSAS—could also clarify the public messaging hy delineating between actions taken to facilitate response and those taken to address a threat and reduce vulnerabilities.

Efforts are currently underway with Congress and DHS to review the current purpose and implementation of the HSAS. If the HSAS is retained, substantially more consideration should be given to making it a more robust, but still highly flexible, system that can more effectively serve its two primary purposes of advising/alerting FSL governments, the private sector, and the public to potential threats, and reducing vulnerability to those threats.

1. Recommended Courses of Action

- Develop a formal process for coordinating and tracking implementation of severe (or Red-level) protective measures across Federal, State, and local governmental agencies and the private sector. Build a database of measures hy threat and agency to help top officials select the measures best aligned with a given scenario.
- Provide more specific guidance regarding actions recommended under the different color-coded threat conditions and link the levels to specific protective measures.
- Re-examine and refine the potential purposes of the HSAS:
    - public warning and advisory;
    - attack prevention; and
    - emergency response.

There may be value in further narrowing and better focusing the purpose of the HSAS to one of these and using means outside of the HSAS to achieve the other purposes, as these can inherently conflict in some cases. Specifically, use of the HSAS should be examined as a means to facilitate response. Although HSPD-3 states that one of its purposes is to enhance response, elevating the HSAS and related State systems after an attack specifically to facilitate response takes the focus

away from their primary role as risk communication and prevention systems, and may complicate emergency response messages. Declarations of States of Emergency, the Stafford Act, the Public Health Service Act, and other emergency powers granted to Federal, State, and local top officials are also associated with facilitating response.

II. Joint Field Office (JFO) Operations

A. Introduction

The T3 Full-Scale Exercise (FSE) provided an opportunity to exercise the recently codified JFO concept and identify issues that could impede its ability to support emergency response operations. The events in Connecticut and New Jersey prompted Federal officials to activate JFOs and select Principal Federal Officials (PFOs) for both States. During the exercise, the JFO and PFO staffs focused their efforts on integrating the Federal and State responses efforts by arranging resource support, coordinating response policies and operations, and sharing information.

Observations made during the exercise indicate that JFO operations were problematic in both States. Two kinds of disconnects were observed. First, the JFO staff encountered problems coordinating their activities and support with State officials. Second, the JFO staff also had trouble coordinating the activities of the JFO staff elements. These internal issues are the focus of this section of the report. The external coordination issues that existed between the JFO and State organizations are addressed in detail in other sections of this report that cover points of dispensing (PODs), resources, and information sharing. This section focuses on identifying the structural and process issues that adversely affected JFO operations during the T3 FSE. The issues included the following:

SUMMARY OF CONCLUSIONS: JFO OPERATIONS

- Lines of authority and coordination among the PFO, FCO, and JFO sections were unclear and hampered unity of effort with the JFOs in both Connecticut and New Jersey.
- The relationship between the PFO and FCO is not formalized, and final authority over the JFO cell was unclear.
- In Connecticut, the PFO cell duplicated much of the capabilities and expertise resident in the JFO sections, but it lacked its own clear purpose or delineated responsibilities. This often resulted in overlapping or competing activities occurring in the PFO cell and the JFO section.
- The JFOs did not follow standard processes for sharing information internally.

- unclear lines of authority within the JFO;
- undefined roles and responsibilities in the PFO cell; and
- a lack of implemented processes for sharing information.

Resolving the internal structural and process issues would ultimately strengthen the JFO's ability to coordinate Federal and State response efforts.

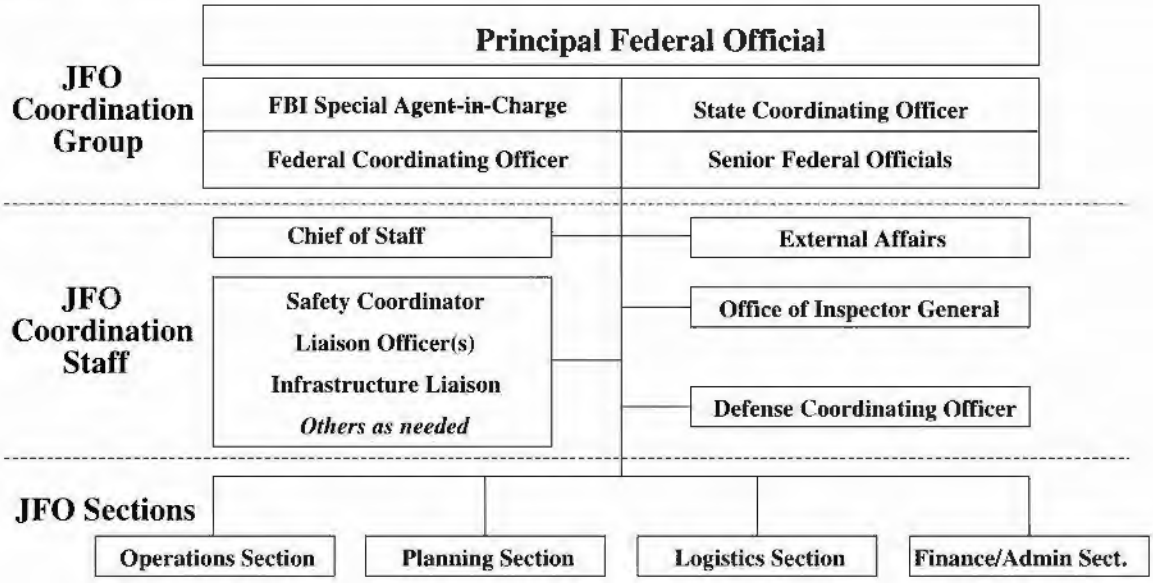
B. Background

The JFO is a temporary facility established locally to coordinate Federal assistance during an incident of national significance. Through the JFO, the Federal government provides a central coordination site for Federal, State, and local response efforts.[24]

1. Structure of the JFO

The National Response Plan (NRP) divides the JFO organization into three different elements: The JFO Coordination Group, JFO Coordination Staff, and JFO sections. Figure II-1 is a diagram of a nominal JFO organization for a terrorist incident that depicts how the three JFO elements are related.

Figure II-1. Nominal JFO Organization for a Terrorist Incident



a. JFO Coordination Group

Within the structure set forth in the NRP, the JFO Coordination Group directs the activities of the JFO elements and sets the operational priorities for Federal agencies responding to the emergency. The JFO Coordination Group establishes priorities across incidents, resolves policy conflicts between agencies, and provides strategic guidance for incident management activities. The key members of the coordination group are the Principal Federal Official (PFO), Federal Coordinating Officer/Federal Resource Coordinator (FCO/FRC), and State Coordinating Officer (SCO). In a terrorist incident, the Federal Bureau of Investigation (FBI) Special Agent-in-Charge

[24] National Response Plan (December 2004).

(SAC), as the Senior Law Enforcement Official, is also a member of the JFO Coordination Group. Other senior Federal officials (SFOs) representing agencies with primary jurisdictional responsibility for some element of the response may also join the group as required. The primary responsibilities of each JFO Coordination Group member are as follows:

- The PFO represents the Secretary of Homeland Security in the field and coordinates the overall Federal response.
- The SAC coordinates criminal investigations and law enforcement activities associated with the incident.
- The FCO manages and coordinates the Federal resource support provided through the Stafford Act.
- The SCO represents the State in the Federal resourcing process by approving State requests for Federal resources provided during the response (e.g., a State may be responsible for 25% of the deployment costs for a disaster medical assistance team).
- SFOs assist in the management of the Federal response as the most senior representatives of their agencies.

b. JFO Coordination Staff

The JFO Coordination Staff supports and advises the officials in the JFO Coordination Group. Typical JFO Coordination Staff positions include a Chief of Staff, Safety Coordinator, Legal Affairs, Equal Rights Officer, Security Officer, External Affairs Officer, Defense Coordinating Officer (DCO), and various liaisons as needed. The JFO Coordination Group selects the personnel who fill the JFO Coordination Staff positions and relies on their subject-matter expertise to inform decisions made by the JFO leadership.

c. PFO Cell

In addition to the JFO Coordination Group and Staff, there is additional staff that directly supports the PFO—the PFO cell. This cell does not appear on the NRP organizational diagram, though it is referenced in the *Interagency Integrated Standard Operating Procedures for JFO Activation and Operations*.[25] The PFO cell is intended to be a small team of subject-matter experts from various Department of Homeland Security (DHS) components and Federal agencies that may be activated and deployed to provide initial support for the PFO prior to the activation of the full JFO. The PFO cell is designed to function primarily during the preincident phase or the initial response; once a JFO is established, the PFO retains a limited number of staff persons to support scheduling, media relations, and other PFO responsibilities. The remaining members of the PFO cell are reassigned into the JFO Coordination Staff and JFO sections.

---

[25] *Interagency Integrated Standard Operating Procedures: Joint Field Office Activation and Operations*, Version 6.0, Approved 14 April 2005. This SOP was in draft form during the exercise itself, and had not been widely distributed.

d. JFO Sections

The remainder of the JFO is organized into four sections: operations, planning, logistics, and finance/administration. The NRP defines an area of responsibility for each section as follows:

- Operations coordinates the bulk of the incident management support provided by Federal agencies to the State and local agencies.
- Planning collects, evaluates, and disseminates situational information and develops plans based on this information.
- Logistics manages logistical support for the JFO and other field locations.
- Finance/Administration tracks Federal costs related to the incident response.

These four JFO sections comprise the multiagency coordination center that is intended to accommodate the agencies essential to incident management and disaster response. Although most of the JFO staff represents Federal entities, local and State agencies can send representatives to the JFO. These four sections are commonly referred to as the JFO cell.

In a terrorist incident response, the SAC becomes the Senior Federal Law Enforcement Official (SFLEO) in the JFO Coordination Group. The FBI Joint Operations Center (JOC) becomes a section of the JFO.

At total of 15 emergency support functions (ESFs) provide the bulk of the staffing for the JFO sections. Each ESF is led by a Federal agency that is responsible for coordinating the ESF's activities and identifying individuals/teams to staff the group. For example, the Department of Health and Human Services (HHS) is the lead coordinator for ESF-8, Public Health and Medical Services; this ESF is also staffed with National Disaster Medical System personnel. The ESFs are key resource providers during response operations. ESF staff members play a significant role in the mission assignment process, which is the primary method for providing Federal support to the State during an emergency response operation.

2. Mission of the JFO

The JFO supports Federal, State, and local response efforts during incidents of national significance. The NRP and the Interagency Integrated Standard Operating Procedures for JFO Activation and Operations (JFO SOP) describe the JFO's three primary responsibilities:

- Coordinating the response activities of Federal, State, and local entities (e.g., facilitate the flow of Federal resources to the affected areas).
- Collecting and disseminating information about the crisis and the response (e.g., provide situation reports [SITREPs] to the Interagency Incident Management Group [IIMG]).
- Providing a communication link between the Federal response and State/local officials (e.g., engage State officials on key response issues).

C. Reconstrnction

In response to the detection of plague in New Jersey and the release of a mustard agent in Connecticut, DHS activated JFOs and selected PFOs for both States. The JFOs focused on coordinating resources with State officials, whereas the PFO cells tracked key issues and assembled information about the crises. The JFO Coordination Group interacted with top officials from the States, set priorities for the Federal response effort, and interacted with State officials. The PFO cells provided the link between Federal operations in the States and the Homeland Security Operations Center (HSOC) and IIMG.

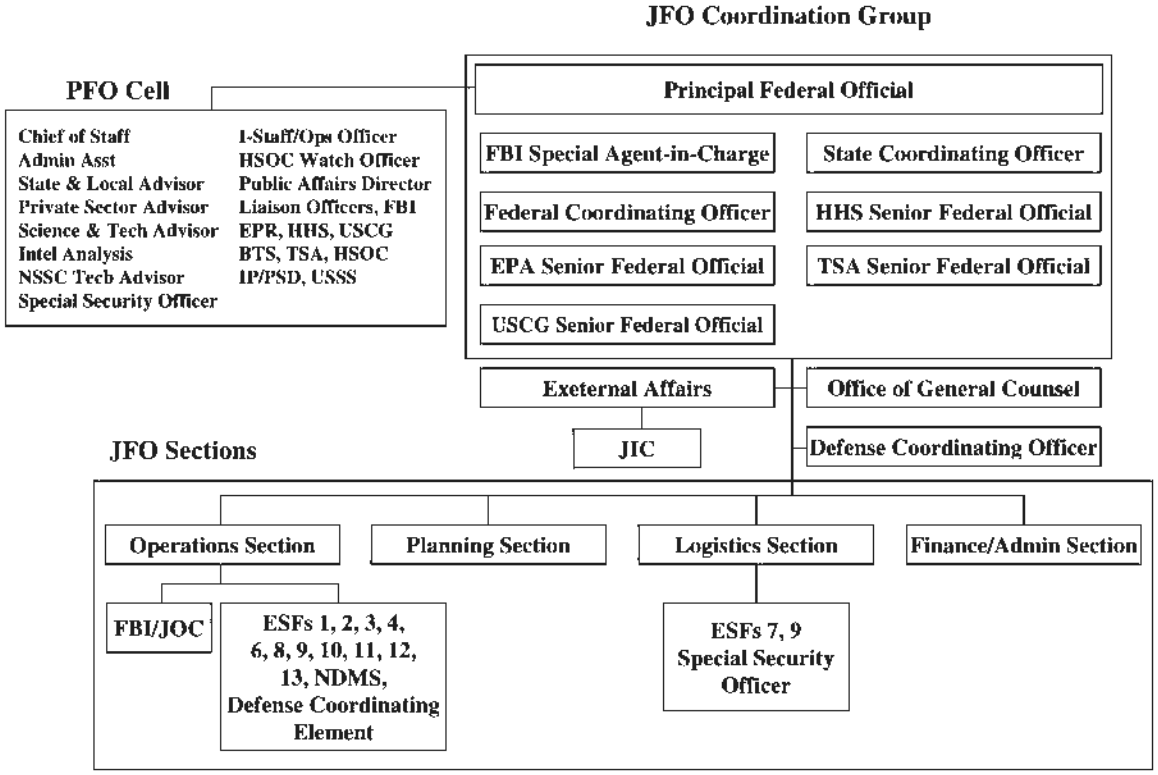
The NRP calls for various parts of the JFO organization to be identified and agreed upon by the JFO Coordination Group; however, an artificiality of a planned exercise is that players and their locations were assigned prior to exercise play. Thus, the responsibility of the JFO Coordination Group to identify the necessary JFO participants was not fully tested in the T3 FSE.

1. JFO and PFO Activities in Connecticut

In response to the explosion in New London on Monday, April 4, DHS and the Federal Emergency Management Agency (FEMA) activated the Regional Response Coordination Center (RRCC) in Maynard, Massachusetts. Shortly thereafter, the FBI redesignated its New London Command Post as the JOC.[26] At 14:20 on April 4, the FBI received approval to coordinate with DHS and FEMA to activate a JFO in Connectieut. The activation began with the deployment of the Emergency Response Team–Advanced Element (ERT-A) by the RRCC. At 16:00, the Secretary of Homeland Security designated a PFO in Connecticut. The PFO support staff, ERT-A personnel, and ESF staffers arrived at the JFO throughout the afternoon. At approximately 20:00 on April 4, the JFO was fully stood-up and had assumed Federal incident management responsibility from the RRCC. Figure II-2 depicts the organization of the Connecticut JFO.

[26] The New London Command Post had been established one week earlier in response to exercise intelligence injects.

Figure II-2. Organization of the Connecticut JFO



The structure of the Connecticut JFO is similar to the notional JFO structure found in the NRP, except that the Connecticut JFO included a substantial PFO cell.

Over the course of the exercise, the JFO Coordination Group participated in daily conference calls with the RRCC, Connecticut State Emergency Operations Center (SEOC), and governor's office. The JFO Coordination Group was briefed numerous times by representatives from the Unified Command Post. There were also at least two conference calls between the Connecticut and New Jersey PFOs, as well as two additional calls between the PFO and the Secretary of Homeland Security. Some of these calls appear to have been an established part of the daily battle rhythm. In addition to daily objectives meetings, the JFO Coordination Group met as needed for conference calls and emerging situations. For the most part, members of this group were on call for meetings and conference calls throughout the day and night.

The PFO was responsible for keeping DHS apprised of the situation in Connecticut. Part of that information flow process was the production of regular SITREPs. These SITREPs reported the actions of participating Federal, State, and local agencies. Over the course of the four-day exercise, the PFO forwarded six SITREPs that detailed events, activities, or findings during the previous operational period. The SITREPs were sent to the Secretary of Homeland Security, IIMG, and HSOC. Eventually the reports were also posted on the Situation Unit's wall in the

JFO to improve situational awareness within the facility. Table II-1 identifies the operational period covered by each SITREP and the PFO's priorities or activities for that period.

Table II-1. Summary of Connecticut PFO SITREPs

Operational Period	PFO Areas of Activity
April 4, 1400-1700	• There has been an explosion at the Port of New London with an estimated 132 casualties. • The Captain of the Port has closed the Port. • There is a report that this was an intentional chemical attack. • Connecticut requests a Stafford Act declaration. • The FBI is coordinating flight restrictions over New London. • Samples are being collected (suspected mustard agent). • Code orange is in effect, and a state of emergency has been declared.
April 4, 1700-2200	• There have been 1,530 casualties (107 dead). • Travel restrictions are in place. • CDC has dispatched Rapid Response Registry. • Evacuations have occurred near the explosion. • Connecticut is considering shelter-in-place strategy. • Federal support is being staged. • FBI has discovered a suspicious aircraft. • Connecticut Governor and PFO held a press briefing on VNN. • JFO and Joint Information Center (JIC) are stood-up.
April 4, 2200-April 5, 0300	• PFO continues to monitor the investigation. • Rescue operations continue. • HHS reports on available assets to support Connecticut. • PFO coordinating with HSOC, NJ PFO, RRCC Region 1, State EOC, and Defense Coordinating Officer. • PFO focusing on public messaging strategy with Connecticut. • PFO expects to develop decontamination strategy with the State. • PFO priority is to assess impact on transportation and critical

Operational Period	PFO Areas of Activity
	infrastructure. • Coordinating sampling and decontamination strategies is a priority. • JFO is working with the State to clarify resource needs.
April 5, 0300-1500	• Rescue operations continue. • A total of 155 people have died, and more than 6,000 people from Connecticut have presented at hospitals. • PFO is monitoring resource needs and resource deployment. • FBI JOC is fully activated. • PFO continues to focus on public messaging. • A priority is to coordinate consistent scientific guidance. • Planning for upcoming response needs is a priority. • Plume modeling has been received.
April 5, 1500-2300	• PFO cell continues to monitor casualties. • Investigation continues, and progress is being made. • Public messaging will remain a priority. • PFO expects to incorporate other SFOs into the JFO Coordination Group. • Resource support continues to be provided to Connecticut. • There is discussion among Connecticut and New Jersey (Governors, PFOs, and FCOs) regarding increasing the HSAS level in Connecticut from Orange to Red.
April 5, 2300-April 6, 1500	• The investigation continues. • The current casualty count is 364 dead and 6,391 hospitalized. • The PFO plans to implement risk communication strategy with State EOC. • The PFO continues to assist State with requests for resources. • The common operating picture continues to be refined.

Table II-1 provides insight into the priorities of the Connecticut PFO. These priorities included providing consistent and pertinent public information, monitoring the investigation, and facilitating the deployment of Federal support.

Communications out of the JFO sections appeared to be more sporadic, depending on the needs of the staff. For example, the Situation Unit in the Planning Section was in fairly regular communication with the State EOC and the Situation Unit at the Unified Command Post. The former was given casualty numbers, and the latter was contacted to promote common situational awareness.

2. JFO and PFO Activities in New Jersey

In response to the detection of multiple, suspected cases of plague in New Jersey, the Secretary of Homeland Security declared the situation in New Jersey to be an incident of national significance (at 14:00 on April 4) and designated the New Jersey PFO (at 11:40 on April 4). Members of the PFO cell initially assembled at the FBI JOC and then transitioned to the Port Authority of New York/New Jersey Building in Jersey City, New Jersey where the JFO was established. During the day on April 5, the remainder of the JFO staff assembled at the Port Authority Building. By 16:00 on April 5, the New Jersey JFO was fully activated.

Figure II-3. Organization of the New Jersey JFO[27]

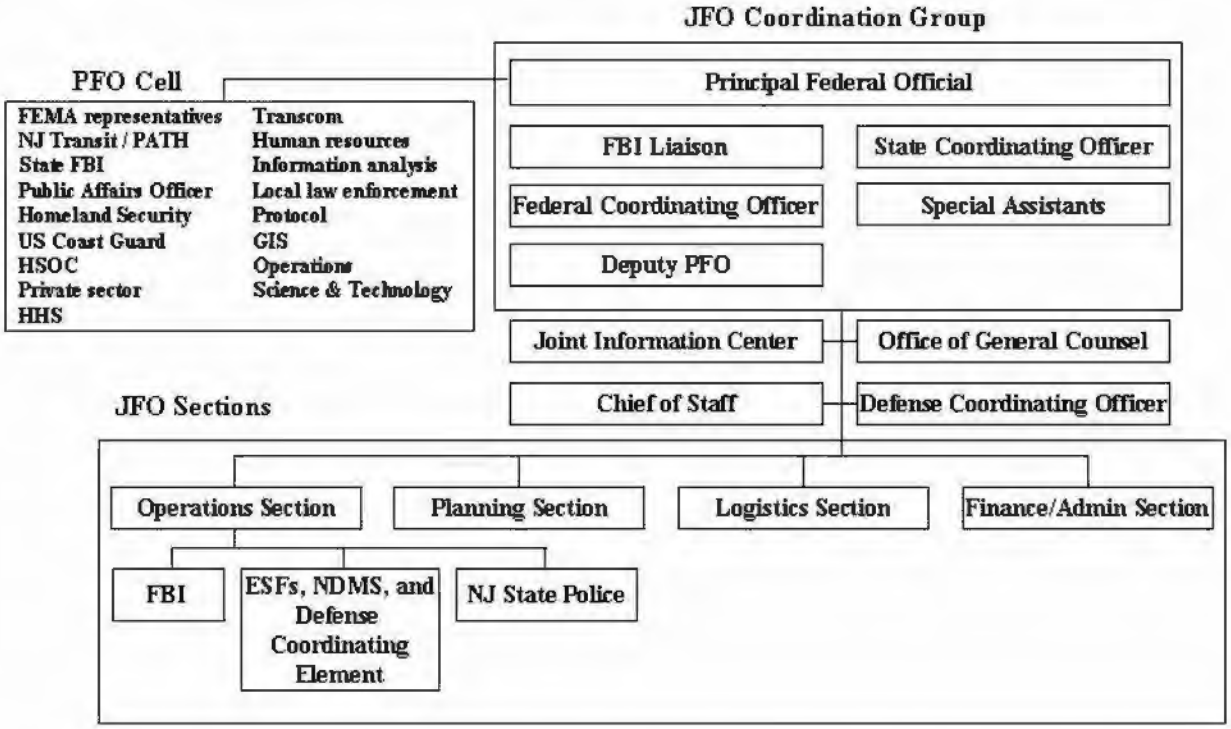


Figure II-3 is similar to the notional diagram found in the NRP. Like Connecticut, the primary difference between the New Jersey organizational diagram and the NRP diagram is the presence of a robust PFO cell. A difference between New Jersey and Connecticut was that in the former, the FBI JOC was not collocated with the JFO; the JOC was located in the FBI Newark Field Office. The FBI provided a liaison who worked in the JFO Operations Section.

Throughout the exercise, the primary activities of the PFO cell and JFO Coordination Group included collecting information and resolving issues that arose during the response. The types of information they collected on a regular basis included the following:

- status of the investigation;
- number of victims and available hospital beds;
- New Jersey's resource needs;
- number of active PODs; and
- number of citizens who had received prophylaxis.

[27] Figure 3 is a composite of several data sources and is intended to provide an overview of the New Jersey JFO structure. The figure may not document every position or organization in the New Jersey JFO.

In addition to collecting information, the Joint Coordination Group and PFO cell sought to resolve issues as they arose during the response. The issues on which they worked included the following:

- coordinating the Homeland Security Advisory System (HSAS) and State Alert System color codes;
- supporting the New Jersey POD effort;
- responding to requests from New Jersey to update the Stafford Act declaration;
- maintaining a consistent public message; and
- supporting State requests for resources.

As in Connecticut, the NJ PFO was responsible for keeping the Secretary of Homeland Security informed about the situation in New Jersey. To do so, the PFO distributed a series of SITREPs to Secretary of Homeland Security, IIMG, and HSOC during the exercise. These documents provide insights into the activities of the PFO cell and the issues it deemed significant. Table II-2 summarizes a sample of the PFO SITREPs from New Jersey and highlights the issues and topics that the PFO and JFO Coordination Group tracked during the exercise.

Table II-2. Summary of Selected New Jersey PFO SITREPs

Operational Period	PFO Areas of Activity
April 4, 10:30-12:30	• New Jersey may be a weapon of mass destruction (WMD) event. • Patients are reporting flu-like symptoms. • A tank sprayer in a vehicle tested positive for *Yersinia pestis.* • VNN is reporting that many people are ill. • This situation could affect infrastructure and the economy.
April 5, 23:00-April 6, 15:00	• JFO has been established. • There have been 6,508 fatalities, and 3,188 people have been hospitalized. • Implementation of the POD plan has begun. • HSAS level has been raised to Red statewide, and PFO cell is working to mitigate effects. • Travel restrictions are in place. • Distribution of antibiotics to heavily impacted counties will occur within 24 hours. • The investigation continues (details provided).

Operational Period	PFO Areas of Activity
	• JFO is facilitating the flow of resources to New Jersey. • An update to the Stafford Act declaration is pending. • BioWatch is deploying. • HHS is providing resources to New Jersey.
April 6, 15:00-23:00	• There have been 6,508 fatalities, and 3,877 people have been hospitalized. • POD operations are continuing. • Travel restrictions have been eased. • The requested declaration update has been completed. • PFO continues to work HSAS issues. • The investigation continues (details provided). • JFO continues to facilitate the flow of resources. • HHS continues to provide resources to New Jersey. • Rail industry remains at Alert Level 2. • Port security measures will have economic impact.
April 7, 08:00-15:00	• There have been 8,070 fatalities, and 4,567 people have been hospitalized. • State POD operations continue. Federal PODs have been demobilized. • Travel restrictions have been lifted. • Operation Exodus has been implemented. • PFO cell continues to work HSAS issues with State. • The investigation continues (details provided). • State requests update to declaration. • JFO continues to facilitate the flow of resources. • BioWatch results are available (details provided). • U.S. Coast Guard continues to work port security issues. • Private sector issues are significant (e.g., tourism, worker absenteeism, and food safety). • HHS continues to support New Jersey response.

The JFO sections staff was located in the Port Authority Building with the PFO and JFO Coordination Group. The principal function of the JFO sections during the T3 FSE was to support the mission assignment process and facilitate the flow of resources to New Jersey.[28]

D. Analysis

The analysis of JFO operations in Connecticut and New Jersey indicates that a combination of factors made it difficult for the JFO staff to manage its internal processes and maintain situational awareness. These factors included the following:

- unclear lines of authority within the JFO;
- undefined roles and responsibilities in the PFO cell; and
- a lack of implemented processes for sharing information.

Together, these factors adversely affected the operation of the JFO during the T3 FSE and ultimately its ability to support emergency response operations in both States.

1. Unclear Lines of Authority within the JFO

Observations from both New Jersey and Connecticut suggest that the NRP and JFO SOP have not clearly defined the lines of authority inside the JFO. In particular, the line(s) of authority that connects the PFO, FCO, and JFO cell is ambiguous. Clarifying this line of authority would identify who in the JFO Coordination Group is responsible for managing staff and directing activities in the JFO cell.

At first glance, the PFO appears to be the Federal official responsible for the operation of the JFO. The NRP states that the PFO represents that Secretary of Homeland Security as the "lead Federal official." Placing the PFO at the top of the JFO organizational diagram (see Figure II-1) implies that the PFO has authority over the JFO. In addition, there was a perception among many at the Connecticut and New Jersey JFOs that the PFO was responsible for JFO operations. The NRP also states that in cases in which a Stafford Act disaster has occurred, but no PFO has been assigned, the FCO provides overall coordination for the Federal components of the JFO. Despite these statements, it is not clear whether the PFO has authority over the JFO cell. This authority is not assigned to the PFO or to any other official in the NRP or the JFO SOP.

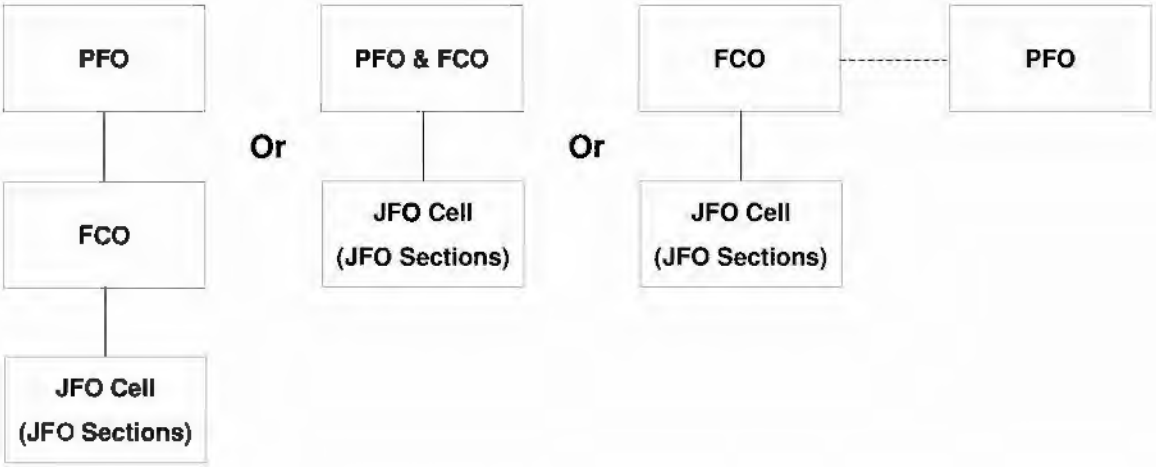
Like the PFO, there are statements in the NRP and observations from the exercise *suggesting* that the FCO has final authority over the JFO cell and the Federal resourcing process. The NRP states that the FCO manages and coordinates Federal resource support. During the exercise, the JFO cells in both States took direction from the FCO.

---

[28] For additional information on the T3 FSE resourcing process, please refer to the "Resource Requests and Resource Coordination" section of this report.

The description of the relationship between the FCO and the PFO provided in the NRP and JFO SOP is also vague. For example, the JFO SOP states that "the PFO and FCO (in Stafford Act situations in which a PFO is not designated) are responsible for the overall coordination and management of the JFO Coordination Group." In addition, the NRP states that the FCO supports the PFO, but it does not use a term that implies a line of authority, such as "reports" or "directs." The descriptions of the PFO and FCO roles and responsibilities could be interpreted at least three different ways. Figure II-4 shows these three possibilities based on interpretations of what is written in the NRP and JFO SOP.

Figure II-4. Possible Lines of Authority Between the FCO and PFO



Resolving the ambiguous relationships between the PFO, FCO, and JFO cell will help to address the following important questions about the organization and operation of the JFO:

- Who ultimately runs the JFO?
- Who establishes priorities?
- Who reports to whom?
- Who can make JFO-wide decisions?

Resolving these questions would encourage a unity of effort and improve the JFO's internal staff processes.

2. Presence of a PFO Cell with Undefined Roles and Responsibilities

In Connecticut and New Jersey, substantial PFO cells operated through the end of the exercise. Their presence added additional coordination requirements, and their functions overlapped with those of the JFO. In some instances, the PFO cells worked on the same issues as the JFO cells;

however, the PFO cells also focused on policy issues and public messaging responsibilities that were not priorities for the JFO cells. The JFO cells tended to focus on resourcing and operational issues, rather than on policy and public information. Although the presence of the PFO cells increased coordination requirements inside the JFO, these costs may have been offset by the contributions that the PFO cell made in areas not addressed by other elements in the JFO.

In structure and performance, the PFO cell was an additional node in the Federal response structure in both States. According to the JFO SOP, most of the individuals in the PFO cell are part of the deployed PFO support staff, a small interagency team of subject-matter experts who deploy with the PFO to provide initial support until a JFO is established. They are expected to serve as the PFO's expanded advance team and then integrate into the appropriate JFO sections once the JFO stood up. In practice, the PFO cells in the Connecticut and New Jersey JFOs remained a separate entity throughout the exercise. It is unclear exactly why that integration never occurred in Connecticut, though the issue was discussed on April 4, between approximately 22:10 and 22:30. Instead, the decision was made to maintain the cell members in the PFO location as technical advisors. The result of this decision was a virtual standalone capability for the PFO and, by default, for the JFO Coordination Group. They did not rely on the JFO sections for information, expertise, or situational awareness.

In New Jersey, the PFO cell had an independent staff of more than 30 personnel per shift and resembled a command center, rather than an advisory group. Members of the cell manned positions in front of large display screens (i.e., a knowledge wall). These members represented a variety of organizations participating in the response, including the HSOC, FBI, U.S. Coast Guard, FEMA, DHS, HHS, NJ Transit, and private sector. The PFO cell operated as an independent staff. It held regular turnover briefs during which the outgoing shift would update the incoming shift about the numbers of victims, status of the investigation, issues that had been resolved, and tasking that the incoming staff was expected to complete. The PFO cell in New Jersey did not rely on the JFO sections as a primary source of information about the response.

In New Jersey, the PFO and JFO cells worked on an overlapping set of response issues. In some instances, they worked on the same issues. In other cases, the PFO cell worked on issues not addressed by the JFO cell. Table II-3 illustrates the issues on which the New Jersey PFO and JFO and JFO Cells tended to focus:

Table II-3. New Jersey PFO and JFO Cell Issues

NJ Response Issues	PFO Cell Focus	JFO Cell Focus
Resourcing States needs	Yes	Yes
POD operations	Yes	Yes
HSAS	Yes	No
Updating declaration	Yes	No

Public messaging	Yes	No
Reporting to DHS	Yes	No
Travel restrictions	Yes	No

According to Table II-3, the New Jersey PFO cell became involved in several response areas, such as shaping response policy (e.g., HSAS, declarations, and transportation restrictions), developing public messaging, and collecting/reporting information to the Secretary of Homeland Security. Observations made during the exercise indicate that the PFO cell assumed ownership of several response issues, thereby fulfilling a constructive role in the response.

That the PFO cell worked on issues not addressed by the JFO cell indicates a need for reliable coordination inside the JFO, because such issues could have an impact on the activities of the JFO cell. For example, travel restrictions could affect the movement of resources and personnel, and changes to a declaration could affect decisions made in the JFO cell regarding the types of assistance that the Federal government can provide and to whom the assistance can be provided.

Table II-3 also highlights issues on which the JFO and PFO cells both worked. This is not a problem per se, but can become an issue if the staffs do not coordinate their activities. For example, in Connecticut, JFO staff members made the erroneous assumption that if something was known by personnel in the PFO cell, it was also known by their counterparts in the JFO cell. When the PFO and JFO cells work on overlapping issues, a reliable mechanism for intrastaff coordination inside the JFO must be implemented.

In Connecticut, the PFO assigned some tasks to the JFO that should have been addressed at the Incident Command Post level, rather than at the JFO. For example, the preparation of sampling and decontamination plans (see Table II-1) for the Connecticut incident is an aspect of tactical operations that should have been undertaken at the Incident Command Post level. (The PFO/JFO may ask to review such plans, but they should be prepared by the ICP.) This illustrated the need for PFOs to have better training on the difference between the scope of work for JFO and ICP operations.

3. Lack of Implemented Processes for Sharing Information

In Connecticut, there were few and varied efforts to ensure common situational awareness across the facility; however, these efforts were largely ad hoc. There were few, if any, opportunities for JFO-wide briefings. Most information sharing was conducted among small groups. Although the New Jersey PFO cell conducted regular turnover briefs, the JFO as a whole faced information-sharing challenges similar to those observed in Connecticut.

The Connecticut JFO did not hold standard shift-change briefs or situational meetings. Different sections in the JFO met as needed throughout the day. The battle rhythm called for an operations, objectives, strategy, and planning meeting each day at approximately 08:00, 09:00, 13:00, and post-16:00, respectively. It is unclear how often these meetings actually occurred. In fact, much

of the data suggest that these meetings did not occur as scheduled. In particular, data collectors noted that the planned daily operations briefing by the Operations and Planning Chiefs for the entire JFO was missing. Additionally, there were no shift-change briefs/meetings for the JFO as a whole. Rather, turnover was largely left up to individuals in the PFO cell, in the different sections, and in the ESFs.

The Situation Unit of the Planning Section, the group responsible for the common operating picture in the JFO, was at a distinct disadvantage for much of the exercise because it was not present in the PFO workspace and conference room and the flow of information out of that room was poor.[29] For example, the Connecticut PFO cell and JFO Coordination Group were getting fairly regular updates from the JOC about the investigation, but the Situation Unit could only get that information from the State EOC or RRCC.

The Connecticut PFO cell and JFO Coordination Group had no formal method by which to pass information to persons outside of the room. The only individuals who went back and forth between the PFO space and the JFO were the FCO and SCO. Although they relayed some information, they had neither the time nor the processes in place to be the primary conduits. Some agencies had representatives in the PFO room, either in the PFO cell or as SFOs in the JFO Coordination Group. To a certain extent, these agencies were at an advantage because they may have received regular updates from those representatives. But this may have also added to coordination challenges, as those individuals and ESFs knew more than the other staffers in the JFO sections. For example, the HHS SFO involved ESF-8 in much of the dialogue and debate about transferring patients out of the State. But when ESF-8 members tried to coordinate with the Operations Branch, confusion reigned because the latter were not up to date on the situation.

The only concerted effort to share information in the Connecticut JFO appeared to be the consolidation of the twice-daily SITREPs for the IIMG, but this was largely a paper drill for DHS headquarters, with different sections and Federal, State, and local agency representatives submitting their input to the Situation Unit, who then passed it to the HSOC watch stander in the PFO cell. Additionally, the SITREP was a one-way information flow for the most part, with contributors pushing information up, but not making an effort to move information horizontally around the JFO or back down from the PFO. Further, it is apparent from reviewing those SITREPs that little effort was made to confirm inputs or correct errors. Within SITREPs, we find examples of contradictory information. For example, much confusion existed in the JFO Coordination Group at the conclusion of the exercise as to the mechanism used by the terrorists to disperse the mustard agent. The group still believed that the agent came from the truck bomb rather than the aircraft. This is troublesome, considering the FBI had concluded that the aircraft was the device and that the SAC was a member of the JFO Coordination Group. It is evident that

[29] The physical layout of the Connecticut JFO included one large room for the JFO sections, a second large room for the JOC, and a small room off to the side for the PFO sell and JFO Coordination Staff. JFO Coordination Group meetings and conference calls were also held in the smaller room. The two workspaces were divided by a set of doors. Access to the JOC was strictly limited to law enforcement personnel and persons with appropriate badges.

consolidation and clarification of information did not occur. In the same SITREP from 03:00 on April 5, it was reported that:

- the airplane [in Maine] tested positive for precursors to mustard; and
- the airplane [in Maine] was only equipped with normal crop dusting equipment, and all further forensic examinations yielded negative results.

The SITREP from 15:00 on the same day did not clarify the contradictory information. In fact, it reported that:

- per the Transportation Security Administration (TSA), the FBI analysis of the 55-gallon tank aboard the plane yielded no trace of mustard, but rather contained residue of ammonium nitrates; and
- per the FBI, the two drums found on the plane tested positive for sulfur mustard, and additional samples analyzed by Edgewood also tested positive.

It is not surprising that the Connecticut JFO Coordination Group was never clear on the dispersal mechanism. In fact (as is discussed in a later thread), confusion persisted throughout the exercise and across the operations centers. Improved coordination and communication within the JFO, to include the JOC, may have resolved some of the misperceptions.

4. Issues from Previous Exercises

As the T3 FSE had, the T2 FSE exercised the PFO position but not the JFO structure, because the JFO is a recent addition to the Federal response effort. The comparison of these two exercises indicates that there has been little improvement in this area since T2. In at least one area, the issue may have worsened. Table II-4 compares the T3 FSE experience with the PFO with the experience of other exercises and notes if any changes were observed.

Table II-4. Comparison of T3 FSE with Previous Exercises

T2 FSE	SOEs	T3 FSE
SIGNIFICANT DECISIONS		
• Secretary of Homeland Security designated PFOs and deployed them to Washington and Illinois. • It was the first time the PFO concept was implemented.	• The JFO would be established after an incident of national significance (INS) was declared.	• Secretary of Homeland Security appointed PFOs in New Jersey and Connecticut. • Once an INS was declared in both venues, JFOs stood up in New Jersey and Connecticut.
ISSUES/OBSERVATIONS		
• FSE demonstrated that the new PFO role would need a dedicated staff to be effective.		• In Connecticut, the PFO cell duplicated much of the capabilities and expertise resident in the JFO sections, but it lacked its own clear purpose or delineated

		responsibilities. • Overlapping or competing activities occurred in the PFO cell and the JFO section.
• Roles and responsibilities of the PFO were not well defined relative to the FEMA Regional Directors and FCO.		• Lines of authority and coordination among the PFO, FCO, and JFO sections were unclear and hampered unity of effort. • The relationship between the PFO and FCO is not formalized, and final authority over the JFO cell was unclear.
		• The JFOs did not follow standard processes for sharing information internally.
	• Participants acknowledged that there would be confusion in the immediate aftermath of an INS prior to the establishment of a JFO. • Once the NRP is activated, the JFO must rapidly assume its role as the central point of coordination for Federal, State, and local officials and for the effective use of Federal incident-related response and recovery resources.	

The comparison of the T2 and T3 experiences suggests that there has been little improvement in the process of PFO operations. Although the addition of the PFO cell addresses an issue identified in the T2 FSE After-Action Report, its presence in the T3 FSE adversely affected the PFO's ability to unify the Federal response effort. The need for better defined roles and responsibilities of the Federal officials supporting the response remains.

E. Conclusions

The detection of plague in New Jersey and the release of a mustard agent in Connecticut prompted Federal officials to activate JFOs and select PFOs for both States. The analysis of JFO operations indicates that the JFO staff encountered problems coordinating the activities of JFO staff elements. For example, lines of authority were unclear, and the prominent role played by the PFO cells in both States complicated JFO operations. Furthermore, the JFO staff did not follow standard processes for sharing information internally. Resolving these structural and process issues would improve staff operations and ultimately strengthen the JFO's ability to coordinate Federal and State response efforts.

The analysis of the NRP, JFO SOP, and exercise observations indicates that lines of authority and coordination in the JFO are unclear. The relationship between the PFO and FCO is not formalized, and final authority over the JFO cell is ambiguous. Clearly documenting these relationships would eliminate a potential source of confusion in JFO operations.

The presence of vigorous PFO cells in New Jersey and Connecticut complicated operations in the JFOs. Their presence added additional internal coordination requirements. In some instances, the PFO and JFO cells on an overlapping set of response issues or worked on the same issues. In other instances, the PFO cell worked on issues not addressed hy the JFO cell, hut the outcomes of these issues could have an impact on activities in the JFO cell. The observations that the PFO operated as a separate node inside the JFO and worked on some of the same issues as the JFO cell indicate a need for a reliable mechanism for intra-staff coordination in the JFO.

Although the PFO cell played a prominent role in the T3 FSE, the NRP and JFO SOP do not provide detailed descriptions of its roles and responsibilities. JFO operations would also benefit from additional information about how the PFO cell is expected to support JFO operations.

Observations from Connecticut indicate that information sharing and dissemination inside the JFO were problematic. There were few, if any, opportunities for JFO-wide briefings, and there was no formal mechanism for establishing a common operational picture. Instead, the sharing of information inside the JFO was largely informal and ad hoc. Formal information-sharing procedures would likely improve the situational awareness of JFO members. Additionally, it may he heneficial to identify an individual whose sole responsibility is the management of the facility and the shared JFO battle rhythm. This person should have no operational responsibilities in the response, but would manage the integration of the JFO itself.

1. Recommended Courses of Action

- Clarify the relationship between the PFO, PFO cell, and FCO, to include the scope of their operational responsibilities and their authorities within the JFO.
- Develop a checklist to manage the integration of the PFO cell with the JFO sections once the latter is fully activated.
- Implement formal information-sharing processes and procedures within the JFO to improve internal situational awareness. Identify, train, and authorize an individual to manage the JFO and the information-sharing processes.

III. Resource Requests and Resource Coordination

A. Introduction

The TOPOFF 3 Full-Scale Exercise (T3 FSE) provided the Federal government an opportunity to exercise the process of supporting States that have been overwhelmed by a significant terrorist attack involving a weapon of mass destruction (WMD). Following the releases of *Yersinia pestis* and sulfur mustard agent, officials in New Jersey and Connecticut requested a variety of resources from the Federal government, including medical supplies, healthcare professionals, transportation support, security personnel, mortuary affairs teams, and decontamination units. In addition to these State requests, Federal agencies pushed assets to support the State responses.

Exercise observations indicate that the resourcing process was problematic in both States. State and Federal officials were uncertain about what had been requested, who requested it, and what

was being provided. The questions were prompted by a combination of factors that included the following:

- participants used three different resourcing processes that were not well coordinated;
- Federal and State officials struggled with the implementation of these processes; and
- reliable information about resources was not readily available.

Delays and uncertainty caused by these issues frustrated participants, who were often uncertain about who had requested what. Resolving these issues would strengthen the ability of State and Federal officials to match the resource needs of responders with available assets.

SUMMARY OF CONCLUSIONS: RESOURCE REQUEST AND COORDINATION PROCESS

- The use of multiple resource processes created uncertainty and adversely affected situational awareness.
- State and Federal officials struggled with the implementation of the Federal resourcing process.
- The role of the HHS SERT was neither well-defined nor understood by participants. At times the SERT duplicated functions performed by ESF #8 in the JFO.
- Information about the status of resources was not readily available and the process lacked transparency.

B. Backgronnd

The Federal government can provide support when States are overwhelmed by a major incident. To access these resources, a State must first identify what is needed to support the response. In this step, State officials compare the response needs with the resources that are available from State and local agencies.[30] If unmet needs remain, the State can request additional resources (i.e., both personnel and materiel) from the Federal government.

During emergency operations, local responders are usually the first to arrive on-scene. At that time, the Incident Commander (IC) assesses the response needs and submits resource requests to the local emergency operations center. Requests that exceed local capabilities are submitted through the State's emergency response chain of command to the State Emergency Operations Center (EOC). The EOC will attempt to match the needs of the IC with assets that may exist elsewhere in the State or be accessible through mutual aid agreements with neighboring States such as the Emergency Management Assistance Compact which was exercised by New Jersey during the FSE. In emergencies that do not have a defined incident site, such as a Statewide disease outbreak, local EOCs and agencies can submit their resource requirements to the State EOC, which will attempt to locate the needed resource somewhere in the State. If it cannot locate the required support, the State can submit its request to the Federal government.

[30] The State may be able to access additional resources through agreements with neighboring jurisdictions such as the Emergency Management Assistance Compact which was exercised by New Jersey during the FSE.

State officials can use two methods to obtain support from the Federal government: (1) support provided under the Stafford Act mission assignment process, coordinated through the JFO, and (2) direct agency support.

1. JFO Mission Assignment Process

During a major incident, States can access Federal resources by engaging the JFO and requesting resources through the mission assignment process. This process requires that States document their requests on action request forms (ARFs), on which State officials describe the assistance they are requesting. Before the JFO can draft a mission assignment, the State Coordinating Officer (SCO), Federal Coordinating Officer (FCO), and the JFO Operations Section Chief review the ARF. If approved, the JFO drafts a mission assignment (a work order) directing a Federal agency to complete a task.[31] For example, a mission assignment could be used to task the Centers for Disease Control and Prevention (CDC) to provide epidemiologists to a State experiencing a disease outbreak.

Once drafted, the mission assignment is assigned to one of 15 emergency support functions (ESFs). ESFs are members of the JFO staff and SMEs on a functional area. Table III-1 lists the ESFs described in the NRP and identifies the coordinator for each.

Table III-1. Emergency Support Functions (ESFs)

ESF No.	ESF Name	Coordinating Department/Agency
ESF #1	Transportation	Dept. of Transportation
ESF #2	Communications	Dept. of Homeland Security
ESF #3	Public Works and Engineering	Dept. of Defense
ESF #4	Firefighting	Dept. of Agriculture
ESF #5	Emergency Management	Dept. of Homeland Security
ESF #6	Mass Care, Housing, and Human Services	Dept. of Homeland Security
ESF #7	Resource Support	General Services Administration
ESF #8	Public Health and Medical Services	Dept. of Health and Human Services
ESF #9	Urban Search and Rescue	Dept. of Homeland Security
ESF #10	Oil and Hazardous Materials Response	Environmental Protection Agency
ESF #11	Agriculture and Natural Resources	Dept. of Agriculture

[31] See Unit 4 at http://training.fema.gov/EMIWeb/IS/is292lst.asp.

ESF No.	ESF Name	Coordinating Department/Agency
ESF #12	Energy	Dept. of Energy
ESF #13	Public Safety and Security	Depts. of Homeland Security and Justice
ESF #14	Long-term Community Recover and Mitigation	Dept. of Homeland Security
ESF #15	External Affairs	Dept. of Homeland Security

A principal function of the ESF groups is to support the mission assignment process, which provides Federal resources to the State.[32] The ESF group responsible for a particular mission assignment will contact the Federal agency and task it to provide the support outlined in the mission assignment. The ESF staff will then coordinate the delivery of the requested support to the State. The tasked Federal agencies can be reimbursed for the costs of providing this support under the Stafford Act if an emergency or major disaster is declared.

2. Direct Federal Agency Support

Some Federal agencies have their own authorities to provide direct support to States. In some instances, the support is provided at the request of the State. In other instances, the Federal agency support is unsolicited, direct support to the State. For example, the Department of Health and Human Services (HHS) may provide epidemiologists and a Secretary's Emergency Response Team (SERT) to a State experiencing a disease outbreak.

The SERT is a deployable team of public health SMEs that "directs and coordinates the activities of all HHS personnel deployed to the emergency site to assist local, State, and other Federal and government agencies as applicable response effort for HHS."[33] The SERT will likely deploy when the HHS Secretary declares a public health emergency. According to the HHS CONOPS, the SERT receives mission assignments, priorities, and objectives from the HHS leadership. These mission assignments will be coordinated with, and may be at the request of, other Federal entities, particularly DHS. Once in the field, the SERT:

- directs and coordinates HHS response assets;
- represents HHS in interactions with local, State, territorial, and tribal government public health and medical incident management authorities, as well as the regional response structure;
- assesses the requirements or potential needs for additional HHS assistance;

[32] ESFs also coordinate assistance among Federal agencies.

[33] U.S. Department of Health and Human Services. Concept of Operations Plan (CONOPS) for Public Health and Medical Emergencies. March, 2004.

- facilitates the transmission of incident information from incident authorities to the Assistant Secretary for Public Health and Emergency Preparedness (ASPHEP) through the Secretary's Command Center; and
- provides continuous assessment of the adequacy of the HHS response to the HHS Secretary through the ASPHEP.[34]

Direct agency support does not use the mission assignment process or require JFO approval. Direct support expenditures are not reimbursed under the Stafford Act. The Federal agency requesting the support usually funds the support.

For additional information about the Stafford Act and the NRP discussion about Federal-to-Federal support, refer to the "Integrating Responses to Incidents of National Significance" section of this report.

C. Reconstruction

The nature of the disasters in Connecticut and New Jersey caused the States to organize their responses differently. These differences affected how the officials in the two States implemented their resource request processes. In Connecticut, there was a definitive incident site containing victims and debris. From a nearby command post, the IC—later the Unified Command—could assess the needs of the tactical units and pass requests for support to State and Federal agencies. In New Jersey, there was no single incident site and no single, designated IC. *Yersinia pestis* was disseminated over areas of Middlesex and Union Counties, and victims were located throughout the State. Unlike in Connecticut, there was no IC to develop resource needs at the tactical level in New Jersey. Agencies, such as county health departments, and organizations, such as hospitals, participating in the New Jersey response coordinated requests for assistance through their local EOC, State EOC, and State Health Command Center (HCC).

1. Connecticut Response Structure and Resource Needs

The sulfur mustard gas attacks in New London resulted in a demand for resources that exceeded the capabilities of the first responders. During the first hours of the crisis, the IC in Connecticut mobilized resources through established agreements for mutual aid or through the New London and State EOCs. Late in the day on April 4, the Unified Command Post (UCP) replaced the Incident Command Post (ICP). The UCP staff included the first responders from the ICP with augmentation from many State and local Federal agencies, including the US Coast Guard, FBI, DHS, EPA, Connecticut Department of Environmental Protection (DEP), National Disaster Medical System, (NDMS) and Connecticut Department of Public Health (DPH). The UCP participated in the resource request and allocation process through the end of the exercise.

---

[34] U.S. Department of Health and Human Services. Concept of Operations Plan (CONOPS) for Public Health and Medical Emergencies. March, 2004.

The State EOC submitted resource requests to the JFO when the State and local agencies could not meet the needs. To minimize disruption as the JFO stood-up, the JFO relied on FEMA's Regional Response Coordination Center (RRCC) located in Maynard, Massachusetts, to coordinate the mission assignment process during the early hours of the exercise.

Table III-2 lists examples of resources employed in Connecticut during the exercise. These resources are grouped into two broad categories, medical and nonmedical.

Table III-2. Examples of Resources Employed or Requested During the Connecticut Response

Resources Needs	Connecticut	Federal/Other
Medical-related support		
Hospital capacity	Area hospitals	Nationwide 10,000 Bed alternate care facility (ACF)
Hospital census		Rapid Response Registry
Medical personnel	DMAT/Medical Reserve Corps	Disaster Medical Assistance Team (DMAT)
Medical supplies		Ventilators/bronchial dilators (SNS)
Mortuary support	Refrigerated trucks	Disaster Mortuary Operations Response Team (DMORT)
Patient movement	EMS/National Guard	National Disaster Medical System (NDMS)
Nonmedical support		
Animal removal	Local resources	
Decontamination	State resources	
Dive teams	Local resources	
Family assistance/feeding		Red Cross
Ground transportation	Local resources	
Response support	State and local resources	ERT JFO and PFO Cells Defense Coordinating Officer (DCO)
Incident support	National Guard (CST)	Domestic Emergency Support Team (DEST) Emergency Response Team-A and ERT-N
Security	State Police, CTNG (QRF)	Department of Defense Quick Reaction Force (QRF)
Urban search/rescue	Connecticut Urban Search and Rescue (USAR)	MA & NJ USAR

Many resource requirements were met entirely with local or State assets, including:

- transportation assets to remove dead animals;
- dive teams to search for secondary devices;
- decontamination assistance for two area hospitals; and
- vehicles to support emergency response personnel at the incident site.

In other cases, State resources were augmented with Federal assets or those from neighboring States. For example:

- New Jersey and Massachusetts provided USAR teams to assist with rescue efforts.
- The Department of Defense provided a Quick Reaction Force (QRF) to relieve Connecticut National Guard units protecting a local nuclear power plant.
- The American Red Cross (ARC) established a Family Assistance Center (FAC) and provided food at the incident site.
- The FBI requested the deployment of the Domestic Emergency Support Team (DEST), an interagency team of subject matter experts who respond to incidents involving WMD.
- FEMA's RRCC deployed an Emergency Response Team—Advanced Element (ERT-A).

The Federal government also supported Connecticut's efforts to care for the victims of the attack. This support included the deployment of Disaster Medical Assistance Teams (DMATs), Disaster Mortuary Operational Response Teams (DMORTs), and medical supplies from the Strategic National Stockpile (SNS).

2. Resources Needed During the New Jersey Response

The release of *Yersinia pestis* in New Jersey created a demand for resources that exceeded the capabilities of State and local governments. The response activities that placed the greatest demands on the State's resources were Points of Dispensing (POD) operations, treating victims, and mortuary affairs. For example, staffing the State's PODs required thousands of workers. Additional resource demands were placed on the State's healthcare facilities—by April 8, approximately 37,500 residents (sick and dead) had developed plague and many of those had sought treatment. Similar demands were placed on New Jersey's mortuary infrastructure. State officials had to locate facilities to store and dispose of more than 9,500 bodies, prompting a request for Federal assistance. Table III-3 lists examples of these resource needs and identifies the organizations from which resources were requested or provided.

Table III-3. Examples of Resources Employed or Requested in the New Jersey Response

Resources/Assistance	New Jersey	Federal/Other
Medical-related support		
Hospital capacity	Area hospitals	10,000 Bed alternate care facility (ACF)
Agent identification	Hospital labs State labs	CDC labs Epidemiologists (CDC)
POD staffing	Local health departments New Jersey National Guard	Veterans Affairs staff Federal Protective Services staff Postal Service employees
Medical personnel	Hospital staffs Local resources	DMAT NDMS management support team (MST) Emergency Management Assistance Compact (EMAC) Veterans Affairs health professionals
Medical supplies	Local supplies	Antibiotics (SNS) Technical advisory response unit (TARU) Ventilators
Mortuary support	Funeral directors County medical examiners	DMORT Refrigerated trucks
Patient movement	Local ambulances	NDMS personnel (Operation Exodus) 250 ambulances NY Air National Gnard C-130 (Operation Exodus)
Nonmedical support		
Veterinary support	Local support	Veterinary medical assistance team (VMAT)
Transportation	Local resources	Helicopters
Response support	State and local resources	FEMA ERT-A deployed to State EOC HHS SERT JFO and PFO Cells DCO
Law enforcement	New Jersey State Police Local law enforcement	FBI

Public messaging	State public info officers County public info officers	Joint Information Center Leaflet drop 50 public information officers

Although Table III-3 is not exhaustive, it lists the types of resources that were provided by Federal, State, and local agencies during the exercise. To access many of the Federal resources listed in Table III-3, officials in New Jersey exercised the mission assignment process through the JFO. Support for health and some medical support could also be requested through the HHS SERT.

In many instances, the Federal support was notional. Equipment and personnel were identified on paper, but not actually deployed (e.g., refrigerated trucks, the alternate care facility, and many medical personnel); however, some support was real, for example:

- The CDC deployed SNS training pallets to the New Jersey receipt, stage, and storage (RSS) site.
- The TARU team deployed to New Jersey and met the SNS shipments.
- The ERT-A deployed to the State EOC in West Trenton.
- The New York National Guard flew a C-130 to New Jersey and loaded the aircraft with Operation Exodus patients.

The resources that were actually deployed during the T3 FSE were preplanned as part of the exercise.

D. Analysis

The analysis of the State and Federal resourcing efforts indicates that a combination of factors impeded the ability of the two States to access Federal support during the T3 FSE. These factors included:

- Participants used three different resourcing processes that were not well coordinated.
- Federal and State officials struggled with the implementation of these processes.
- Reliable information about resources (e.g., the status of requests) was not readily available.

Together, these factors contributed to a breakdown in the resourcing process, making it difficult for participants to match the State's needs with available Federal resources. In New Jersey and Connecticut, participants were uncertain about what had been requested, who had requested it, and what the status of the request was. Without access to this information, response planners and decision makers could not fully comprehend the complete resource picture.

1. Impact of Resourcing Issues

The comparison of resource awareness presented in Table III-4 indicates that the T3 FSE resourcing process did not meet the needs of the response organizations. The data in Table III-4 demonstrate that responding organizations in New Jersey were often unaware of the activities of their counterparts. This lack of awareness and the inconsistent information provided by and available to these organizations suggests that the process of matching the resource needs of New Jersey with available Federal assets did not function as intended.

The entries in Table III-4 are compiled from T3 FSE authoritative sources. The State EOC entries are based upon copies of ARFs provided by the New Jersey Office of Emergency Management (OEM). The entries under the IIMG heading are based on the IIMG list of "Federal Assets Deployed." The entries under the HHS support heading are based on HHS SITREPs. The JFO/RRCC entries are based on two mission assignment logs compiled and provided by FEMA. These entries indicate that officials supporting the New Jersey response did not have a consistent picture of the resources that had been requested and deployed.

Table III-4. Lack of Resource Awareness in New Jersey

Resource	State EOC	IIMG	HHS Support	JFO/RRCC
Bio Emer. Support Team (BEST)	No request	Deployed	Not listed	No MA*
800 units of blood	No request	Deployed	Not listed	No MA
Relocatable field laboratory	No request	Deployed	Not listed	No MA
Disaster portable morgue unit	2 requested	1 deployed	Not listed	1 assigned
DMORT	8 requested	2 deployed	Deploy all available	2 assigned 2 via NDMS
DMAT	No request	2 deployed 14 staged	5 deployed	No action -10 DMATs staged
VMAT	2 requested	2 deployed	Not listed	1 via NDMS
Management support team	No request	3 deployed	Deployed	No MA
Strategic national stockpile support	Requested by governor	Deployed	Deployed	No MA
Ventilators	2500+ requested	2000 deployed	Not listed	MA issued
1200 US Public Health officers	No request	Deployed	Not listed	No MA
3000 personnel from MRC	No request	Deployed	Not listed	MA issued
Epidemiological teams	No request	Deployed	40 deployed	No MA
HHS ARC mental health team	No request	Deployed	Not listed	No MA

Resource	State EOC	IIMG	HHS Support	JFO/RRCC
10,000 bed alternate care facility	No request	Not listed	HHS direct request	No MA
Alternate care facility staff	Requested	Not listed	HHS direct request	MA issued
Refrigerated trucks/trailers	100 requested	Not listed	Deployed 12–15	MA issued
400 emergency medical techs	No request	Not listed	Deployed	No MA
2 x 250 bed DoD field hospital	No request	Not listed	Requested	No MA
SNS TARU	No request	Not listed	Deployed	No MA
Epidemiologist to NJDHSS	Requested**	Not listed	Deployed	No MA
15,000 POD workers	No request	Not listed	Working	No MA
4,000 POD security personnel–FPS	Reqnested	Not listed	Not listed	MA issued
DMART	No request	Not listed	Not listed	Requested
2,000 crisis counselors	Requested	Not listed	Not listed	Rejected
100 body handlers	Requested	Not listed	Not listed	Unresolved
250 ambulances	Requested	Not listed	Not listed	Unresolved
500 POD personnel	No request	Not listed	Not listed	Unresolved
12,000 medical personnel	No request	Not listed	Not listed	MA issued
Mobile communications for NJ ME	No request	Not listed	Not listed	MA issued
261 medical personnel	Requested	Not listed	Not listed	Unresolved
50 public information officers	Requested	Not listed	Not listed	Unresolved
Staff for 500 bed facility	Requested	Not listed	Not listed	Unresolved
100,000 N95 respirators	Requested	Not listed	Not listed	MA issued
100 PPE for DMORT	Requested	Not listed	Not listed	No MA
4 helicopters	Requested	Not listed	Not listed	No MA
POD security 1826 personnel	Requested	Not listed	Not listed	No MA
POD security 2350 personnel	Requested	Not listed	Not listed	No MA
50 body trackers	Requested	Not listed	Not listed	No MA
Generators and mobile lights	Requested	Not listed	Not listed	No MA
Leaflet drop	Requested	Not listed	Not listed	No MA

* MA = mission assignment; ** Based upon a request from the NJ Department of Health and Senior Services

The list of requested and provided resources in Table III-4 highlights the impact that the three resource issues noted above (i.e., the use of multiple processes, implementation struggles, and a lack of ready information) had on the T3 FSE resourcing process. In short, this process was fragmented. Most organizations involved in the resourcing process had little insight into what other organizations were doing to provide New Jersey with the resources it needed to respond to the release of *Yersinia pestis*.

The lack of consistent information about resources and uncertainty among those supporting the resourcing process is problematic because:

- Decisions made under such conditions often do not account for key information or address relevant issues.
- Effective planning is dependent on maintaining situational awareness.
- Staff members have to take time to resolve the uncertainties and establish situational awareness.

The time they take to do so will reduce the time they can devote to other response activities, thereby delaying the deployment of needed resources.

2. Multiple Resource Processes Existed Not Coordinated

The T3 FSE resource request and coordination process was actually three separate processes:

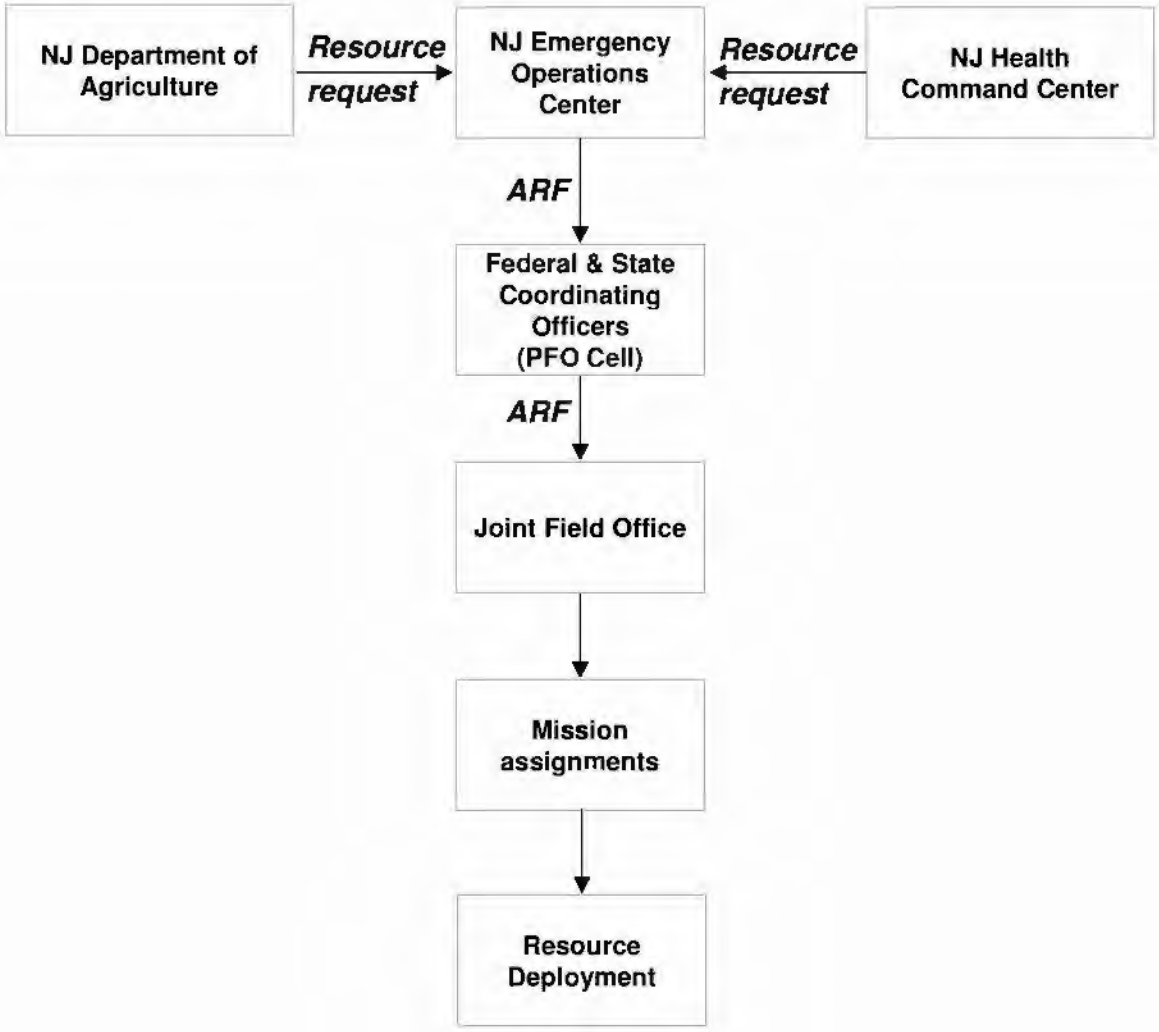
- the Stafford Act mission assignment process through the JFO;
- State requests for direct support made through the SERT (New Jersey) and the Unified Command Post (Connecticut); and
- direct support provided by the Federal government without requests from the State.

The process of requesting and coordinating resources broke down (e.g., many State ARFs were not resolved and organizations lost situational awareness) when these three processes became intertwined. In many instances, participants were not clear about which process they were supporting. The employment of all three processes in the T3 FSE hampered resource coordination. In both New Jersey and Connecticut, many resource requests were not addressed and State officials were not aware of assets sent to the States by the Federal government.

a. Resourcing Process #1: Mission Assignment Process

Figure III-1 depicts the New Jersey Stafford Act mission assignment process in which the State's requests for support were submitted to the JFO through the FCO, SCO, and JFO Operations Chief.

Figure III-1. JFO Mission Assignment Process in New Jersey[35]



The mission assignment process depicted in Figure III-1 was the primary mechanism used by New Jersey to request support from the Federal government. With the support of the ERT-A, which deployed to the State EOC, New Jersey officials submitted 43 ARFs through the mission assignment process. New Jersey's requests for support originated from the NJDHSS, New Jersey Department of Agriculture, or State EOC. Requests were submitted through the State EOC to the JFO. The State EOC submitted eight ARFs on behalf the NJDHSS and one on behalf of the NJ Department of Agriculture. The remaining 34 ARFs originated in the State EOC.

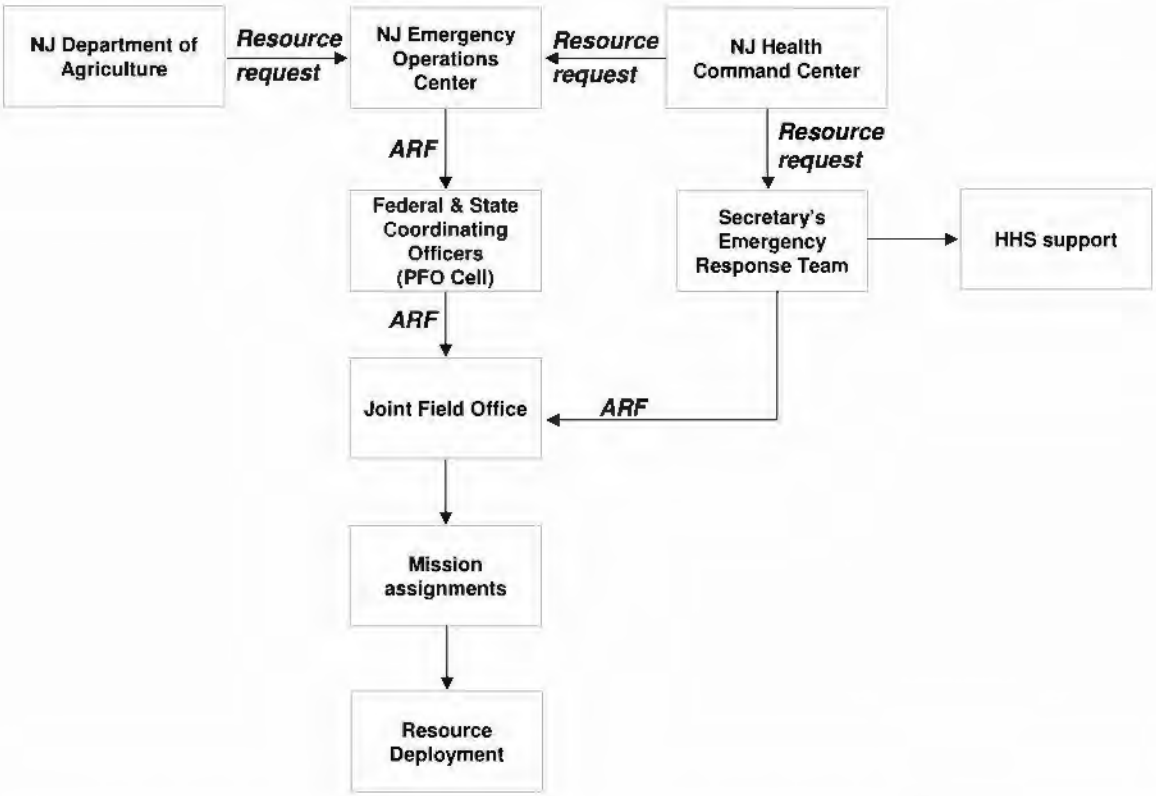
[35] A similar process existed in Connecticut.

b. Resourcing Process #2: SERT Process

The presence of the SERT affected the resourcing process in two ways. First, the SERT introduced another resource process, direct agency support. Second, its role in the overall resource process was unclear.

In the exercise, participants merged (albeit unintentionally) the direct support and mission assignment processes into a single resource request structure. Figure III-2 depicts the combination of the two processes with the new connections between the HHS, State Health Command Center, and the JFO.

Figure III-2. SERT Support for the Resource Request Process in New Jersey



The process depicted in Figure III-2 differs from the model mission assignment process depicted in Figure III-1. In the first structure, ARFs are typically assembled by a single State organization, such as the State EOC, passed to the Federal and State Coordinating Officers in the PFO Cell, and then forwarded to the JFO for mission assignments. The T3 FSE experience in New Jersey was different because two different State organizations—the EOC and HCC—submitted resource requests to two different Federal organizations (i.e., the JFO and SERT).

As depicted in Figure III-2, the SERT accepted resource requests from the State under the authority of the public health emergency declaration.[36] The SERT deployed to New Jersey to help State officials integrate available Federal medical resources into the State's response efforts. In this capacity, the SERT participated in both the mission assignment and direct support resource request processes. Examples of SERT support for the mission assignment process included helping to arrange the following assets for New Jersey:

- 250 ambulances;
- security for PODs through ESF #13;
- 100 refrigerated trucks; and
- NDMS counseling at the PODs.

The SERT also responded to direct requests from the NJ Department of Health and Senior Services to locate 12,000 medical professionals to support the State's acute care facilities. Supporting both processes simultaneously complicated tracking efforts and tended to blur the SERT's role in the response, rather than facilitate the flow of Federal support.

Participation by the SERT further complicated the New Jersey resource request process because the role of the SERT was not well-defined or understood by the participants. State officials had difficulty distinguishing the roles of the SERT and JFO. At times, the reaction of State officials was to work with both organizations, thereby increasing the likelihood that their request would be fulfilled. This method, however, made it difficult to coordinate the overall resource process.

Uncertainty over the role of the SERT was not limited to New Jersey officials. Near ENDEX, the SERT Operations Chief consulted with ESF #8 staff members in the JFO to resolve outstanding resource requests. The ESF #8 staff asked why the SERT was passing ARFs to ESF #8 to give to the JFO Operations Chief when it appeared to them that the support would be funded directly by HHS. It is not clear whether this exchange was the result of a misunderstanding between officials or a lack of familiarity with the process, but it suggests that the SERT's role in the Federal resource process had not been resolved during the exercise.

One potential concern is that the SERT duplicates the function of the JFO's ESF #8, which is responsible for supporting the mission assignment process. According to the NRP, ESF #8 "provides a mechanism for coordinated Federal assistance to supplement State … resources in response to public health and medical care needs." HHS defines a similar role for the SERT. The function of the SERT is "to provide assistance to State and local jurisdictions responding to public health emergencies."[37] The primary difference between ESF #8 and the SERT is that ESF #8 can task other Federal agencies to support the State's medical response. During the exercise,

---

[36] For more information about the T3 FSE declarations please refer to the "Integrating Responses to Incidents of National Significance" section of this report.

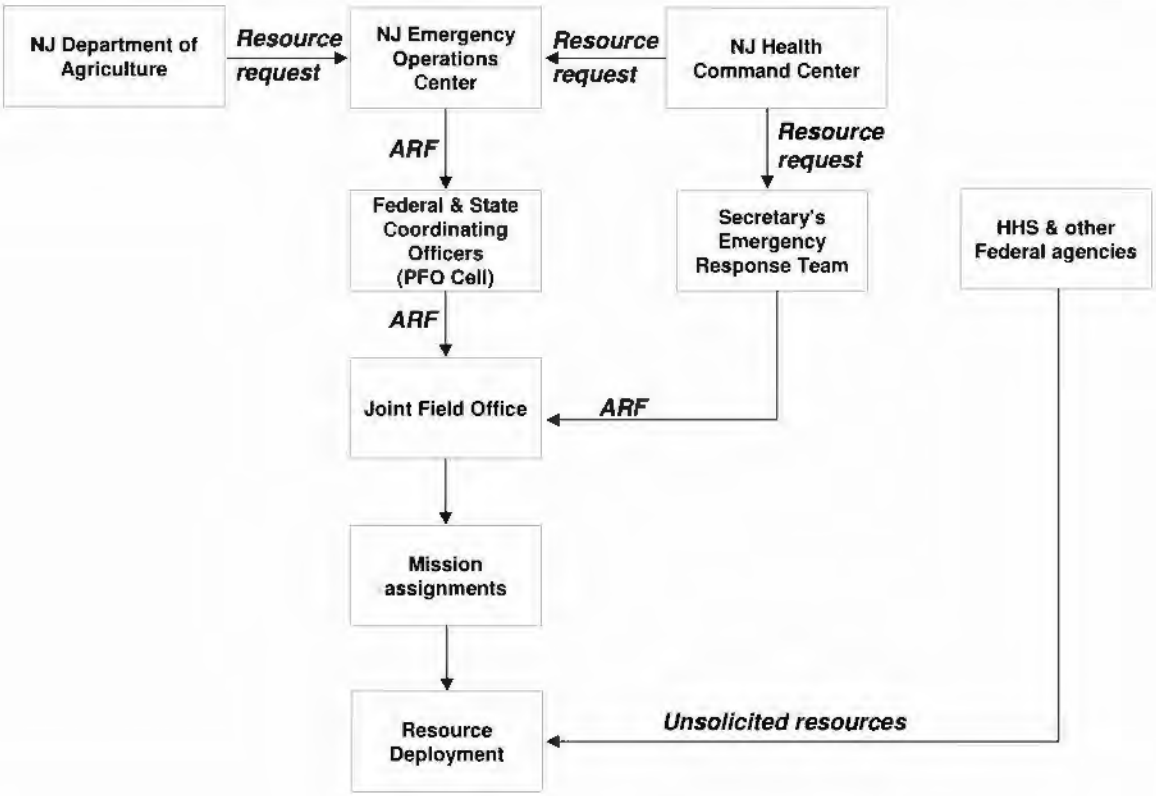
[37] www.hhs.gov/ophep/presentation/hauer3.html

SERT members helped to staff the ESF #8 in the JFO, further confusing their role in the resource request and coordination process.

c. Resourcing Process #3: Unsolicited Support (i.e., "Asset Push")

Unsolicited support from the Federal government was the third resource process observed in the T3 FSE that further complicated the resourcing efforts of officials in New Jersey and Connecticut. Figure III-3 depicts the deployment of these resources and completes the resource request and coordination process diagram for New Jersey.

Figure III-3. Complete Resource Request and Coordination Process for New Jersey



During the exercise, the Federal government "pushed" unsolicited resources to New Jersey, including:

- a 10,000 bed alternate care facility (ACF);
- two 250-bed DoD field hospitals;
- several Disaster Medical Assistance Teams;
- 30,000 remains pouches;
- Biological Emergency Support Team;
- 400 emergency medical technicians;
- 800 units of blood;
- 300 military police;
- field laboratory; and
- 20 chaplains.

The most notable of these resources was the 10,000-bed ACF. The States' experience with the ACF highlights the types of resourcing issues that can arise when unsolicited assets are unknowingly pushed to the States. HHS attempted to deploy the ACF to New Jersey without consulting State officials. When these officials learned about the deployment, they requested that the delivery be canceled. The next day, the New Jersey State Medical Director reversed the

earlier decision and requested that the SERT arrange the redeployment of the ACF. HHS also pushed an ACF to Connecticut and expected the logistics to be managed by the DPH ECC; however, Connecticut was not aware of the arriving ACF or the need to manage the logistics. HHS also determined that the facility would he staffed with several out-of-state DMATs, even as the State was trying to distribute these DMATs to various area hospitals. Neither ACF deployment was coordinated with State authorities. The deployment of unsolicited assets can be helpful, but their arrival can also surprise State officials, who must replan on short notice to incorporate the asset into the response.

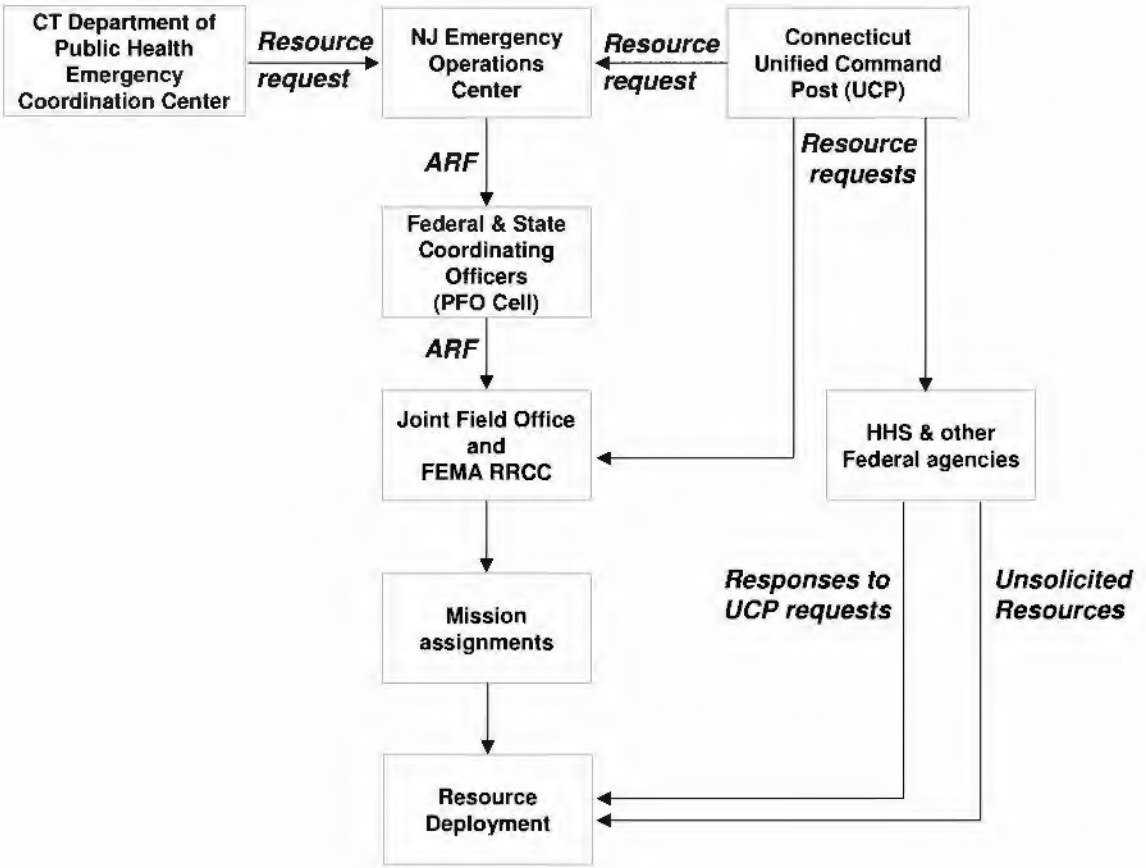
3. Resourcing in Connecticut

To this point, the resourcing analysis has focused on events in New Jersey; however, resourcing issues also existed in Connecticut. The resourcing structure in Connecticut was similar to the structure observed in New Jersey; in both States, there were three primary resource paths. The foremost difference between the two States was that in Connecticut, the Unified Command Post, rather than the SERT, provided another resource path in addition to the mission assignment and unsolicited support paths. Nevertheless, the result was the same: participants were uncertain about who had requested what.

In Connecticut, observations indicate that the UCP injected itself into the resource request and allocation process. After the transition from the ICP, representatives from the UCP began bypassing the State EOC. The UCP became an independent node in the Connecticut resource allocation process. Rather than submitting resource needs to the State EOC, the UCP assessed Connecticut's needs and submitted requests for support directly to organizations in the Federal government and other States.[38] Figure III-4 details the relationships among organizations participating in the Connecticut resource request and allocation process.

[38] Some of the requests sent by the UCP to the JFO were handled appropriately under the National Contingency Plan authority and under the NRP's Federal-to-Federal response mechanism (i.e., a fourth resource process). The addition of another resource request channel increased confusion among the participants.

Figure III-4. T3 FSE Connecticut Incident Management Structure



The UCP's participation (i.e., the addition of another node) in the resource request process made it difficult for participants to coordinate their activities. This structure did not facilitate the orderly exchange of requests because there was no mechanism (i.e., a gatekeeper) that could manage all requests, deconflict similar requests, and answer questions. Planners and decision makers had to rely on a patchwork of reports concerning resource requests.

The analysis of the resourcing process in New Jersey and Connecticut indicates that three different processes were used to provide Federal resources to the States and these processes were not well-coordinated. This lack of coordination helps to explain why key resourcing organizations, such as the New Jersey State EOC, IIMG, HHS, and the JFO, had such different resource pictures (refer to Table III-4). In both States, there was no mechanism that managed the flow of requests from the State and the flow of resources from the Federal government.

4. Implementation of Resourcing Processes by State and Federal Officials

Observations made during the exercise indicate that neither Federal nor State officials fully understood the processes for accessing Federal support. When documenting some requests, State officials either omitted key information or requested specific resources, rather than capabilities. Several requests were returned because the State was not familiar with the capabilities of the assets it was requesting. The processing of requests was also problematic and the outcomes of many New Jersey requests remain unresolved. In both States, there was uncertainty about who had asked for what. It is not clear whether the information was communicated to either system.

5. Problems with Request Documentation

Many resource requests were too specific and/or lacked important information. For example, Connecticut requested 3–5 refrigerated trucks to transport/store 100 bodies. Similarly, the Connecticut request for the Quick Reaction Force (QRF) stated a need for a "company size element of Federal troops numbering 100–120." The first request should have included the location(s) of the bodies requiring transport and their destination(s). As for the second request, an appropriate way to request the QRF would have been to describe the requirement to secure a nuclear power plant, rather than requesting a particular unit. The request should also have included details about the expected mission and its duration, which Connecticut did not specify. In several other requests, Connecticut stipulated the source of the asset (e.g., DMORT, DMAT, or DoD security) instead of asking for the type of assistance or capability required. Requests that lacked specifics included one that simply asked for an "additional quantity of supplies from HHS" and one for "mental health counselors, psychologists, and social workers to provide psychological aid in hospital emergency departments." Neither included details needed to fulfill the request, such as the types of medical supplies required, the number professionals needed, the locations, or the expected duration of the mission.

More than once, Connecticut asked for an asset without a good understanding of what capability came with it. In a discussion between the State EOC and JFO about the options for increasing the number of medical professionals, the State EOC had to ask what a DMAT could do. The response to a State request for DMORT to remove 100 dead bodies, 20 of which were contaminated, was that DMORTs do not handle contaminated bodies. Similarly, Connecticut's request for mortuary assistance included both DMORT and refrigerated trucks, although DMORTs hring their own temporary morgue facilities. A request to the National Guard for explosive ordnance disposal support was returned because the National Guard does not have this capability.

6. Officials Unfamiliar with the Processes

At times, State and Federal officials were also uncertain about how to process requests. Despite statements from the Connecticut EOC that all requests for Federal resources would be coordinated through the State EOC, confusion about how to access Federal assets persisted among State agencies. In a teleconference on April 4, a Connecticut Department of Public Health (DPH) representative in the State EOC called the DPH for clarification on how to request HHS

assistance. There was also evidence that Connecticut officials were unfamiliar with the ESF structure and to whom resource requests should be sent at the JFO. One data collector log noted that DPH staff members at the State EOC thought that ESF #8 (Public Health and Medical Services) was a form, rather than part of the JFO. This lack of familiarity may explain why requests were sent directly to different entities within the JFO and PFO cells. The same request for medical support was sent by the State EOC directly to a DoD representative (presumably at the JFO), another to the ESF #8 desk, and yet another to the PFO. In another example, requests were sent directly from representatives in the State EOC to the JFO without the knowledge of the Operations Chief within the State EOC. The result in Connecticut was uncertainty about who had asked for what.

Several of the requests submitted by State officials in Connecticut were not resolved during the exercise. During the T3 FSE, Connecticut officials submitted at least 12 requests, but mission assignments were issued for only 7 of these requests. The remaining 5 requests were unresolved. Table III-5 lists these 12 requests and the outcome of each request.

Table III-5. Matching Connecticut ARFs with JFO Mission Assignments

Resource Requested by State Using an ARF	Federal Action Taken
State DMAT	Asset provided
Federal DMAT	Asset provided
Medical Reserve Corps	Asset provided
Out-of-state hospital capacity	Asset provided
Nation-wide hospital capacity	Unresolved
Rapid Response Registry	Unresolved
Patient movement in-state	Unresolved
Patient movement out-of-state	Unresolved
Ventilators/dilators	Unresolved
Refrigerated trucks	Asset provided
DMORT	Asset provided
Federal Quick Reaction Force (QRF)	Asset provided

The number of unresolved requests in Connecticut suggests that the mission assignment process was not able to meet the needs of the State's response.

Uncertainty about the resourcing processes may help explain why a large number of State ARFs were not resolved during the exercise. In New Jersey, the State EOC submitted 43 ARFs, but 24

were not resolved during the exercise.[39] The JFO made nine mission assignments in response to the New Jersey ARFs. The remaining ten ARFs were canceled, rejected, superseded, or provided by National Disaster Medical System (i.e., outside the mission assignment process). The large number of unresolved resource requests noted in New Jersey indicates that the mission assignment process broke down during the exercise, leaving many State resource needs unmet.

Uncertainty about the resource request and coordination process may have caused officials in New Jersey to submit several ARFs requesting similar resources. It is unclear whether the State was requesting additional resources or simply updating earlier requests. For example, the State submitted three requests for mental health workers to support POD operations. In separate requests, the State requested 2,000, 1,500, and 500 crisis counselors. From these ARFs, it is not clear how many mental health workers the State was requesting. A similar problem arose over POD security. The State submitted six different ARFs requesting POD security. At various times during the exercise, the State requested:

- armed security for the PODs (n = 1,826);
- POD security (n = 2,350);
- POD security (n = 4,000);
- POD security (10 per POD, n = 1,680);
- POD security (20 per POD); and
- security to protect the State's 200 PODs (n = 4,000).

It is unclear exactly how many POD security personnel the State was requesting. The numerous submissions also made it difficult to discuss security resources because, among staff members, it was difficult to discern which requests were being discussed.

Uncertainty about the process was not limited to State officials. In Connecticut, the Operations Chief in the JFO expressed concern that ESF #8 was processing requests made directly to them by the State EOC at the same time that the JFO Operations Branch was processing the same requests. This led to a discussion about procedures and the pronouncement that all requests should be formally made through the FCO.

As in Connecticut, officials in New Jersey were not familiar with the resource request and allocation process. The observations summarized in Table III-6 indicate that staffs at Federal sites in New Jersey encountered problems with the resourcing process.

[39]The daily distribution of ARFs submitted to the New Jersey JFO was: April 4 = 1, April 5 = 4, April 6 = 18 , April 7 = 17, April 8 = 0, and Unknown = 3 .

Table III-6. Resource Request and Allocation Process Issues at Federal Sites in New Jersey

Time/date	Location	Data Collector Observations
23:58 April 4	ERT-A	The DMORT request is halted, because the SERT thought that the request had to be vetted through HHS. Later clarified that the DMORT is a FEMA asset.
17:50 April 5	RRCC	The Operations Chief requests that ESF #8 find out what they are doing under HHS funding and what is being done under Stafford Act.
22:20 April 5	RRCC	There is a disconnect between what is being conducted in the ESFs and what the RRCC Director and Operations Chief are aware of.
06:30 April 6	JFO	It does not seem that anyone in this section knows the correct way to submit properly filled out ARFs.
13:45 April 6	JFO	The JFO was trying to figure out how an ARF was submitted and approved for the 10,000 bed facility without consulting the State or FEMA. The SERT indicated that HHS requested the facility for New Jersey.
16:10 April 6	JFO	The Mission Assignment staff wants to know the origin of the request for the Army Corps of Engineers to provide power and shelter for citizens.
17:30 April 6	JFO	The Operations Chief is requesting from all Branch Chiefs and ESFs what the latest information is on all mission assignment—wants status on all.
18:30 April 6	JFO	It does not appear that anyone in this section knows the process for completing and submitting ARFs.
09:30 April 7	JFO	ESF #7 is being directly tasked by FEMA Headquarters without going through the FCO.
16:00 April 7	JFO	The JFO staff does not know how HHS fits into the resource allocation process. The ARF/MA process is broken.
17:45 April 7	JFO/SERT	SERT Operations Chief comes into JFO and introduces himself to the JFO Operations Chief. SERT Operations Chief asks how exactly they can get the items they need.
17:50 April 7	JFO/SERT	ESF #8 staff consulted with SERT Captain regarding why mission assignments are coming from the SERT if HHS is directly funding these resources. It appears that the SERT is submitting ARFs to ESF #8 to pass to the JFO Operations Chief for items that have already been completed using HHS resources. The JFO wants to understand why the SERT is using a FEMA process—confusing.
08:00 April 8	JFO	JFO Operations Chief is discussing how to clarify the process of receiving ARFs and entering them into a tracking log.

The observations in Table III-6 indicate that personnel from the RRCC, JFO, and SERT were confused by the operation of multiple, overlapping resourcing processes. This lack of familiarity is problematic because these personnel are expected to manage the Federal resource process in the State. This lack of familiarity with the mission assignment process may explain why so many State requests were unresolved at the end of the exercise.

7. Information about Resourcing Process Not Readily Available

Throughout the exercise, participants from both State and Federal agencies did not have access to current information about the status of resource requests or about the deployment of unsolicited assets. Information that was available about what had been requested, the status of these requests, and the arrival of Federal resources was often incomplete and outdated. This lack of transparency (e.g., the ability to track a request from submission through delivery) made it difficult for State and Federal officials to access information about:

- which resources had been requested and by whom;
- the status of the requests (e.g., received and under review);
- the outcomes of these requests (e.g., denied, approved, or modified); and
- the status of the resource (e.g., mobilizing, en route, or arrived).

Without access to reliable information, response planners and decision makers lacked a key element of situational awareness. For example, the reconstruction of the T3 FSE events indicates that the New Jersey PFO Cell was not aware of many New Jersey resource requests. At a 1500 briefing on April 6, the PFO Cell reviewed the status of resource request submitted by the State. In this meeting, the PFO Cell noted that New Jersey had requested:

- SNS support;
- DMAT;
- DMORT;
- NDMS MST; and
- DPMU.

The PFO Cell's list of requests differs from the list of submitted ARFs provided by the New Jersey State EOC. A review of the State EOC ARFs submitted by 1200 on April 6 indicates that in addition to the items listed above, the New Jersey EOC had submitted additional ARFs for the following:

- VMAT;
- 80–100 epidemiological investigators;
- 12,000 medical personnel to support acute care facilities; and
- 8 pathologists.

Such differences suggest that reliable information about State resource requests was not readily available to officials in New Jersey. Similar issues were observed in the New Jersey JFO Cell. Data collectors noted resource request confusion on at least eight occasions. In Table III-7, several examples of this confusion are provided.

Table III-7. Confusion Regarding New Jersey Resource Requests

Time/Date	Data Collector Observations
04:03/April 7	There are ten ARFs being played by the DCO with no play from the ESFs. There is confusion over who is doing these ARFs. Nothing has been passed to the Operations Chief about who is handling them.
04:06/April 7	There are questions regarding who is responsible for purchasing the 100 refrigerated trailers.
04:50/April 7	The JFO Operations Chief and the Deputy Federal Coordinating Officer were trying to resolve who is in charge of the CDC Vector Control Team and who is paying for them.
07:00/April 7	The State is sending duplicate ARFs to the JFO forcing the Operations Chief to sort through them to identify those ARFs that are already in process.
08:00/April 7	The Operations log indicates that new ARFs came in during the night shift, but many are duplicates and some have been returned to be reworked.
19:15/April 7	NJ EOC had to resubmit an ARF for a VMAT because the first had been lost.
April 7	ARFs went directly to the ESFs.
08:00/April 8	Several (9) ARFs received at the JFO during the night shift are unassigned. The JFO is still receiving duplicate requests.

A lack of understanding about what had been requested at the JFO Cell is particularly troublesome because managing the resource allocation process is the primary function of the JFO.

Similar issues existed in Connecticut. At the operational level, officials realized that information about resource requests had not been adequately maintained and were not readily available. For example, the Logistics Chief at the RRCC remarked to the Operations Chief that it was unclear to him what, if anything, had been done on State resource requests. State officials echoed these sentiments. The Operations Chief at the State EOC commented that he never knew if or when requests were addressed by Federal authorities. The State Logistics Chief added that he could not distinguish new requests from clarifications of previous requests.

Such observations suggest that information about resource requests and deployment was not readily available to officials in New Jersey and Connecticut.

8. Issues from Previous Exercises

Many of the same issues observed during T2 regarding the resourcing process recurred during the T3 FSE. In at least one area, the issue may have worsened. In the T3 FSE, information about the process of requesting resources was not documented in the National Response Plan (NRP). The document that preceded the NRP and was in use during T2, the Federal Response Plan, included a thorough description of the process.

In Table III-8, a comparison of the T3 FSE resourcing process with the T2 experience is provided.

Table III-8. Comparison of T3 FSE with Previous Exercises

T2 FSE	T3 FSE
ISSUES/OBSERVATIONS	
• **Considerable uncertainty existed at the local and State levels about available Federal assets and the processes for obtaining them.** *States often requested specific assets—sometimes requesting inappropriate or unnecessary assets by error.* *States appeared not to be aware of the range of Federal resources potentially available.*	• **State and Federal officials struggled with the implementation of the Federal resourcing process.**
• **State and local agencies requested resources through a number of different channels directly from the Federal departments/agencies and also through the FEMA mission assignment process.** *Direct requests for Federal assistance occurred before Stafford Act declarations (e.g. Washington State requested assistance from DOE in response to the RDD atteck).*	• **The use of multiple resource processes created uncertainty and adversely affected situational awareness.**
• **A complete and consistent source of information about deployed Federal assets was not available.**	• **Information about the status of resources was not readily available and the process lacked transparency.**
	• **The role of the HHS SERT was not well-defined or understood by participants. At times the SERT duplicated functions performed by ESF #8 in the JFO.**

The comparison of the T2 and T3 experiences suggests that there has been little improvement in the process of matching State needs with Federal assets.

E. Conclusion

During the T3 FSE, officials in New Jersey and Connecticut requested Federal support; however the resource request process used in this exercise was problematic. At least three different resource processes were used during the exercise and the activities of those supporting each one were not well-coordinated. Officials struggled with implementing the process, many requests were unresolved, and information about the status of requests was not available. Additionally, the role of the HHS SERT was not well-defined or understood by the participants. Together, these factors adversely affected the ability of State and Federal officials to match State needs with available Federal assets. Resolving these issues would clarify the process and strengthen the ability of Federal and State agencies to respond to a major disaster.

The use of multiple resource processes created uncertainty and adversely affected situational awareness. State and Federal efforts would likely benefit from a simplified resourcing process. Developing a unified Federal emergency resourcing process would likely address many of the coordination and situational awareness issues observed during the T3 FSE.

State officials struggled with the implementation of the Federal resourcing process. Integrating a team familiar with the Federal resource allocation process into a State EOC would likely improve the State's ability to access the Federal resources it needs. Such an organization (e.g., ERT-A) already exists, but its impact on the T3 FSE resource process is unclear. The ERT-A is a deployable FEMA organization familiar with JFO operations. In New Jersey, the ERT-A deployed to the State EOC. In Connecticut, the ERT-A deployed to the JFO. The analysis of the T3 FSE observations indicates that officials in both venues struggled with the resource request process. It is not clear that the ERT-A in New Jersey improved the State's ability to access Federal resources. One difference between the two venues is that New Jersey submitted 43 ARFs and Connecticut submitted 12; however, this difference could be caused by a number of factors and exercise artificialities. Nevertheless, observations from the T3 FSE indicate that States require substantial support and guidance on the Federal resource request process.

Information about the resource process(es) was not readily available. Both State and Federal officials would benefit from readily available and clear documentation on the mission assignment process. Although the NRP makes numerous references to the mission assignment process, few, if any, details of the process are provided in the document. Without guidance from the NRP, State and Federal officials must locate other sources of information about how the Federal government provides disaster assistance to States. During such emergencies, officials have little time to thoroughly research the process. In the T3 FSE, State and Federal officials learned about the process while attempting to engage and/or implement it.

The documentation that describes the mission assignment process should be crafted so that even those officials with limited exposure to the process and little time to learn can successfully participate. The information should be clear and concise. Although Federal officials may have many opportunities to participate in and learn about the mission assignment process, State officials will likely have far fewer opportunities to do so.

The role of the HHS SERT was not well-defined or understood by the participants. In the T3 FSE, the HHS Secretary activated the SERT in both New Jersey and Connecticut, despite the fact that a public health emergency was declared only in New Jersey. Observations from New Jersey indicate that its presence adversely affected the resourcing process.

There are at least two alternative roles that the SERT could fulfill during a crisis that involved multiple Federal agencies: augment the ESF #8 or deploy to the State's Department of Health.

The T3 FSE analysis indicates that in situations in which the Stafford Act mission assignment process is being used, both ESF #8 and the SERT do not need to be present because they performed nearly identical functions in the exercise (i.e., coordinate Federal medical resources). This conclusion suggests that when the JFO stands-up and ESF 8 activates, the SERT should either augment the ESF #8 staff or not deploy to the JFO. This approach would benefit the resource allocation process by:

- clarifying the process for accessing Federal resources;
- reducing coordination requirements (one less node in the resource request structure); and
- infusing ESF #8 with an experienced staff of subject matter experts.

The T3 FSE experience indicates that maintaining the SERT and ESF #8 as separate entities, as they were in the T3 FSE, will preserve a source of confusion that will adversely affect the State's ability to access Federal resources during a major disaster.

A second alternative to deploying with the JFO would he for the SERT to deploy to the State's Department of Health or other location at which the SERT could provide subject matter expertise needed for the response, including expertise about Federal medical resources, and advise the State health officials how to request those assets. Such a mission would require the SERT staff to become more familiar with the Federal resourcing process.

Access to information about the status of resources would help the State plan their response; however, such access was not available during the T3 FSE. Througbout the exercise, both Federal and State officials asked a version of the same question over and over again: What is the status of the State's resource requests? Many of those participating in tbe response had little insight into the process and were not notified when a request was received, approved, denied, or modified. The lack of access to the status of resource requests limited the ability of response organizations to incorporate Federal resources into their response plans.

During the exercise, the JFO maintained at least two logs of mission assignments, but it is not clear the extent to which State officials had access to either log. There are no observations indicating that State officials had access to or used either log. Even if they did, the logs are incomplete; several State requests do not appear in either log. State officials also did not have access to information about the deployment of unsolicited resources from the Federal government.

Access to information about the status of resources requests and the deployment of all resources is an essential element of situational awareness among State and Federal officials during major disasters. During tbe exercise, these officials devoted large amounts of time and effort to the resourcing process. Documenting this process and its results during the T3 FSE would have contributed important information to the participants' situational awareness.

Providing the information needed to support resource allocation awareness does not require an extensive infrastructure or an elahorate process. A readily available, authoritative spreadsheet containing a few pieces of information (e.g., a description of the requested/deployed resources, a

JFO point of contact, and the status of the request) would provide officials with significant situational awareness. Once again, a simple process and an accessible mechanism for sharing information would be sufficient. For example, the JFO could attach the resource request spreadsheet to a regular update that it e-mails to a large number of State and Federal officials. This authoritative update would become the basis for situational awareness about the resourcing process. Such a simple solution is more likely to be used by State officials who may have few opportunities to learn about the Federal resourcing process and the information sharing mechanism.

1. Recommended Courses of Action

- Develop a unified Federal emergency resourcing process that supports resource requests from the State under the Stafford Act and resource requests for Federal-to-Federal support under other Federal authorities. Include a description of how resource request/status information will flow between the Incident Command Post(s) and the JFO.
- Provide States with a team of subject matter experts, who are knowledgeable on Federal capabilities and the resource requesting process itself.
- Document the mission assignment process more thoroughly in the NRP.
- Clarify the role of the SERT during emergencies. Consider using the SERT to augment ESF #8 at the JFO or deploying it to the State Department of Health to provide subject matter expertise in identifying and requesting Federal medical support.
- Make information about resource requests readily available, including what resources or capabilities were requested, who made the request, how the request is being funded, and its current status.

IV. Information Sharing

A. Introduction

Accurate and timely sharing of information and the development of a common operational picture are critical for the success of an integrated Federal, State, and local response to domestic emergencies. Despite efforts to improve communications and information sharing across response organizations, the lack of shared situational awareness and the dissemination of incorrect information remain significant roadblocks to a coordinated emergency response, as evidenced by experiences in the T3 FSE.

Previous sections of the AAR touched on information sharing and coordination problems associated with resource requesting and coordination,[40] agent identification,[41] status of advisory levels,[42] and integration of operating centers into the response,[43] among others. The following discussion focuses on some additional examples of inadequate information sharing that affected T3 operations from the tactical to the strategic levels of the response, and then proposes some broad explanations as to why communications broke down in these and other cases.

Analysis of information sharing in T3 suggests a number of contributing factors to the information sharing problems observed during the exercise, including:

- proliferation of stovepiped electronic information systems;
- presence of many nodes in the response network;
- lack of formal information flow processes and the use of alternative channels; and
- lack of uniform reporting guidelines and estahlished procedures for validating information to build shared situational awareness and a common operating picture (COP).

SUMMARY OF CONCLUSIONS: INFORMATION SHARING IN THE T3 FSE

- Information systems used in T3 were largely stovepiped within agencies and/or response communities.
- The vast number of operating centers activated during T3 negatively affected information sharing by increasing the scope and complexity of the problem.
- The use of informal or alternate channels for sharing information caused problems by enabling circular reporting and bypassing authoritative sources.
- The T3 FSE revealed a lack of uniform reporting guidelines and procedures for validating information received from secondary or tertiary sources.
- Agencies and operating centers acted and made decisions on different information
- Situational awareness was not effectively shared across operating centers and agencies.

The result of information sharing problems in the T3 FSE was that shared situational awareness was not achieved nor was a COP developed and effectively shared across the response network. Instead, agencies and operating centers in T3 were often making decisions and acting on different information.

B. Background

Shared situational awareness is the synthesis of information across organizations or among individuals used to generate a common bank of knowledge about an incident or situation. The concept of shared situational awareness does not necessarily imply perfect information, though that is the goal, but rather common information, be it good or bad, shared by all persons or

[40] See discussion in "Resource Requesting and Resource Coordination."

[41] See discussion in "Agent Confirmation and Hazard Area Determination."

[42] See discussion in "Homeland Security Advisory System."

[43] See discussion in "Joint Field Operations."

organizations. Part of shared situational awareness is building a COP. Most definitions of a COP imply a physical or technological display of information accessible by all the parties. This picture facilitates collaborative planning by visually presenting information relevant to achieve shared situational awareness. Key to developing a COP and shared situational awareness is an understanding of an incident's or operation's essential elements of information (EEIs), or the significant pieces of information that need to be shared. Some EEIs can only be tracked with words, not pictures.

Casualty figures and the means by which contaminating agents were disseminated are EEIs in an emergency response. These data drive decision making at multiple levels and across different communities.

- The numbers of persons injured, sick, and dead are used for predicting resource requirements including hospital beds, ventilators, and mortuary services; for supporting any epidemiological investigations; for determining prophylaxis requirements; and for framing Federal support to a region, State, or locality.
- Information on a contaminating agent and how it was released is used for supporting the criminal investigation, for predicting the spread of contamination, for assessing remediation requirements, and for determining public safety measures.

In a domestic emergency response operation, operating centers and agencies at the local, State, and Federal level develop their own situational awareness of the incident, and then strive throughout to align their knowledge with that held by other centers or agencies. In other words, they create their own operational picture, then constantly update and validate it with information gleaned from other responders, thereby building a COP. The NRP identifies the Homeland Security Operations Center (HSOC) as the national hub for information sharing and tasks that center with maintaining situational awareness.

C. Reconstruction

During the T3 FSE, Operations Centers across the response network frequently held contradictory information about casualty figures and the means by which terrorists released the mustard agent in Connecticut.

1. Victim Numbers

The first casualties from the T3 FSE terrorist attacks appeared in New Jersey at 08:00 on Monday, April 4, when three victims were admitted to hospitals in Union and Middlesex Counties, New Jersey. Showing flu-like symptoms and coughing up blood, these victims marked the first of many casualties from the overnight release of *Yersinia pestis* along the State's highways. Using a credible epidemiologic model, T3 planners were able to project the numbers of plague casualties both temporally and geographically. According to the model, by the end of the first day, over 900 people were sick and another 900 dead from pneumonic plague. Within

four days, over 60,000 State residents were sick, and 9,500 people were dead. Table IV-1 shows the ground truth numbers of plague deaths between April 4 and 8.

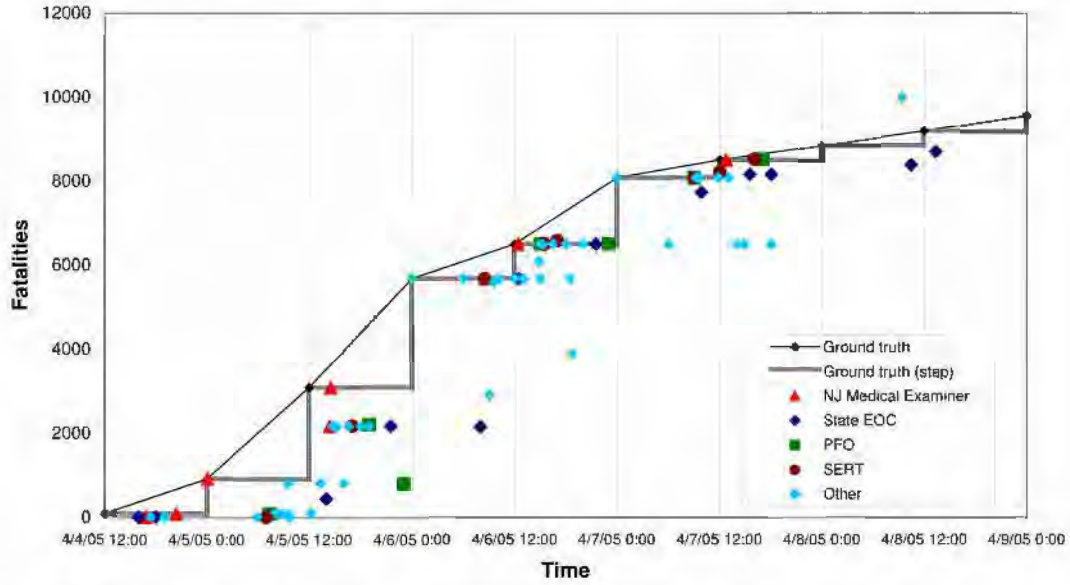
Table IV-1. Persons Dead from Plague in New Jersey (Ground Truth)[44]

Date and Time	Total Dead (Cumulative)
Monday, April 4, Noon	92
Monday, April 4, Midnight	909
Tuesday, April 5, Noon	3,077
Tuesday, April 5, Midnight	5,692
Wednesday, April 6, Noon	6,509
Wednesday, April 6, Midnight	8,071
Thursday, April 7, Noon	8,490
Thursday, April 7, Midnight	8,839
Friday, April 8, Noon	9,181
Friday, April 8, Midnight	9,554

Figure IV-1 shows the number of fatalities that were reported by various sources in New Jersey, the Federal government, and the media compared to the ground truth as injected by exercise control based on the epidemiological modeling.

[44] Note that the dates and times are based on planned injects by exercise control. Data is insufficient to prove whether injects occurred precisely as planned.

Figure IV-1. Fatalities from Plague in New Jersey



In the chart, the black line bounding the data-points corresponds to the ground truth as injected by the controllers. The gray stair-step line corresponds to what the ground truth would appear to be with numbers injected in 12-hour intervals, as they were once hospital play concluded prior to midnight on April 4. The points on the chart that are not in agreement with the ground truth fall into two main categories—"late" and "other."

The late points are those that match injected ground truth fatality numbers, but were reported after new injects. On the chart, the late points fall on a line horizontal to the inject, but after a stair-step riser indicating a new inject. For example, there are at least eight points that correspond to the 6,508 fatality deaths injected at 12:00 on April 6. These eight points fall on a horizontal leg of the ground truth stair-step line, to the right of the 4/6/05 12:00 and 6,508 point; therefore, these reports were timely and accurate, falling as they do before new numbers were injected into play. The chart shows, however, that there were four more reports of 6,508 deaths, by the FEMA ERT, the CDC, and DHS, all of whom were reporting or working from out-of-date information. Data points that fall under the "other" descriptor are those that do not align with any ground truth data on a horizontal access.

Figure IV-1 indicates that the lack of a common and accurate fatality count in New Jersey was largely an issue of late reporting. Except for a few instances, agencies and operating centers appeared to report fatality numbers that aligned with figures that were, at the very least, accurate at some point during the exercise, if not at the moment they were reported. This suggests a problem with keeping all operating centers and agencies updated with new information.

Victims of the terrorist attack in Connecticut included persons injured or killed in the truck bombing on the New London City Pier and those contaminated by mustard dispersed from an

airplane prior to the explosion. Over 100 people were killed and another 300 wounded in the bombing. The mustard attack resulted in the hospitalization of over 5,600 people, with close to 50,000 more filling hospital waiting rooms fearing they had been contaminated. Table IV-2 shows the ground truth numbers of people hospitalized for mustard exposure as a result of the Connecticut attack.

Table IV-2. Victims Hospitalized in Connecticut (Ground Truth)[45]

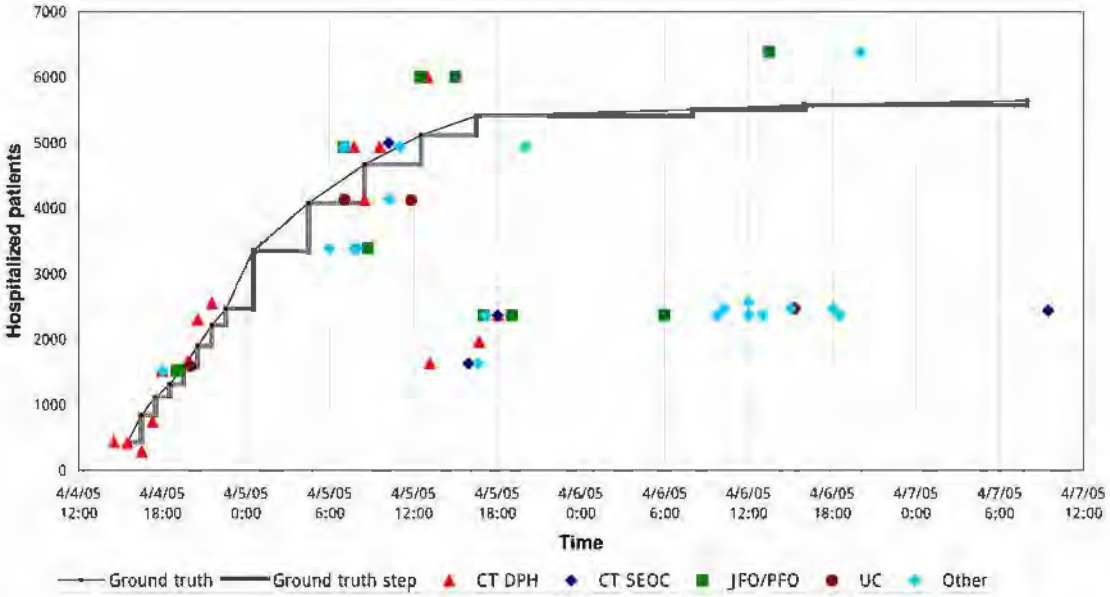
Date and Time	Total Hospitalized (Cumulative)
Monday, April 4, 15:30	429
Monday, April 4, 16:30	835
Monday, April 4, 17:30	1,119
Monday, April 4, 18:30	1,327
Monday, April 4, 19:30	1,587
Monday, April 4, 20:30	1,906
Monday, April 4, 21:30	2,220
Monday, April 4, 22:30	2,469
Tuesday, April 5, 00:30	3,351
Tuesday, April 5, 04:30	4,086
Tuesday, April 5, 08:30	4,674
Tuesday, April 5, 12:30	5,115
Tuesday, April 5, 16:30	5,409
Wednesday, April 6, 08:00	5,508
Wednesday, April 6, 16:00	5,579
Thursday, April 7, 08:00	5,644

Figure IV-2 shows the number of victims hospitalized for mustard exposure as reported by various sources in Connecticut, the Federal government, and the media, compared to the ground

[45] Note that the dates and times are based on planned injects by exercise control. Data are insufficient to prove whether injects occurred precisely as planned.

truth as injected by exercise control. In the Connecticut portion of the T3 FSE, new casualty numbers were not injected in a consistent pattern as they were in New Jersey.

Figure IV-2. Victims Hospitalized for Mustard Exposure in Connecticut



The reported hospitalization numbers from Connecticut show more discrepancies across reporting agencies and as compared to the ground truth than did the New Jersey fatality data. Few of the differences in casualty reporting in Connecticut appear to be attributable to late reports. Instead, the reported hospitalization numbers are widely dispersed across time and operating centers.

2. Agent Release

The terrorists used two methods to disseminate the mustard agent in Connecticut. First, at approximately 11:20 on April 4, a small aircraft flew over the New London City Pier on the Thames River releasing mustard over the waterfront area. Roughly two hours later, at 13:20, a vehicle-borne improvised explosive device (VBIED), hidden in the back of a truck that also carried mustard, detonated at the head of the pier. Most of the mustard agent present in the truck bomb was destroyed during the explosion, limiting contamination to the immediate vicinity of the detonation, where a pool of mustard had collected prior to the explosion. The aircraft release contaminated a much larger area and had a greater impact on the people attending the festival at the pier.

First responders and hazardous material specialists at the incident site quickly recognized that victims were showing symptoms beyond those expected after a bombing. Most responders assumed that the truck itself was responsible for the contamination. The investigation into the

attack in Connecticut progressed rapidly. Interviews with victims revealed that most reported feeling ill prior to the explosion and remembered seeing a low flying aircraft leaking an unknown substance over the pier roughly two hours before the bombing. This led the FBI to investigate five small aircraft matching witness descriptions that were reportedly in the area on April 4. Over the course of a few hours, law enforcement personnel had contacted and interviewed the owners or pilots of all but one of the aircraft, a Beechcraft Baron 58, owned by three individuals as part of a timeshare. At 14:20, the FBI was advised that an airplane matching that description had landed at a private airstrip in Millbridge, Maine, under suspicious circumstances and with a steel drum inside. At 15:35, the senior investigator at the Connecticut JOC sent agents to Maine to investigate the aircraft. The search of the aircraft began at 17:00, and by 17:13, investigators had located the steel drum and were testing it and the aircraft for signs of mustard. At 22:00, the FBI Senior Agent in Charge (SAC) informed the Primary Federal Official (PFO) and the other members of the JFO Coordination Group that initial tests on the aircraft were positive for mustard, but that definitive confirmation would not be available until the next morning. At 10:00 on April 5, the Connecticut JOC informed the FBI's Strategic Intelligence Operations Center (SIOC) that test results on the aircraft were positive for mustard. The confirmation was briefed within the JOC at 12:00 and posted to the Law Enforcement Online (LEO) system at 14:05.

Unaware of the FBI's investigation into the suspicious aircraft, other agencies hypothesized about the means of dispersal. At 18:08 on April 4, the Connecticut Department of Public Health (DPH) and the treating hospitals reasoned that the timetable in which victims became symptomatic was too quick for the mustard to have been released in the explosion, suggesting the agent was released prior to the explosion (or was not mustard). The next morning, at 06:20, a representative from the Connecticut DPH also expressed skepticism that the ten-gallon container discovered in the debris from the truck bomb could produce the number of casualties being seen at area hospitals. Representatives from the Environmental Protection Agency (EPA), located at the JFO, considered that a blast strong enough to destroy a five-story building would likely have destroyed any mustard present. The Interagency Modeling and Analysis Center (IMAAC) determined from the initial set of field measurements, injected at 19:30 on April 4, that the bulk of the contaminant had to have been released from an airplane; this scientific conclusion was included in Set 4 of the IMAAC products, released at 23:50 on April 4.

Despite these hypotheses, scientific evidence, and the FBI's ongoing investigation, between 03:00 on April 5, and the conclusion of the T3 FSE on April 7, numerous agencies and operating centers incorrectly reported or believed that the aircraft found in Maine had tested negative for mustard and was likely not responsible for the chemical release over the New London City Pier.[46] Table IV-3 identifies the agencies, their incorrect assumptions, and when they were corrected relative to the 10:00 confirmation that the aircraft was positive for mustard.

---

[46] Data suggest that the initial genesis of the incorrect information about the aircraft was the result of controller error. However, the spread of bad information and the inability of operating centers and agencies to successfully correct the mistake across the response network are worth analyzing.

Table IV-3. Misinformation about the Aircraft that Released Mustard

Agency/ Operating Center	Time of Incorrect Assumption	Incorrect Information	Time When Corrected	Time Since FBI Confirmed Mustard on Aircraft
CT PFO/ JFO CG	April 5, 03:00	FBI Boston examined aircraft in Maine and determined it was only equipped with normal crop dusting equipment, and that all other forensic tests yielded negative results	April 5, 11:50[47]	1 hr, 50 min
UCP	April 5, 04:09	Airplane in Maine was a red herring	April 5, 13:05	3 hrs, 5 min
USCG	April 5, 04:18	FBI reported the inspection of the aircraft resulted in no evidence of mustard	April 5, 16:17	6 hrs, 17 min
IIMG (DHS S&T)	April 5, 07:28	FBI reported positive identification of mustard on the ground in Connecticut but only precursors on the aircraft. Instructed the IMAAC to ignore the aircraft and focus on the truck as the source of the mustard.	April 5, 14:22	4 hrs, 22 min
CT DEP	April 5, 09:45	Local FBI determined the aircraft was a false lead. Requested IMAAC plume analysis for truck-based release.	April 5, 10:53	53 min
HSOC	April 5, 10:27	A drum in the aircraft tested positive for HD. However, on further examination it was determined that the aircraft was only equipped with normal crop dusting equipment. All other forensic examinations yielded negative results.	April 5, 14:22	4 hrs, 22 min
TSA	April 5, 15:00	FBI analysis of the drum on the aircraft in Maine yielded no trace of mustard. *(as reported in DHS/PFO SITREP)*[48]	Unknown	
FEMA RRCC	April 6, 09:00	Vehicle bomb appears to be primary dissemination device.	Unknown	
OSHA	April 6, 15:00	Mustard disposition assumptions not established. *(as reported in DHS/PFO SITREP)*	Unknown	

[47] Despite data indicating the JFO Coordination Group was told at 11:50 on April 5, that the aircraft tested definitively for mustard, members continued to question the validity of that information through the end of the exercise.

[48] The 15:00 SITREP from the Connecticut DHS/PFO contained contradictory information, with the TSA section reporting the aircraft yielded no trace of mustard and the FBI section reporting the aircraft tested positive for mustard.

D. Analysis

Shared situational awareness is essential for the successful integration of Federal, State, and local operations during an emergency response. The T3 FSE demonstrated examples of both successful and less than successful information movement and coordination, many of which are described throughout this AAR. To improve on integrated responses to national emergencies, it is important to understand what does and does not work in terms of information flow, where information sharing tends to break down, and what actions or events influence the information sharing processes.

Analysis of information sharing in T3, particularly the movement of casualty figures and the flow of information about the mechanisms used by the terrorists to disperse the contaminating agents, suggest a number of contributing factors to the difficulties observed, including:

- proliferation of stovepiped electronic information systems;
- vast number of nodes in the response network;
- lack of formal information flow processes and the use of alternative channels; and
- lack of uniform reporting guidelines and established procedures for validating information to build shared situational awareness and a COP.

1. Proliferation of Stovepiped Electronic Information Systems

The purpose of an electronic information system is to facilitate the exchange of information among a select group of individuals. In T3, the audience for different information systems ranged from the very narrow—a single agency—to the very broad—multiple operating centers staffed by different agencies and physically located in three separate countries.

During the exercise, participants were observed using a number of different information systems. In some cases, the participants used secure intranets. In others, they used public websites to share information. T3 responders in New Jersey, Connecticut, at the interagency level, and in Canada and the United Kingdom used the following patchwork of information systems to disseminate time-critical information, pass requests for support, task issues, respond to requests for information, and log events:

- Communicable Disease Reporting System (CDRS). CDRS is an interactive web-based information management application that tracks communicable disease data. With these data, public health officials can generate reports and monitor trends in the spread of a disease. Plague patient data was entered into the NJ CDRS throughout the exercise.[49]
- E-Team. E-Team is a commercial off-the-shelf (COTS) crisis management application that provides personnel with the ability to exchange information, manage resources, track

[49] See http://sph.umdnj.edu/campus/Dviriglio.pdf

requests, log events, and monitor deployments.[50] During T3, the New Jersey State EOC relied on E-Team to support its response to the T3 scenario, whereas HHS used it to support its internal information management.

- Health Operations Tracking System (HOTS). HOTS is an application used to document health-related incidents in New Jersey.[51] During T3, New Jersey State and county health officials used HOTS to exchange information about the spread of plague and the State's response to the emergency. For example, the Health Command Center used HOTS to log significant events as they occurred. County officials used HOTS to request medical resources through their county OEM.
- Homeland Security Information Network (HSIN) International. HSIN International is a secure website that allows DHS representatives in U.S. embassies to exchange information with the HSOC via event logs, SITREPs, and chat sessions. During T3, it connected DHS representatives in the United Kingdom and Canada with Federal operations and information in the HSOC.
- Information Control System (ICON). ICON is a Microsoft© Access-based software program used internally by the FBI to run large-scale investigations. It allows for Bureau-wide communications to manage and share information about a specific investigation, including leads and results. During T3, the FBI used ICON to set leads and monitor the status of the investigation.
- JFO Net. JFO net is the intranet developed and implemented by DHS to support emergency management activities and information flow across Federal operations centers, including the JFO, PFO cell, HSOC, and IIMG. During T3, JFO net was used to post tactical information from the Unified Command in Connecticut as well as more operational and strategic information from the JFOs and the HSOC in Washington, DC.
- Law Enforcement Online (LEO). LEO is a secure information system maintained by the FBI that provides a communication link for all levels of law enforcement in the United States. Through LEO, authorized users can access a variety of information tools, including an electronic law enforcement library, e-mail, chat, topical web pages, and areas for special interest groups.[52] During T3, the law enforcement community used LEO to document their activities and share information regarding the ongoing investigations in New Jersey, Connecticut, and internationally.
- New Jersey Local Information Network and Communications System (NJLINCS). NJLINCS is a system of public health professionals and electronic public health information that enhances the identification and containment of diseases and hazardous conditions that threaten the public's health. Built on personal computer and Internet technologies, LINCS is a network of 22 strategically positioned local health departments located throughout the State, the New Jersey Department of Health and Senior Services,

[50] See http://www.eteam.com

[51] See https://www.hots.nj.gov/

[52] See http://www.fbi.gov/hq/cjisd/leo.htm

all other local health departments, and public/private organizations working at the community level to protect the public's health.[53]

The following list is not exhaustive, but represents the large number of information systems in use during the exercise, as well as how different response communities relied upon their own systems:

- The State health community used HOTS, NJLINCS, ETEAM, HERMIS, and CDRS to coordinate a response to the spread of plague in New Jersey.
- The State emergency response community in New Jersey used E-Team.
- The Federal emergency response community used JFO net and HSIN International.
- The law enforcement community used LEO and ICON.

For the most part, these information systems used by different communities and levels of government have evolved independently. The result is a series of stovepiped systems that compartmentalize information. For example, in New Jersey, the State EOC was often unaware, or belatedly informed, of decisions made in the Department of Health and Senior Services (DHSS) Health Command Center (HCC) that were broadcast across HOTS but not communicated via other means until later. In another example, although the law enforcement community in both States was well informed via LEO of the status of the FBI's investigation, the same cannot be said for members of the medical community or the Federal response apparatus, who had limited or no access to the FBI's information system. This may have contributed to the delay or failure to correct misconceptions about the presence of mustard in the Beechcraft Baron found in Maine. Whereas other operating centers and agencies made decisions and developed plans under the incorrect belief that the aircraft was a red herring, persons with access to LEO could track the FBI's investigation of phone numbers found on the aircraft, the four individuals who exited the aircraft shortly after its arrival in Maine, and the venting/dispersal equipment found onboard during the initial search. In other words, only agencies with access to LEO knew that the aircraft was still under investigation.

The widespread use of information systems can also foster the misperception that information has been widely distributed. However, their use can actually result in persons who need access to the information not having it, and persons with access not knowing new information is available or not having the time to retrieve it. Additionally, because these systems are not interoperable, any inputs or updates retrieved from another system must be entered manually, thereby increasing dissemination time, the likelihood for error, and the potential that information may not be entered at all, particularly as responders get busier during a crisis. The result can be that different communities, agencies, or operating centers are using different information for planning and decision making. The lack of common casualty numbers and the difference in information about the role of the aircraft in the mustard attack are key examples of this.

---

[53] See http://www.state.nj.us/health/lh/lincs/

2. Vast Number of Nodes in the Response Network

The vast number of nodes in the response apparatus complicated the information sharing problem in a variety of ways. First, it takes a tremendous level of effort to keep all agencies and operating centers informed and up-to-date. Second, the more people who touch a piece of information, the greater the chance that that information will be changed in some way. Therefore, the large number of nodes in the response network increases the likelihood that incorrect or time-late information will be passed along. Table IV-4 identifies the 220 operating centers that were part of the T3 FSE domestic response network. Managing information flow becomes even more complex when the roles of international operating centers are taken into account. In effect, the number and variety of operating centers, or nodes, defines the scope of the information sharing problem by establishing the requirements for confirmation of a COP across all the centers.

Table IV-4. Nodes in the T3 Emergency Response

	Connecticut	New Jersey	Interagency
Field	• Incident Command Post • Unified Command Post • Hospitals (32)	• Hospitals (96) • Points of Dispensing (22)	
Local	• New London EOC	• Local EOCs (22)	
State	• State EOC • Area IV Coordinator • DPH ECC • Governor's Office	• State EOC • DHSS HCC • NJ Hospital Association • Governor's Office	
Federal	• JFO • PFO • JOC • JIC • RRCC • SERT • USCG	• JFO • PFO • JOC • JIC • RRCC • SERT	• HSC • HSOC *(DHS)* • IIMG *(DHS)* • NRCC *(DHS)* • TSOC *(DHS)* • IOC *(DHS)* • NICC *(DHS)* • USCG NRC *(DHS)* • SOC *(HHS)* • FDA EOC *(HHS)* • CDC DEOC *(HHS)* • HRSA *(HHS)* • USMS EOC *(DOJ)* • EPA EOC • NORTHCOM *(DOD)* • FBI SIOC • JTTF *(FBI)* • DOT CMC • FAA EOC • NCTC • OSHA EOC *(DOL)* • ARC HQ DOC • VA ROC • IMAAC/NARAC

3. Lack of Formal Information Flow Processes and Use of Alternative Means for Passing Information

The proliferation of information systems and the vast number of agencies and operating centers involved in an emergency response expand the means or channels through which information can be shared.

At the field level, incident radio communications procedures could have been improved. First responders spent a significant amount of time developing and de-conflicting an incident communication frequency plan.

Like much of the information relative to the situations in New Jersey and Connecticut, details about victim numbers initiated at a very local level—the incident site and hospitals in Connecticut, and hospitals and county medical examiners in New Jersey. In both cases, data on casualties moved from the local level to one or more State agencies, and then into the emergency response network of operating centers and State and Federal agency representatives. Figure IV-3 shows the expected process for moving victim data on fatalities in New Jersey. Figure IV-4 shows the same process for moving casualty data in Connecticut. The arrows at the top of the figures indicate that the expected flow of movement is left to right, from the local level to the Federal response organizations. The expectation would be an increased time delay in accurate casualty reports the further to the right an agency or operating center appears on the chart.

Figure IV-3. Expected Information Flow for New Jersey Casualty Data

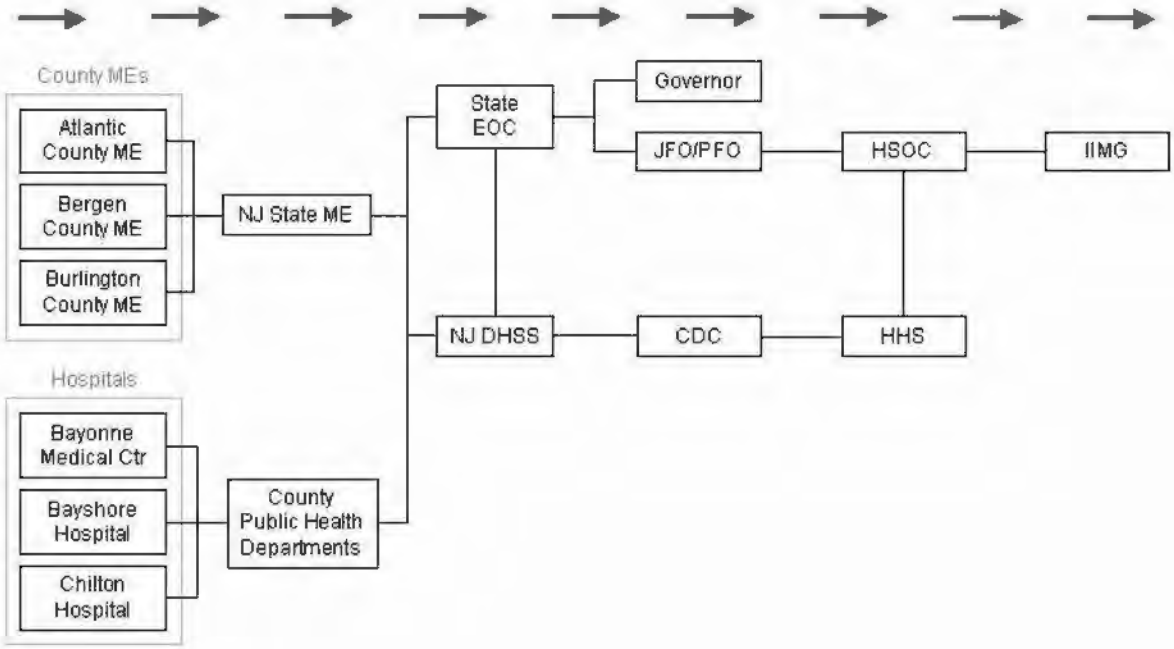
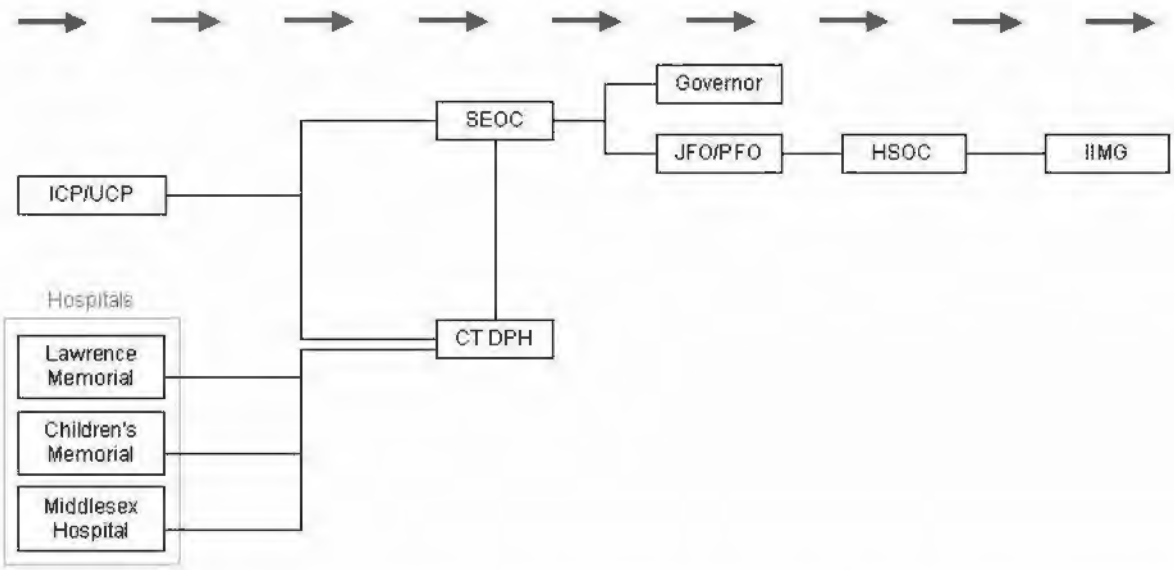
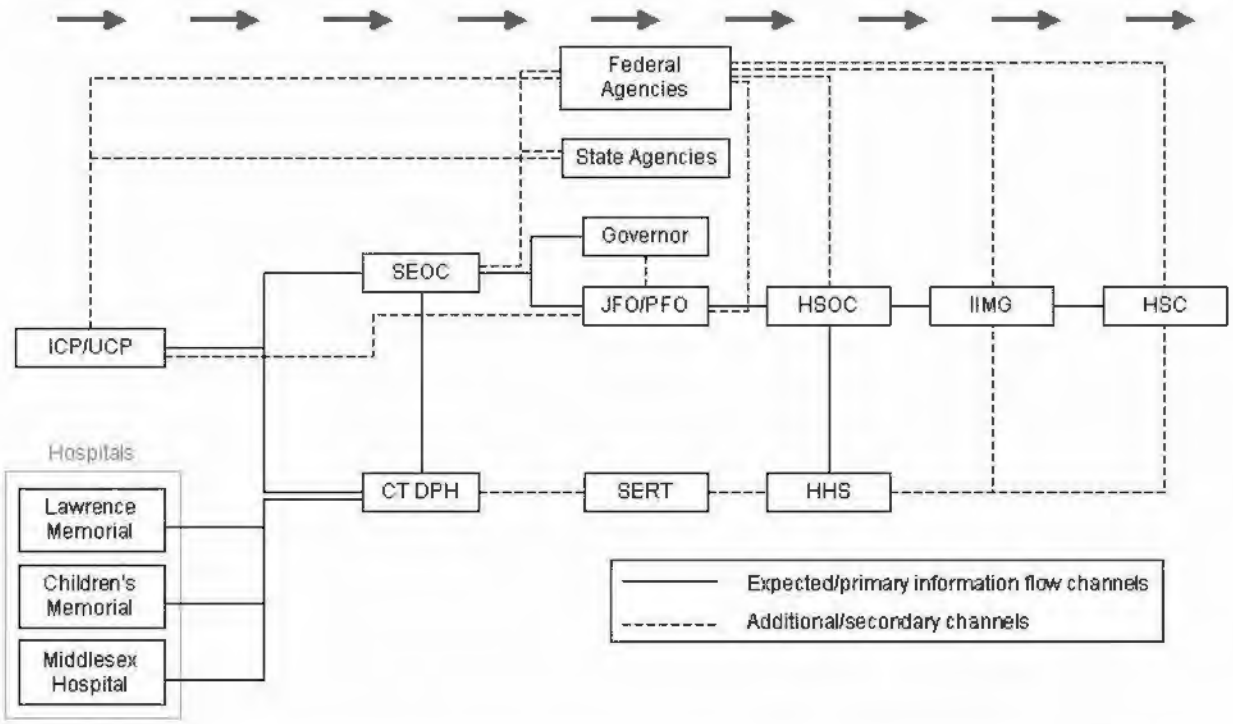


Figure IV-4. Expected Information Flow for Connecticut Casualty Data



Although Figures IV-3 and IV-4 show the expected information flow processes regarding casualty numbers, the data from the exercise suggest a less organized process. Figure IV-5 shows an example of the information flow, as it occurred in Connecticut.

Figure IV-5. Actual Information Flow for Connecticut Casualty Data



With the dashed lines, Figure IV-5 shows some of the secondary, or additional, means by which information moved among the responding agencies. Representatives from State and Federal agencies located at the Unified Command Post, the State EOC, and the JFO pushed casualty data (as well as other information) through their internal agency processes. Local, State, and Federal agencies within the same responder community shared information. For example, medical/public health information was shared among the New London Public Health Office, the Connecticut Department of Public Health, and HHS; information relative to the environmental community was shared among the Connecticut Department of Environmental Protection, the EPA, and the US Coast Guard. Casualty data was shared via conference calls (e.g., between the governor and the PFO). Not shown in this chart, but also a source for information sharing, was VNN, representing all media, which often served to inform agencies and operating centers of new or updated information such as casualty figures. All of these means of information flow are logical, but in the end they often complicate a picture rather than clarify it due to the potential for circular reporting and uncertainty over the authoritativeness of sources and the timeliness of the data.[54]

[54] For additional discussions of alternate information flow processes and examples from T3, refer to the chapters on Emergency Operations under a Unified Command and Agent Confirmation and Hazard Area Definition.

D. Lack of Uniform Reporting Guidelines and Established Procedures for Validating Information to Build a COP

During the T3 FSE, the ill-defined and inconsistent use of language, coupled with the use and forwarding of information from secondary or tertiary sources, led to a limited shared situational awareness across the Federal, State, and local response network.

1. Ill-Defined and Inconsistent Use of Language

The primary reason for the disparity in reported casualties in Connecticut was the use of many different terms to describe the status of victims. The ground truth scenario divided the patients into pools of hospitalized, worried well, and fatalities. A review of the many different situation reports or updates that provided victim numbers in Connecticut revealed players used at least twelve separate descriptors:

- missing;
- casualties;
- deceased/dead;
- worried well;
- walking wounded;
- injured;
- patients;
- sick;
- treated/released;
- hospitalized;
- awaiting hospitalization; and
- symptomatic, but not hospitalized.

Definitions of the descriptors were not provided, and exercise participants and operating centers used many of them interchangeably. For example, at 13:00 on April 5, the representative from the HHS SERT at the Connecticut Department of Public Health's Emergency Command Center (CT DPH ECC) reported to his counterpart at the JFO that 6,000 persons had been hospitalized as of 12:30 that afternoon. Ten minutes after that update, at 13:10, the CT DPH representative at the SEOC briefed that 1,632 persons had been admitted to hospitals, and 5,000 were awaiting hospitalization. This is just one example of how two people from the same facility have different numbers as well as different descriptions of how those numbers break out. The result is different information originating from the same source. The effects of differences in how numbers are reported became noticeable by noon on April 6, when some individuals and operating centers appeared to begin differentiating between hospitalized, symptomatic but not hospitalized, sick, and "treated and released." The result was significantly lower numbers of hospitalized patients reported than the ground truth provided. The use of unclear terminology by persons passing information to other operating centers resulted in a very different picture of casualty numbers and the State's associated medical needs. At issue here is not which term best described the

medical status of victims in Connecticut, but rather the fact that all operating centers and agencies were using different descriptors.

The varying use of language to characterize casualties was also a problem in New Jersey, though it did not show up in the fatality data. In that State's response to plague, the terminology problem revolved largely around case definitions, and different criteria for counting plague victims. During the first day of the exercise, the CDC and State of New Jersey had different definitions for a probable plague case. It also appeared that the CDC was reporting confirmed case numbers, while New Jersey was reporting confirmed and probable cases. Data also show evidence of sources reporting different numbers for hospitalized victims versus those sick but not hospitalized. Once again, this contradicts the ground truth scenario, which simply divided the patients into pools of sick and dead.

2. Use and Forwarding of Information from Secondary or Tertiary Sources

The use and forwarding of information from other than primary sources was a particular problem during the T3 FSE. As is indicated by Figure IV-5, information flow from the local to the Federal level always involves secondary sources, or agencies and operating centers that receive information and pass it along through the response network. Problems arise when authoritative information is lost in all the traffic, or when documents labeled as formal and authoritative use information provided by secondary or tertiary sources.

An example of the use of secondary sources and how they can complicate the operational picture is the dissemination of information associated with the aircraft used by the terrorists in Connecticut. Long after the FBI received confirmation that the aircraft tested positive for mustard, other agencies were still reporting time-late, incorrect information. Particularly noteworthy is that the reports by TSA and OSHA were included in the Connecticut PFO's SITREP to the DHS Secretary with contradictory information from the authoritative source. That 15:00 SITREP reports that:

- per TSA, the FBI analysis of the 55-gallon tank aboard the aircraft yielded no trace of mustard, but rather contained residue of ammonium nitrates; and
- per the FBI, the two drums found on the aircraft tested positive for sulfur mustard and additional samples analyzed by Edgewood also tested positive.

As a formal document from the PFO to the Secretary informing him of the status of the situation in Connecticut, the SITREP should not contain secondary information, particularly when the authoritative source is nearby and available. It is unclear why the PFO and JFO Coordination Group continued to be uncertain of the means of dispersal through the conclusion of the FSE, considering the FBI Senior Agent in Charge (SAC), a member of the coordination group, should have served as the authority on the subject, immediately correcting any misperceptions about the source of the contamination. The contradictory information in the 15:00 SITREP offers an example of questionable consolidation and validation of secondary information.

The use of questionable sources and the issue of who is responsible for validating information also influenced the differences in casualty figures observed during the T3 FSE. Particularly at the Federal levels, variation in numbers appeared to be a result of who was providing the data and where in the operating center it was routed. For example, in the Connecticut JFO, both the Situation Unit in the Planning Section and the HHS representative to the JFO Coordination Group were tracking victim numbers, but were reporting different results. Initially, the Situation Unit was getting its data from a variety of different sources, including the FBI, the Unified Command, and the State EOC. ESF #8 and the HHS Senior Federal Official (SFO) received updates from the SERT and from the Connecticut DPH. At the same time, the PFO cell and JFO Coordination Group were receiving casualty updates via conference calls with the State EOC and the Unified Command. Frustrated with the different victim numbers, the JFO Coordination Group sought to correct the problem by tasking the HHS SFO to clarify the casualty situation at 12:20 on April 5. Although that resolved the issue in the short term, it did not fix the underlying process problem, which was that multiple groups and teams in the JFO were requesting and receiving casualty data from various sources. The issue arose again the next day at 13:15, when the JFO Planning Section discussed the most current numbers received from ESF #8, the Unified Command, the State EOC, and the PFO, all of which varied. Recognizing the need for a more permanent solution to the problem of contradictory figures, the Planning Section Chief determined that the SEOC would be the single, authoritative source for updating the JFO's casualty data. This example indicates that exercise participants recognized the need for identifying authoritative sources.

3. Inadequately "Shared" Situational Awareness across Operating Centers

During the T3 FSE, agencies and operating centers were often making decisions and acting on different information. In Connecticut, the Unified Command drafted its initial air and ground sampling plan under the misconception that the truck bomb was the means by which the mustard was dispersed. Top Federal officials responding to the plague crisis in New Jersey had different casualty figures than State and Federal operating centers. These different figures drove the decision to open more PODs than State public health officials initially recommended.

Both of the previous examples originated from errors by exercise controllers. However, it should not matter where bad information originates or how it enters the system; it still needs to be corrected. For example, on September 11, 2001, television news stations reported disturbances on the National Mall in Washington, DC, which were later proven to be false. More recently, initial reports out of London contended that the July 7, attacks were not the work of suicide bombers, information that later proved to be incorrect. Law enforcement officials immediately proceeded to correct the error. Whether incorrect information is from an exercise artificiality, a product of premature reporting, or a result of the chaos of a situation, there need to be methods and means for correcting or updating the information.

Overall, the examples from the T3 FSE indicate failures to adequately validate and consolidate information at all levels of the response. Situational awareness was not effectively shared, nor a COP developed, across responding operating centers and agencies.

At the Federal level, the NRP tasks the HSOC with developing the COP and maintaining situational awareness of the incident and the response. To this end, the HSOC SOP provides specific guidelines for the COP display. The HSOC's COP is an electronic display of a map of the United States embedded with nodes of the national infrastructure. The map contains a variety of icons that allow users to drill down to threat information, SITREPs, and spot reports. The COP is available to operating centers outside the HSOC via JFO Net.

Observations during T3 FSE indicate that the COP described in the HSOC SOP does not adequately support emergency situational awareness across the Federal operating centers. This is evidenced by examples of HSOC desk officers searching through e-mails and querying other desk officers for status of EEIs. The COP did not lend itself to displaying such information because it is largely just a graphical user interface, through which users can post and access situational reports or intelligence provided by other operating centers or agencies. This approach to a COP may be sufficient for daily operations, when the HSOC is monitoring threats or potential threats, but during an emergency response, information is more fluid and the EEIs themselves are different. The HSOC SOP focuses on the picture itself, not the EEIs that need to be tracked. Moreover, not all EEIs can be displayed visually, but they still need to be tracked and shared. As a result, the COP itself became useless.

Additionally, the HSOC SOP does not establish the processes needed to maintain and share the EEIs, including the mechanisms necessary for consolidating and validating information. EEIs to he shared hetween operating centers and agencies were never clearly defined. During the T3 FSE, the primary means of sharing information among the responding Federal agencies was forwarding e-mails to all the representatives in the HSOC. Each individual was then responsible for developing and maintaining their own knowledge of the state of the incident, to include filtering and consolidating information for movement outside the HSOC itself. This process, or lack thereof, also meant there were no opportunities for group sharing, to support validation or conflict resolution. Finally, no process existed and no effort was made to insure that everyone in the HSOC had common knowledge.

E. Issues from Previous Exercises

The T2 AAR identified two overarching information flow issues:

- lack of formal processes/channels (or understanding of them) for official information and lack of consistent understanding of formal, validated sources for information; and
- use of inconsistent or technical language.

It is clear from the T3 FSE that these issues remain a significant challenge in an emergency response operation.

The prevailing communications issue during the T2 FSE was the lack of formal processes or channels for official information and the prevalence of informal processes, all of which led to difficulties validating information. The T3 observations indicate that although some formal

processes have been instituted, namely the PFO-HSOC-IIMG connection, the informal and internal agency processes continue to complicate the flow of valid information.

The use of inconsistent language proved to be another communications challenge during T2, specifically the interchangeable use of the term "casualties." The T3 FSE revealed continued problems with inconsistent and ill-defined terminology.

Inaccurate reports of casualty figures were also a considerable problem during the T2 FSE play in Illinois, where a plague attack was simulated. Analysis attributed the problems to the complex and multiple ways in which patient data were communicated (e.g., fax, landlines, and cell phones), variation in the descriptors used with the data, and exercise artificialities associated with additional, unscripted injects by an organization outside the T2 planning team and scripted or pretaped media play. The experience in T3 did not suggest any improvement in the accurate and timely reporting of casualty figures. In particular, problems with language, namely inaccurate and inconsistent use of descriptors, were still a significant problem in the T3 FSE.

The T3 CPX revealed little evidence of consolidated information flowing from the HSOC to the other Federal agencies. Additionally, no specific information requirements, or EEIs were developed for the exercise, nor was there a shared COP. These issues continued to be problematic during T3 FSE.

Table IV-5. Comparison of T3 FSE with Previous Exercises

T2 FSE	SOEs	T3 FSE
ISSUES/OBSERVATIONS		
• Lack of consistent understanding of formal, validated sources for information. • Inconsistent use of terms/unclear technical language.		• Lack of uniform reporting guidelines and procedures for validating information received from secondary or tertiary sources.
• Too many official reporting channels. • In some cases, lack of formal processes/channels for official information. • Various agencies had their own, independent procedures and redundantly requested updates • Hospital data was largely paper-based and disparate reporting processes were burdensome.	• Lack of a robust system for sustained coordination with FSL governments and private sector partners—especially how to reduce, and not add to, the "white noise" or "fog of war" anticipated in preattack threat stages.	• The use of informal or alternate channels for sharing information caused problems by enabling circular reporting and bypassing authoritative sources.
	• Participants discussed the large number of operations centers and coordinating entities that are involved in a response to a terrorist incident.	• The vast number of operating centers negatively affected information sharing by increasing the scope and complexity of the problem. • Agencies and operating centers acted and made decisions on different information.
	• Officials questioned how effectively the large number of operations centers and coordinating entities would share information and the degree to which they would share a "common" picture of the incident.	• Agencies and operating centers made decisions and acted on different information. • Situational awareness was not effectively shared across operating centers and agencies.
	• Concern that information that is shared is not being transmitted in formats or with needed tear lines so that some agencies can use it. • What influence (if any) that concern about potential media leaks should have on the release timing and content of unclassified intelligence bulletins (and tear lines).	
	• Concern regarding the sharing of information between the incident site, JOC, JFO, and State EOCs.	•

F. Conclnsions

Accurate and timely sharing of information and the resulting development of a COP are critical for the success of an integrated Federal, State, and local response. Experiences during the T3 FSE indicate that these issues remain problematic for the operating centers and agencies involved in a domestic response.

The information systems used in T3 were largely stovepiped within agencies and/or response communities. Instead of facilitating exchanges, these systems contributed to the compartmentalization of information and a misperception that information was widely disseminated. The entire domestic response community should be working toward interoperability and integration of systems. The Homeland Security Information Network initiative is likely a good starting point, as it works to link at least some of the Federal response operating centers (e.g., JFO, HSOC, and IIMG) and the law enforcement community.

The vast number of operating centers activated to support the emergency response during T3 negatively affected information sharing by increasing the scope and complexity of the problem. The more operating centers and/or agencies involved in the response, the greater the number of operating pictures that need to be aligned with the COP, the more channels are available through which information can pass, and the greater the number of opportunities for errors or changes to be made in the information. Each Federal agency should assess its emergency response operations and consider reducing the number of operating centers activated, consolidating them, or collocating personnel to facilitate better communication during an Incident of National Significance.

During T3, participants made use of informal or alternate processes to move information throughout the response network. This complicated information sharing and the development of a COP by enabling circular reporting and increasing uncertainty over the authoritativeness of information sources.

Ill-defined and inconsistent use of language and the extensive use of information from secondary and tertiary sources indicate a lack of uniform reporting guidelines and procedures for validating information. To preempt inconsistent use of language, the different response communities should identify key terms that are likely to appear during a WMD response, standardize their definitions, and then disseminate the information across the entire response network. Much of this work can be done in advance of any incidents. However, some definitions may need to be revised or developed during an emergency response. For example, during the outbreak of Severe Acute Respiratory Syndrome (SARS) in 2003, the CDC and other health agencies around the world developed and revised case definitions throughout the crisis. Therefore, response communities also need to identify mechanisms to update and disseminate definitions during response operations.

Stovepiped systems, the vastness of the response network, the existence of alternate information flow channels, and the lack of uniform reporting guidelines and validation procedures resulted in situational awareness not being effectively sbared, nor a COP developed across responding

operating centers and agencies. Instead, agencies and operating centers made decisions and acted on different information. To build shared situational awareness, the response network needs to:

1. Identify and define the overlapping critical information required by all the responding communities.
2. Establish specific reporting protocols and guidelines for all levels of government.
3. Identify the authoritative sources for EEIs.
4. Identify an operating center at each level of the response to act as "keeper of the COP.
5. Develop protocols for horizontal and vertical coordination (i.e., horizontally across one level of government and vertically between levels) to align the operational pictures developed and maintained by different operating centers and agencies.

1. Recommended Courses of Action

- Support the development of interoperable information systems and/or a suite of emergency response/management applications that can be used across response communities.
- Consider development of a DHS field operations guide that lists radio frequencies/preferences of Federal, State, and local responders to expedite the development of communications plans.
- Assess the roles and responsibilities of each emergency response operations center and consider reducing the number of operating centers, consolidating them, or collocating personnel.
- Require that all casualty numbers reported are attached to a clear description of the information included in the report.
- Identify key terms that are likely to appear during a WMD response, standardize their definitions, and then disseminate the information across the entire response network.
- Establish mechanisms to update and disseminate new definitions during response operations.

To build an accurate and effective common operating picture, the response network needs to:

1. Identify and define the overlapping critical information required by all the responding communities.
2. Establish specific reporting protocols and guidelines for all levels of government.
3. Identify the authoritative sources for EEIs and what EEIs should be communicated.
4. Identify an operating center at each level of the response to act as "keeper of the critical information."

   Develop protocols for horizontal and vertical coordination (i.e., horizontally across one level of government and vertically between levels) to align the operational pictures developed and maintained by different operating centers and agencies.

Part 5: Analysis of Critical Task Performance

The number of participants in TOPOFF 3 (T3) makes it impossible to evaluate the critical tasks of every player and organization. Hotwashes and an After-Action Conference allowed players to discuss the exercise and their perceived participation and performance within the exercise. They also gave the evaluation team a chance to focus the topics that would be discussed in this document. The fact that an issue was not selected for analysis does not signify that it is not a critical task in our national Homeland Defense Strategy. Rather, the six items offer a cross-section of the complex nature of the exercise and the various lessons learned. As stated earlier in this report, the items to be discussed in this section are:

Critical Tasks	• Stafford Act Declarations • Emergency Public Information • Integrating Responses to Incidents of National Significance: Public Health Emergency and the Stafford Act • Strategic National Stockpile and Points of Dispensing • Agent Confirmation and Hazard Area Definition • Emergency Response Operations under a Unified Command

This section of the report reviews performance of critical tasks as identified by the HSEEP Volume II Exercise Evaluation Guide (EEG). Each critical task was chosen because of the significant effect that these issues had on the exercise participants and the exercise as a whole.

Some topics overlap, but each account is written so that it may stand on its own. The format for discussion of each critical task is provided in accordance with HSEEP Volume II EEG guidance. Accounts begin with a brief introduction to the issue and related EEG task and number, followed by a summary of observations. The summary contains a background discussion of any relevant policies, doctrine, or procedures. This is followed by a reconstruction of key events from the exercise. The analysis section presents the issues that emerged in the exercise, including detailed examples and potential explanations for the behavior or result. The analysis is followed by a comparison of the T3 Full-Scale Exercise (FSE) results with any relevant conclusions from previous exercises. Finally, each account concludes with a review of recommended courses of action.

I. Stafford Act Declarations—Task # III-10: Request State/Federal Assistance

A. Summary of Issue

The issue is whether an incident with a non-explosive biological, chemical, or radiological weapon would fit the definition of a major disaster under the Stafford Act. During the T3 FSE, there were several declarations and proclamations of emergencies and disasters. State and local jurisdictions in both exercise venues invoked their authorities to declare emergencies and also requested Federal assistance under the Stafford Act. These requests ultimately led to presidential declarations of major disaster in Connecticut and of emergency in New Jersey.

In this exercise, just as in the T2 FSE, participants discussed the applicability of a Stafford Act major disaster declaration to terrorist attacks, especially to attacks that feature non-explosive biological weapons. Although the Governor of New Jersey requested a major disaster declaration, an emergency declaration was provided. Under an emergency declaration, there are limitations in the types and amount of assistance that can be provided. The effects of these limitations were not fully explored in the T3 FSE. However, in the T3 Large-Scale Game (LSG), uses of the existing Stafford Act and other Federal programs were identified to make up for the shortfalls in assistance that New Jersey experienced under the emergency declaration. Throughout the exercise, it has been acknowledged that the Stafford Act needs amending to include all hazards, including terrorist acts.

B. Background

Federal declarations made under the Stafford Act generally start with a request from a State Governor.[1] Requests for declarations of both emergency and major disaster must "be based on a finding that the disaster is of such severity and magnitude that effective response is beyond the capabilities of the state and the affected local governments and that Federal assistance is necessary."[2] The Stafford Act defines a *major disaster* as:

> *any natural catastrophe (including any hurricane, tornado, storm, high water, wind driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this chapter to supplement the efforts and available resources of states, local governments, and disaster*

[1] In T3, the President declared an emergency in New Jersey before application was made.
[2] The Robert T. Stafford Disaster Relief and Emergency Assistance Act, As Amended, 42 U.S. Code (U.S.C.) 5121, et seq., http://www.fema.gov/library/stafact.shtm.

> *relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.*

Under a presidential declaration of major disaster, States may be reimbursed for up to 100% of qualifying expenses.

An *emergency* is defined as:

> *any occasion or instance for which, in the determination of the President, federal assistance is needed to supplement state and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.*

Federal assistance under a presidential declaration of emergency is limited to $5 million for a single emergency except in circumstances in which the President determines that:

- Continued emergency assistance is immediately required;
- There is a continuing and immediate risk to lives, property, public health, or safety; and
- Necessary assistance will not otherwise be provided on a timely basis.[3]

Differences between a major disaster declaration and an emergency declaration include limitations in public assistance, individual assistance, and hazard mitigation. Table I-1 summarizes the differences in Federal assistance under a major disaster declaration and an emergency declaration.[4] Exceptions may be made if the President determines that additional assistance is necessary to "to save lives, protect property and public health and safety, and lessen or avert the threat of a catastrophe."

Table I-1. Types of Federal Assistance for a Major Disaster and an Emergency

Type of Assistance	Major Disaster	Emergency
Public Assistance		
Category A: Debris removal	X	X
Category B: Emergency protective measures	X	X
Category C: Road systems and bridges	X	
Category D: Water control facilities	X	
Category E: Public buildings and contents	X	
Category F: Public utilities	X	
Category G: Parks, recreational, and other	X	

[3] Section 503 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as Amended, 42 U.S.C. 5121.

[4] Based on comparison sheet faxed to New Jersey State EOC from DHS Emergency Preparedness and Response on April 8, 2005.

Type of Assistance	Major Disaster	Emergency
Individual Assistance		
Housing assistance	X	X
Other needs assistance (e.g., medical, funeral)	X	X
Disaster unemployment assistance	X	
Legal services	X	
Food coupons and distribution	X	
Crisis counseling	X	
Hazard Mitigation	X	

C. Reconstruction

At 12:14 on April 4, 2005, the Governor of New Jersey declared a state of emergency, initiated the activation of the State Emergency Operations Center (EOC), and raised the State's threat condition level to Orange after the presumptive diagnosis of pneumonic plague and the discovery of a suspected dispersal mechanism. At 14:12, the Governor of Connecticut responded to the explosion at the New London City Pier by declaring a state of emergency, activating the State EOC, and raising the State's threat condition level to Orange.

The Secretary of Homeland Security declared the events in New Jersey to be an incident of national significance (INS) at 14:00 and designated a Principal Federal Official (PFO). Later at 16:00, the Secretary declared the events in Connecticut to be an INS and designated a PFO.

The Governor of Connecticut verbally requested a declaration under the Stafford Act from the President at 15:00. This was followed by a faxed written request. At 16:30, the National Response Coordination Center (NRCC), Interagency Incident Management Group (IIMG), Regional Response Coordination Centers (RRCCs), and other operations centers reported that the President had verbally declared emergencies for Connecticut and New Jersey under the Stafford Act. Later, the declaration in Connecticut was corrected to a major disaster. The major disaster declaration covered public assistance Category A (debris removal) and Category B (emergency protective measures). Individual assistance was initially not included in this declaration, even though it was included in the Governor's request. Individual assistance later was approved.

New Jersey faxed a formal request for an emergency declaration under the Stafford Act to the Region 2 RRCC at 16:59. In New Jersey, the emergency declaration provided public assistance for Union and Middlesex Counties. On April 6, the emergency declaration was amended to include 10 additional counties: Bergen, Burlington, Essex, Hudson, Mercer, Monmouth, Morris, Passaic, Somerset, and Sussex Counties. On April 7, the Federal Emergency Management Agency (FEMA) added the remaining nine counties in New Jersey to the emergency declaration and designated residents of all counties eligible to receive individual assistance. Because individual assistance was

approved for New Jersey, the Small Business Administration was able to provide disaster loan assistance. New Jersey requested 2,000 crisis counselors/mental health professionals. On April 8, FEMA denied New Jersey's request, because New Jersey had received an emergency declaration instead of a major disaster declaration. Although the Governor of New Jersey had attempted to have the emergency declaration converted to a major disaster under the Stafford Act, the exercise ended before the Governor's request was addressed.

D. Consequence

Both of the simulated terrorist attacks in the T3 FSE led to presidential declarations under the Stafford Act.

The Stafford Act does not explicitly include events involving non-explosive radiological, chemical, or biological weapons in its definition of major disasters. However, some participants indicated that the Stafford Act may be interpreted to include such incidents under its definition of major disasters. Clarifying this point would reduce debate and confusion during a time of crisis. If these types of incidents are not covered under a major disaster declaration, Congress should consider adding them to the definition.

If it is determined that biological, chemical, or radiological incidents do not fit the definition of a major disaster, subgranting under Stafford Act declarations may provide additional types of Federal assistance. However, this would require the emergency to be linked to another incident involving an active major disaster declaration. Other Federal assistance programs not connected to the Stafford Act may be able to provide additional assistance. Federal agencies should develop a list of what assistance programs may apply and under what circumstances they would apply.

Most likely, Federal assistance to the victims of an attack with a non-explosive biological, chemical, or radiological weapon would exceed the $5 million limit of an emergency. In the past, Congress has granted exceptions to this limit under such circumstances. Therefore, this monetary limit is unlikely to result in significant impacts on response spending.

E. Analysis

Under the Stafford Act, a major disaster declaration would provide more types and a greater amount of assistance than an emergency declaration. In T3, the primary issue with Stafford Act declarations was the applicability of a major disaster declaration to a biological incident. Because New Jersey received an emergency declaration instead of a major disaster declaration and the additional assistance that comes with a major disaster, Federal agencies worked to provide assistance that was not covered by the Stafford Act Declaration. By the end of the FSE the SBA had provided assistance to New Jersey. Additionally, the use of verbal approvals for the initial declarations without supporting documentation and formal requests caused uncertainty as to what type of declarations

were approved and what types of assistance should be provided. Analysis of T3 revealed that:

- It is unclear whether a major disaster declaration under the Stafford Act can be applied to a biological incident.
- Subgranting under the Stafford Act and other Federal programs may provide for some shortfalls in types of assistance provided under an emergency declaration.
- Because of exception clauses in the Stafford Act, limitations in the amount of monetary assistance under an emergency declaration would probably not result in any substantive real-world impact.
- Verbal declaration approvals and a lack of written requests led the NRCC, both RRCCs, and both State EOCs to be uncertain as to what type of declaration was approved and what types of assistance were granted.

1. Uncertainty about Applicability of a Major Disaster Declaration to Biological Incidents

The incidents in New Jersey were not addressed by a major disaster declaration under the Stafford Act because the circumstances of a biological attack are not explicitly included in the definition of a major disaster. In the initial request for a declaration, the Governor of New Jersey stated that he was aware that "under current application of these provisions [Stafford Act], the spread of an infectious, biologically based disease is not regarded as a major disaster." He asked the President and Congress "to seek revision of the Stafford Act to ensure that appropriate assistance is available." The Governor also requested crisis counseling, legal services, food stamps, and unemployment benefits assistance, which are not covered under an emergency declaration. Later, the Governor of New Jersey asked FEMA to convert the emergency declaration to a major disaster declaration, because the State sought some of the assistance available only under the latter declaration. New Jersey had submitted a specific request for crisis counseling, but did not receive it because crisis counseling is not covered under an emergency declaration.

To clarify the application of a major disaster declaration, the most straightforward solution would be to amend the Stafford Act and update the disaster definition. However, some FEMA participants in the T3 FSE did not believe that amending the Stafford Act was necessary. Instead, they suggested that the language used in the Stafford Act to define a major disaster could be interpreted to include a significant biological attack.[5] However, they did not want to set a policy precedent in an exercise.

Because of the differences in the types and amounts of assistance and because of the potential scale and scope of such an incident, it would be preferable to have a major disaster declaration apply to any incidents involving a weapon of mass destruction (WMD). Furthermore, the experiences from the T2 and T3 FSEs indicate that the definition of a major disaster declaration and the range of incidents to which it applies

[5] These FEMA participants did not specify the details of the reinterpretation, but simply suggested it as a viable option.

need to be clarified to eliminate any uncertainty. It would be inappropriate and ineffective to debate these types of issues during an actual crisis.

2. Alternatives for Shortfalls in Types of Assistance

Because a major disaster declaration did not apply to incidents like the simulated biological attack in New Jersey, T3 participants identified alternative sources to compensate for the shortfalls in the emergency declaration. NJ residents were not eligible for some types of individual assistance that were available to residents in New London. Under the emergency declaration, NJ residents could not receive unemployment disaster assistance, legal services, tax considerations, or crisis counseling. The impact of these shortfalls would not have been felt in the timeframe of the T3 FSE and therefore were not played. However, they were discussed during the T3 LSG.[6]

At the T3 LSG, participants focused extensively on how to make up for a lack of assistance under an emergency declaration. The Human Services group had a lengthy discussion about how to provide crisis counseling and other services to NJ residents without statutory changes to Stafford Act language or supplemental appropriation from Congress. The proposed solution was "subgranting" through the major disaster declaration in Connecticut to provide mental health services in both States.

The subgranting of crisis counseling for an emergency declaration through a major disaster declaration does have a limitation. Using a subgrant to provide crisis counseling requires an active major disaster declaration in a State with a linked situation. Although New Jersey was not one of the sites of the September 11, 2001 (9-11) terrorist incidents, a large portion of the NY workforce lives in the State. As a result, an emergency declaration was issued for the State, along with the major disaster declaration for New York. In T3, the terrorist attacks in Connecticut and New Jersey were conducted by related terrorist groups and during the same timeframe. T3 LSG participants believed that this was sufficient to link the incidents. Connecticut's major disaster declaration fulfilled the requirement of an active major disaster declaration.

Another potential method for augmenting the assistance limitations of an emergency declaration would be to provide funding for crisis counseling through other sources, such as the Substance Abuse and Mental Health Services Administration (SAMHSA) Office for Victims of Crimes (OVC). Other Federal programs also may address the shortfalls related to the types of assistance not provided under an emergency declaration.

A major disaster declaration can provide more types of Federal assistance than an emergency declaration. These types of assistance may be needed by individuals and businesses that are victims of a significant biological attack. Subgrants under the Stafford Act, if applicable, and assistance from other Federal programs could compensate for the

[6] The T3 LSG was conducted from May 3-5, 2005, at the National Conference Center, Lansdowne, VA. The T3 LSG focused on recovery issues at 30 days, 90 days, and 180+ days after the T3 FSE scenario. Refer to the section on T3 building block events for more information on the T3 LSG.

limited assistance provided by an emergency declaration. Another option is for Congress to appropriate additional funds to compensate for the limited assistance.

3. Limitations in the Amount of Assistance

Another difference between declarations of emergency and major disaster is the limit on the amount of funding. An emergency declaration has a $5 million limit on assistance. This limit can be exceeded if the President determines that it is required. As discussed above, the criteria for exceeding limits on Federal assistance are: a continued need for emergency assistance; an immediate risk to lives, property, public health, or safety; and assistance that will not otherwise be provided on a timely basis. The events in New Jersey would have met the criteria for exceeding the funding limits. To obtain additional funding, the President would have to "report to Congress on the nature and extent of the emergency assistance requirements" and "propose additional legislation if necessary."[7]

The Governor of New Jersey stated in his request for an emergency declaration that preliminary "indications of costs are well in excess of $5 million." Continued assistance would be required. With the exception of a FEMA Mission Assignment log, however, exercise data do not indicate that there was any further discussion of extending Federal assistance to New Jersey or any action taken to address supplemental authorizations.

It is unclear how exceeding the funding limits would have affected response efforts in T3. In previous incidents, Congress granted additional assistance when requested. For 9-11, the President asked Congress to pass emergency appropriations to provide immediate resources for responding to the terrorist attacks.[8] By September 18, 2001, Congress had appropriated $3 billion in Federal assistance to New York City and followed up with additional appropriations as the scope of the disaster was revealed. The 9-11 experience suggests that the President would request additional assistance and that Congress would act quickly in response. Congress did not play in this exercise, and the exercise was too short to examine the actual impact of the spending limits of an emergency declaration.

For an incident of the size and scope of that in New Jersey, the Federal government would have probably quickly exceeded the spending limits imposed under a Stafford Act emergency declaration. The Stafford Act provides for additional funding based on Congressional approval. However, the T3 FSE did not provide the opportunity to test that approach to funding. It is unclear how difficult or time consuming it would be to ask Congress for additional assistance, but real-world experience suggests that this approach would not have any substantive impacts on the Federal response.

[7] Section 503 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, As Amended, 42 U.S.C. 5121.

[8] GAO report, September 11, Overview of Federal Disaster Assistance to the New York City Area, October 2003, Report number 04-72.

4. Initial Uncertainty about Declaration Type and Assistance

The NRCC and RRCCs first heard about the emergency and major disaster declarations through the announcement of the President's verbal approval of two emergency declarations. The NRCC did not receive the written request until 18:00 on April 4, approximately three hours after the announcement. During the hours between the announcement of the approval and receipt of the written request, representatives at the NRCC tried to locate the formal request and determine what type of declaration was approved and what types of assistance would he provided.

The State EOCs, both RRCCs, and NRCC held conference calls to sort out what was approved. The verbal reports of approval for an emergency declaration for Connecticut conflicted with Connecticut's request for a major disaster declaration. Federal and State agencies were uncertain about what types of public assistance were approved and whether individual assistance had been requested. Although the resulting delay in requesting resources was not substantial, this incident highlights a source of uncertainty and is an example of an event in which the results of meetings held by decision makers were not relayed in sufficient detail for their staffs to execute.

5. Issues from Previous Exercises

In T2 FSE, a large-scale bioterrorism attack did not qualify as a major disaster. It was recommended that future efforts, including exercises, continue to refine the applicability of the Stafford Act to bioterrorism and other non-explosive disasters not explicitly defined by the Act, as well as continue to familiarize Federal, State, and local (FSL) agencies with applying the Act during such disasters (Table I-2).

The T3 Command Post Exercise (CPX) featured a unique application of the Stafford Act. The President signed a declaration of emergency for the area between Boston, MA, and Norfolk, VA. The declaration was based on an imminent threat rather than an actual incident. The exercise prompted department and agency participants to question the use of the Stafford Act as a tool for the Federal government to take preparatory measures in anticipation of a terrorist attack.

In particular, the T3 CPX highlighted the need to clarify policy and guidance for deployment of emergency response assets and funding in anticipation of an imminent terrorist attack. In addition, the CPX suggested the need to examine the ramifications of pre-incident deployments if no incident occurs.

Table I-2. Comparison of T3 FSE with Previous Exercises

T2 FSE	T3 CPX	T3 FSE
SIGNIFICANT DECISIONS		
• The President declared a major disaster for Seattle as a result of the radiological dispersal device (RDD) attack. • Illinois requested a declaration of major disaster for Chicago and its surrounding counties as a result of the outbreak of pneumonic plague. The President declared an emergency for those locations to include Individual Households Program and Categories A and B under Public Assistance.	• Based on intelligence, the President signed a declaration of emergency for the area between Boston, MA, and Norfolk, VA, in advance of an actual incident.	• The President declared a major disaster in Connecticut as a result of the vehicle-borne improvised explosive device (VBIED) and chemical attacks. • New Jersey requested and received an emergency declaration for the two most affected counties, later amended twice to include the entire State as a result of the outbreak of pneumonic plague. • New Jersey requested that the emergency declaration be converted to a major disaster, but the exercise ended before the request was addressed.
ISSUES/OBSERVATIONS		
• Despite Illinois' request for a disaster declaration, FEMA determined that "an emergency declaration is ... [the] most appropriate immediate action." • The outbreak of pneumonic plague did not qualify as a "major disaster" within the meaning of the Stafford Act.	N/A	• The Governor of New Jersey stated that he was aware that "under current application of these provisions [Stafford Act], the spread of an infectious, biologically based disease is not regarded as a major disaster." • FEMA applies a strictly literal interpretation of the Stafford Act. Because biological attacks are not explicitly included in the definition of a major disaster, only emergency declarations can be applied.
• Illinois officials were unaware that the $5 million limit to assistance under an emergency declaration can be exceeded under certain conditions.	N/A	• No evidence of concern about the spending limitations in New Jersey • Concerns about the ***specific types*** of assistance available in an emergency declaration *This problem was accentuated because Connecticut was receiving types of assistance not available to New Jersey as a result of the different declarations.*
	• Participants questioned the use of the Stafford Act as a tool for the Federal government to take preparatory measures in anticipation of a terrorist attack.	

F. Recommendations

- Determine the applicability of a Stafford Act major disaster declaration to non-explosive incidents involving WMDs, particularly those involving a large-scale bioterrorism incident.
- If these types of incidents do not fit the definition of a major disaster declaration, determine whether exemptions within the Stafford Act for Emergency Declarations and other Federal programs can result in an equivalent level of assistance and can be delivered with an equivalent level of expediency during an incident. If they can, ensure that States are aware of them.
- If the Stafford Act major disaster declaration does not cover these types of incidents and if equivalent Federal assistance is not available through other means, pursue legislation to address this problem.
- Until legislation is passed that would allow these types of incidents to receive the full range of Federal assistance provided under a major disaster declaration, identify other Federal programs that may be able to provide assistance and ensure that States are aware of them.

II. Emergency Public Information—Task # III-14: Provide Emergency Public Information to Media and Pnblic

A. Summary of Issue

The issue is that FSL agencies may still not be prepared to provide swift, accurate, and consistent lifesaving protective action guidance to the public. The term "emergency public information" reflects an understanding that public information during an emergency might differ from normal, day-to-day, public information provided to citizens by the government. In the event of a major disaster or emergency, this often means the coordination, development, and delivery of time-critical, lifesaving information to all potentially affected people. For this reason, public officials and government spokespersons often find that this aspect of their jobs is different in an emergency environment, and more important. In a climate of heightened uncertainty and concern, the timing and content of official statements can save lives, the media and general public are likely to scrutinize statements more, and some statements could incur heightened political liabilities.

> "Communicating in a major emergency situation, particularly a terrorist event, is very different from communicating about routine matters or smaller crises...In ordinary circumstances, your role is to provide the public with information. This role does not change during the extraordinary time of an emergency, such as a terrorist attack, but the stakes are much higher."
>
> *Incident Communications Emergency Reference: A Guide for Communications Professionals*

This section examines the use of policies, procedures, and mechanisms employed by participating FSL governmental departments and agencies and/or non-governmental organizations (NGOs) to communicate with the public in response to potential and actual INS in the course of the T3 FSE. This included governmental interaction with media outlets—Virtual News Network (VNN) live television; VNN.com website; and notional radio, print, and other media outlets (press releases). This also included other means of reaching the public with official lifesaving information, including the use of hotlines, call centers, agency website postings, e-mails, blast faxes, flyers, and reverse 911 to telephones and cell phones of citizens. All of the National Response Plan (NRP)-related coordination structures and mechanisms used by FSL governmental agencies during the exercise to develop and deliver messages to the public are also examined.[9]

[9] Transcript-level notes for VNN; press releases; VNN.com archives; follow-up discussions with media Simulation Cell (SIMCELL), VNN, and public affairs officials; and the T3 FSE searchable reconstruction database, which incorporates agency situation reports and logs and data collector/analyst and media SIMCELL logs served as inputs to this analysis.

B. Background

Public affairs officials have long noted that, with terrorism, a local attack can be national in impact and in importance. Public information emerged as one of the most frequently referenced issues in the T2 exercise cycle, as well as in the Senior Official Exercises (SOEs) under the National Exercise Program (NEP).

C. Accomplishments since the T2 FSE

The Department of Homeland Security (DHS) has led the continued development of a national public affairs framework since the T2 FSE. Major accomplishments in this regard include:

- the development and release of the NRP Incident Communications Emergency Policy and Procedures (ICEPP), comprised of the Emergency Support Function (ESF) #15 (External Affairs) and Public Affairs Support Annexes;
- the development of the associated Incident Communications Emergency Reference (ICER), which provides tactical guidance to Federal incident communications professionals; and
- active participation in the NEP-sponsored SOE process to bring visibility to critical incident communications issues.

D. Development and Release of NRP ICEPP

The ESF #15 Annex to the NRP addresses emergency public information and protective action guidance, media and community relations, congressional and Indian affairs, and tribal/insular affairs. It states that it provides the resources, mechanisms, and structure to implement the NRP ICEPP. The DHS Assistant Secretary for Public Affairs, in coordination with the NRCC, directs activation and implementation of ESF #15. Resources available to support ESF #15 include the Emergency Alert System and other emergency broadcast systems. A DHS/Emergency Preparedness and Response (EPR)/FEMA Public Affairs staff member represents ESF #15 functions at the NRCC. During an INS, ESF #15 activities are coordinated by Office of Public Affairs (OPA) representatives of the Homeland Security Operations Center (HSOC) and IIMG.

The Public Affairs Support Annex outlines the policies and procedures to "rapidly mobilize Federal assets to prepare and deliver coordinated and sustained messages to the public in response to Incidents of National Significance." It describes the entities and mechanisms involved in incident communications coordination, such as Joint Information Centers (JICs). It also describes the types of incident communications coordination that occur at various stages (prevention, preparedness, response, and recovery) of an INS. It

provides a checklist of the types of activities that should be conducted in the first hour, day, and week of a response to an INS.[10]

Together, the ESF #15 and the Public Affairs Support Annexes outline organizational roles, tools, and mechanisms available to support incident communications coordination, generally describe these resources and tools, and provide general message development considerations. They do not provide guidance on how these roles, tools, or mechanisms could or should be used by FSL entities to coordinate a consistent message.

E. Development of ICER

The ICER was developed to provide public affairs officials with "basic information on homeland security public affairs organization, communications response activity for an incident and contact information."[11] It introduces readers to the Homeland Security Advisory System, provides guidance for what to do before an incident (such as "Develop a Public Affairs Action Plan," "Develop relationships with responders in your area," and "Train your leadership on your Action Plan," etc). It outlines "message components" such as "expression of empathy" and "clarification regarding steps being taken to obtain more facts," etc. It provides a "First 48 Hours Checklist," which outlines steps such as notification of leadership, "Contact local, State and Federal partners now," and "Connect with the JIC." It encourages early outreach through a basic formal statement to the media and "partners" and encourages sharing "pre-cleared facts," as well as what steps the agency is taking to support the emergency with the public. Finally, it provides a State Public Affairs Contact List and numerous templates (e.g., press release template). It focuses on what steps should be taken to conduct and coordinate public affairs, with less emphasis on how coordination should occur.

F. Participation in the SOE Process

Four discussion-oriented tabletop exercises (TTXs) were conducted for senior Federal officials prior to the T3 FSE. These TTXs covered a range of topics and scenarios. Two exercises, SOEs 05-2 and 05-3, used the T3 FSE scenario. The purpose of the SOEs was to prepare top officials for participation in the T3 FSE.[12]

Since the T2 FSE, DHS has also:

- Implemented the DHS Office of Public Affairs Coordination Center, or "Ready Room," which serves as the public affairs "nerve center" in an emergency. There, DHS officials staff the National Incident Communications Conference Line (NICCL), as well as telephone lines dedicated to communications with the State JICs and with DHS intra-agency, international, and special media. The NICCL is

[10] Table 1 of the NRP Public Affairs Support Annex, Interagency Incident Communications Planning Guide.
[11] ICER Introduction Letter, Susan Neely, DHS Assistant Secretary for Public Affairs.
[12] SOE 05-2 used the bioterrorism scenario and 05-3 used a combined biological and chemical attack scenario.

a standing conference line maintained by DHS Public Affairs as the primary means for interagency incident communications information sharing during an INS.[13] In the Ready Room, DHS personnel also check and record facts, monitor the media, develop talking points, support speech writing, and provide support to other functions as needed.

- Initiated and finalized an international agreement between the United States and the governments of Canada and the United Kingdom (UK), pledging mutual support to coordinated incident communications efforts in emergencies. DHS held two pre-FSE exercises with incident communications offices from Canada (with some limited UK participation) in order to strengthen and rehearse the logistics supporting this aspect of international collaboration.
- Created the Incident Management Public Affairs Coordination Committee. The White House Communications Office and Homeland Security Council (HSC) oversee this committee, which is coordinated by DHS OPA and is comprised of representatives from 15 Federal departments and 12 Federal agencies/independent bureaus. It meets quarterly to exchange lessons learned and to promote teamwork within the public affairs community for managing incident communications.
- Actively participated in the Public Affairs Working Group, which involved the FSL public affairs offices that participated in the T3 FSE.

G. Reconstruction

This reconstruction focuses on how the public affairs design elements facilitated exercising incident communications.

The DHS-sponsored TOPOFF exercise series offers FSL and NGO top officials and public affairs professionals the most challenging and realistic environment of any exercise. The T3 FSE incorporated three elements for multi-dimensional incident communications play—*VNN Live* simulated television coverage, VNN.com simulated electronic print media, and a robust media simulation cell. Together, these entities made more than 1,000 phone calls over five days to nearly 340 public affairs participants. These elements provided top officials and their supporting public affairs staffs with a challenging and realistic opportunity to gain experience interacting with the media during an unfolding disaster or emergency.[14]

[13] The NICCL is not a tool for coordinating Federal response operations.

[14] Nearly 340 public affairs participants registered to be "pushed" by simulated media. This does not include additional public affairs participants with support roles.

1. VNN Live

VNN Live provided more than 35 hours of original and live coverage during the course of the exercise. It employed five news studios with nationally known television anchors and experienced reporters in each venue who challenged spokespersons in the exercise as they would in a real event. VNN conducted more than 140 live interviews and 13 press conferences during the exercise.[15] The VNN news desks and reporters incorporated department/agency (D/A) press releases, stories that were posted on VNN.com, and news gathered via the simulated wire services into their interviews with spokespersons, much as would occur in the real world.

2. VNN.com

VNN.com simulated print media through an electronic website that was available to organizations participating in the T3 FSE. Nine news editors located across the five exercise venues posted more than 200 articles throughout the FSE based on information gathered through D/A press releases, press conferences, and the media simulation cell. A total of 48 FSL and private sector organizations posted more than 130 public messages on VNN.com.[16] VNN.com also included articles based on interviews with incident communications participants. The website streamed 35 hours of *VNN Live* video over the course of the exercise, providing a wider reach for *VNN Live* coverage. More than 8,000 individual users logged onto VNN.com during the exercise, providing an indication of the widespread use of this media outlet.

3. Media SIMCELL

Acting as a news wire service, five media simulators located in the three domestic venues supplemented *VNN Live* and VNN.com by calling FSL Public Information Officers (PIOs) to ask questions and conduct telephone interviews. The intent of the Media SIMCELL was to put "media pressure" on the entire incident communications system in accordance with the objectives of participating D/As. It reached many players who would

[15] Source: T3 VNN Broadcast Log.
[16] Source: T3 PIO Play Summary Report.

not have otherwise been challenged by incoming calls from reporters.[17] The Media SIMCELL also followed up on stories that played on *VNN Live* and, in some cases, fed news stories to the VNN News Desk operation based on the information it gathered, much as a wire service would do.

H. Consequence

DHS has initiated a number of initiatives designed to facilitate better coordination of public messages among FSL and international governmental agencies, the private sector, and NGOs. Progress has been made in the provision of guidance (the NRP ICEPP and ICER), tools (NICCL), and other resources (regular dissemination of DHS public affairs guidance in an incident) since T2. Future efforts should seek to further define concepts for how these tools can be better used to promote more consistent messages by FSL governmental agencies. Particular emphasis should be placed on the development of an efficient Joint Information System (JIS) concept.

The provision of early, unified, and accurate lifesaving protective action guidance by top officials in time-sensitive scenarios, such as those examined in the T3 FSE, should be a top priority in public affairs initiatives. This represents a low-cost, yet highly effective, method that could substantially reduce the number of casualties in these types of incidents. Federal officials (in addition to State and local officials) may need to be prepared to provide comprehensive and specific protective action guidance to the public in the event of an attack with widespread implications, such as a bioterrorism attack using a contagious agent.

I. Analysis

Since the T2 FSE, substantial progress has been made in creating coordination mechanisms to promote the release of a more consistent message by FSL governmental agencies. There was no overarching incident communications framework or guidance during the timeframe of the T2 FSE, as DHS had only recently been created. For this reason, incident communications play in that exercise could only he examined in terms of outcomes based on general incident communications principles—how consistent, accurate, and timely were the messages provided to the public by FSL agencies across the various phases of the incident.

The NRP and its annexes, the National Incident Management System (NIMS), and the ICER allow a framework for examination of how incident communications were executed. The T3 FSE is still examined in the context of the outcomes—incident communications principles of consistent, accurate, and timely messages still apply. However, it is recognized that no one agency can guarantee these outcomes across the range of independent authorities and stakeholders delivering messages to the public during an emergency, even if it is taking as many steps as it can to promote coordination.

[17] *VNN Live* and VNN.com components focused primarily on top officials and were charged with developing and disseminating news stories. They were not staffed to physically visit or call all PIOs who would be operating behind the scenes.

Therefore, the focus of this analysis is on examining the current incident communications framework as documented in the NRP, NIMS, and ICER in the context of the FSE to determine the relative strengths or weaknesses of this framework when implemented and to determine whether and what potential modifications may need to be considered to improve the framework or its implementation. Also, the purpose of this analysis is to provide a wide-angle perspective on the overall messages provided to the public, the potential implications of those messages, and the degree to which the delivery of the messages would have enhanced or detracted from the credibility of the spokespeople as a key element in a successful public notification campaign.

1. Tools Implemented After T2 FSE and Used in T3

The T3 FSE served as a "proof of concept" opportunity to introduce, test, and/or refine new DHS-sponsored public information coordination mechanisms, such as the NICCL and Ready Room. Prior to the exercise, the DHS OPA released informal preparatory guidance via e-mail to agencies participating in the FSE to further raise awareness of the key incident communications support tools that would be available in the exercise and to outline the purpose and usage protocols for the NICCL.[18] It summarized the lead agencies for the scenario, outlined DHS Public Affairs products that would be prepared and distributed (such as Public Affairs News Updates, Public Affairs Guidance, NICCL updates, and web products), and outlined DHS incident communications contact information. It requested that Federal agencies provide courtesy copies of press releases and encouraged "wide distribution." This helped build awareness of the available coordination tools and encouraged mutual awareness of respective messages that would be disseminated by Federal agencies.

As designed, the NICCL served as the primary tool for interagency public affairs coordination during the exercise. The Federal Core Group convened on a regular basis throughout the exercise via NICCL teleconferences. Data suggest that, using the NICCL, the group coordinated agreements that outlined which agencies would address certain facts and outlined the generally consistent messages that Federal D/A spokespeople would relay to the public regarding Federal assistance to the affected areas, national preparations, protective measures, and Federal law enforcement activities.

DHS provided informational updates up to 10 times a day on this conference call forum and published summaries for tracking purposes. DHS established a fairly regular morning and evening update cycle and announced other periodic updates via e-mail as well as on this line as needed. It was staffed 24/7 so that even outside of the formal, scheduled "updates," callers could obtain information from a DHS public affairs official. DHS disseminated a written "NICCL Update" over e-mail after each of these updates to provide a record of the discussion.

DHS also regularly disseminated Public Affairs Guidance (approximately four times a day and hourly in some cases) to provide the activated incident communications staffs at

[18] E-mail from Jeff Karonis, DHS Public Affairs, to interagency public affairs offices, dated April 1, 2005.

all levels with periodic updates on the evolving facts as DHS understood them. This guidance was intended to support a common information baseline across FSL organizations in a rapidly evolving event and represented a formal, written means of transmitting information. However, because the updates were rather general and did not contain details on specific public message content, it was not clear whether they were effective in promoting a consistent message.

FSL D/As were inundated with general informational updates from other agencies who distributed regular situation reports, including other offices in DHS. The DHS OPA observed that, in the future, it may be more effective to send out sets of more specific "message points" rather than general status updates. The Public Affairs Guidance has the potential to contribute to more consistent messaging. Integrating it with NICCL updates may he another way to further streamline DHS incident communications support to the interagency and enhance its perceived value by establishing it as a definitive "go-to" product during an incident.

More consideration should he given to further refining and formalizing the business processes that define how the new incident communications coordination tools are used. A concept of operations document could be useful to reinforce awareness of these tools and to outline how they can be even better used by Federal agencies (as well as State and local governments) as a hackbone to a JIS to promote a more consistent message.[19] Also, it could be useful to expand the NICCL forum to a secure web-based collahoration environment (e.g., using technology similar to that of WebEx[20]) to enable participants to hear and see updates. Collaboratively maintaining a written file that is periodically updated by participating agencies, and in which facts are mutually vetted, could contribute further to a common operational picture.

2. Agencies Adhered to the NRP and ICER Guidance

a. Public Affairs Mechanisms

By using a variety of means to reach the public, making joint public statements, and actively working to control rumors, agencies adhered to the NRP and ICER Guidance. FSL D/As employed many systems and tools to reach the public. Both New Jersey and Connecticut deployed central information hotlines and websites, which served as cornerstones of multifaceted public information campaigns.[21] Both States activated their hotlines on April 4. Connecticut fielded questions from individuals throughout the first day. New Jersey kept its hotline and associated e-mail operations open all week to receive and respond to inquiries from the public. Both hotlines provided multilingual and

[19] See related issue and Course of Action (COA) on JICs.

[20] WebEx is an integrated collaborative meeting and audio/visual teleconferencing services provider. More information can be found at http://www.webex.com and http://www.pcmag.com/article2/0,1759,1787545,00.asp.

[21] The NJ telephone hotline (866-234-0964) was announced via a press release at 13:58 on April 4. The CT hotline (211) was announced via a 17:00 press release on April 4.

text telephone (TTY) services. The telephone numbers were regularly included on press releases produced by the State and, in some cases, local governments.

FSL D/As also provided informational websites and phone numbers, including dedicated resources for mental health support. Some people may have found the volume of public information telephone numbers overwhelming or difficult to track.[22] However, the State hotline numbers and the American Red Cross's contact information were the ones most frequently presented. Maintaining and publicizing a centralized list of the various numbers would be useful.[23]

b. Message Considerations

Generally speaking, the public messages from top FSL officials satisfied the following guidelines offered in the ICER:

- Expression of empathy
- Clarification of facts
- What is not known
- Steps being taken to obtain more facts
- Call to action (giving the public things to do)
- Referrals (where to go for more information)

In press releases and via VNN, Federal officials provided regular and generally consistent updates regarding Federal assistance to the response efforts in New Jersey and Connecticut. DHS, Department of Health and Human Services (HHS), and Centers for Disease Control and Prevention (CDC) officials consistently directed the public to listen to State and local government officials for protective action guidance and specific informational updates. This is generally consistent with the NRP, which states that:

> *State, local and tribal authorities take a lead incident communications role in their respective jurisdictions, while the Federal core group coordinates communications covering Federal assistance to the affected areas, FSL D/A response, national preparations, protective measures and Federal law enforcement activities.*

[22] Sampling of informational numbers, not including websites, provided during the T3 FSE: Connecticut: Hotline (211); Family Assistance Center (800-438-4636). Interagency: American Red Cross (866-446-2600 and 999-867-6333); Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) (888-ATF-BOMB); CDC (800-CDC-INFO); HHS information (866-509-8000); Federal Bureau of Investigation (FBI) (800-FBI-TIPS); Will Backus Disaster Information Line (866-425-3855). New Jersey: Department of Health and Senior Services (DHSS) Hotline (866-234-0964, 609-633-2083, and 866-555-5555); Medical Examiner's Office (201-599-6097 or 292-6468); Victim Hotline (609-292-6468); Mental Health Hotline (800-294-4357); TTY (973-571-1898). Local health departments provided individual numbers.

[23] The *Wall Street Journal* and *Washington Post* (among other publications) published consolidated lists of contact information for relief organizations in the aftermath of the December 2004 tsunami.

New Jersey provided some strong public health and law enforcement spokespeople early on, in addition to the Governor, who likely would have helped establish the credibility of government leaders. They provided a comprehensive informational presence regarding the unfolding crisis. The State Epidemiologist established himself early on as a credible spokesperson regarding the unfolding health crisis and made regular and frequent appearances on VNN. The Superintendent of NJ State Police provided authoritative messages regarding law enforcement updates early on as well.

c. Joint Statements

There were also numerous examples of joint appearances and public statements by various combinations of FSL officials, which helped to convey a coordinated response to the public. The Secretaries of DHS and HHS provided joint statements on April 4 at 12:20 and then again at 17:00. State officials in New Jersey and Connecticut also conducted some joint interviews. On April 4 at 15:00 and April 5 at 14:00, the Governor of New Jersey, Commissioner of DHSS, and State Epidemiologist made a joint appearance on VNN. Also in New Jersey, at 13:20 on April 5, the Deputy Superintendent of the NJ State Police appeared with the State Epidemiologist. In Connecticut, the Governor and PFO made two joint appearances and were joined the second time by the FBI Special Agent in Charge (SAC) overseeing the investigation. Senior CT State departmental officials appeared together twice on April 6. Also in Connecticut, key local officials appeared together on VNN. Although there were still problems in the consistency of messages provided by these officials across FSL levels, joint appearances represent one way to convey that the government is working together for a unified response.

d. Rumor-Control Efforts

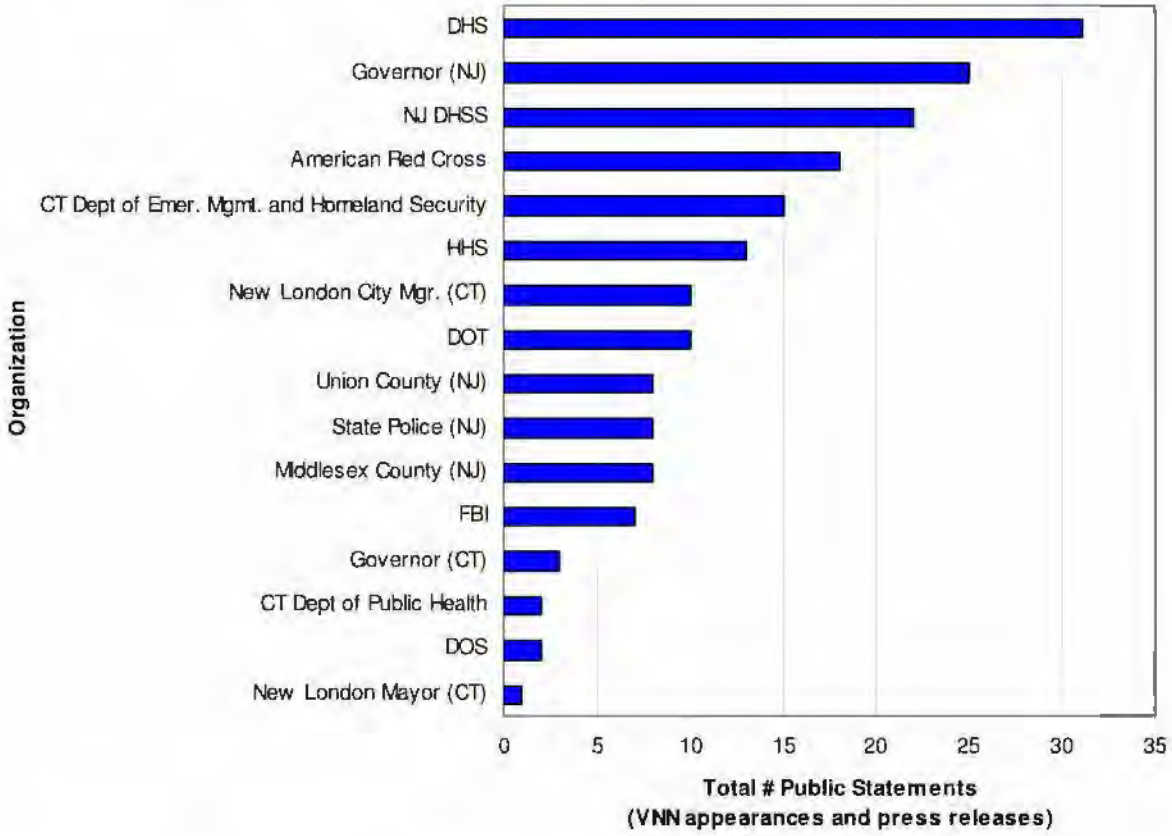
Throughout the T3 FSE, Federal and State D/As acted to correct misinformation or rumors reported through media channels. DHS staffed its Ready Room with a dedicated media monitor to assist with rumor control and to reconcile instances of conflicting information. For example, on April 7, the HSC, in coordination with HHS and CDC, released talking points to correct erroneous statements by other spokespeople referring to the availability of a "vaccine" for plague. In New Jersey, DHSS made "clarifying VNN rumors" one of its top priorities. The State PIO in Connecticut used its 211 hotline to combat rumors. The CT Department of Environmental Protection (DEP) released a press release the afternoon of April 6 to specifically clarify that a rumor "regarding a chemical spill that allegedly occurred in the area of the explosion in New London" was false.

3. Distribution of Domestic Incident Communications Spokespersons/Agencies

The distribution of domestic incident communications spokespersons/agencies reflected NRP ICEPP guidance. Nearly 50 FSL agencies, private sector entities, and NGOs provided messages to the public during the T3 FSE. Of these organizations, DHS provided the most messages in the form of VNN appearances by the Secretary and other officials and press releases reported on by VNN.com reporters. The American Red Cross

and HHS were the next most-visible Federal agencies, followed by the Department of Transportation (DOT) and FBI. Such visibility was consistent with the decisions and response activities occurring at the Federal level. Figure II-1 depicts the total number of public messages made or issued by primary spokesagencies on VNN or via press releases.[24] Figure II-2 shows the total number of VNN appearances by a spokesperson or agency. Figure II-3 identifies the total number of press releases issued by participating domestic organizations.

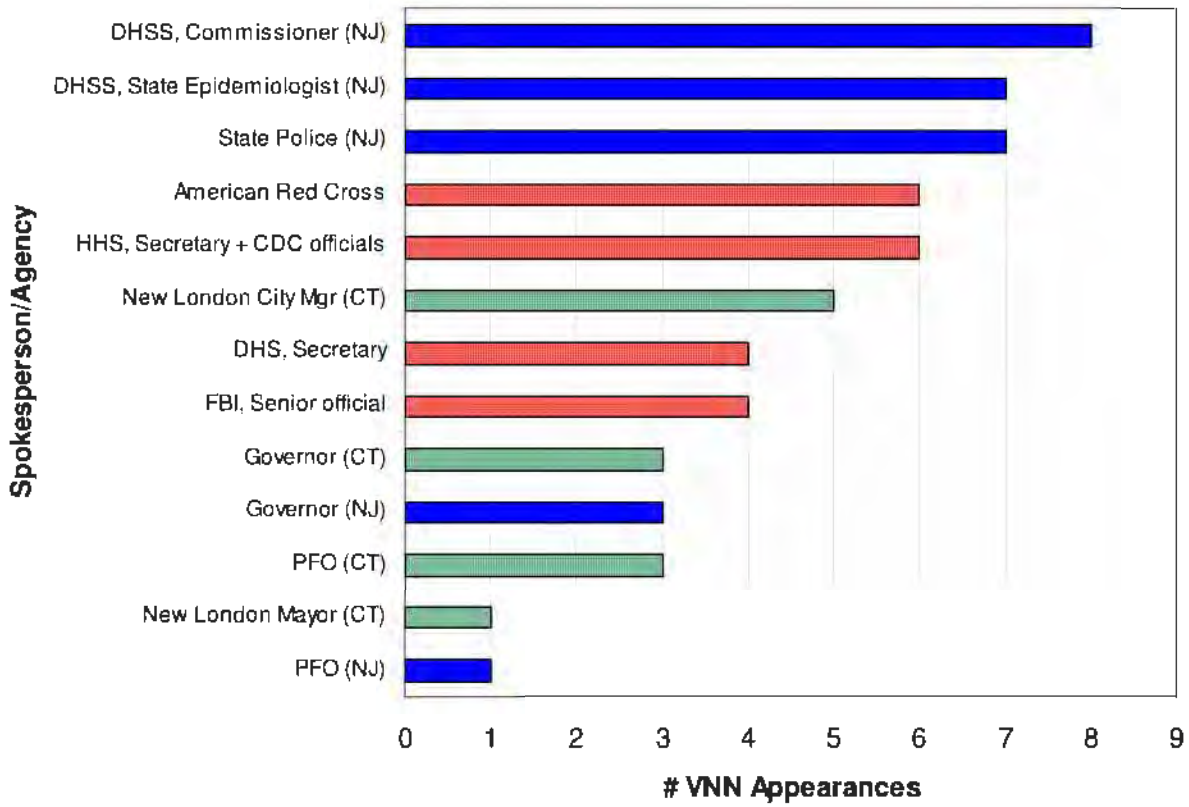
Figure II-1. Overall Incident Communications (VNN and Press Releases)



In New Jersey, the Governor and top DHSS officials led incident communications in the early stages of the plague outbreak, as evidenced by the number of their VNN appearances and press releases. Their leadership was supplemented by widespread press release activity by localities after the decision was made to execute a statewide prophylaxis strategy. Middlesex County, one of the two hardest hit counties in the State, issued press releases that were especially thorough and informative.

[24] Note that only primary NRP-related agencies are reflected in Figure II-1. Also, only Union and Middlesex Counties in New Jersey (the two hardest hit counties) are included in the summary figures, because most other county press releases were largely focused on providing information or updates regarding points of dispensing (PODs).

Figure II-2. VNN Appearances by Primary Spokesagencies



It should be noted that the incident communications approach to the prophylaxis strategy in New Jersey in T3 was more State-centric than that of Illinois during the T2 FSE. In that exercise, the city of Chicago and the surrounding "collar" counties assumed more localized control of incident communications when they issued joint press releases with instructions to the puhlic on PODs.[25] This resulted in more consistent messages regarding PODs than occurred in T3, which will be discussed in a later section. However, joint press releases would have been harder to coordinate in New Jersey due to the participation of a large number of counties.

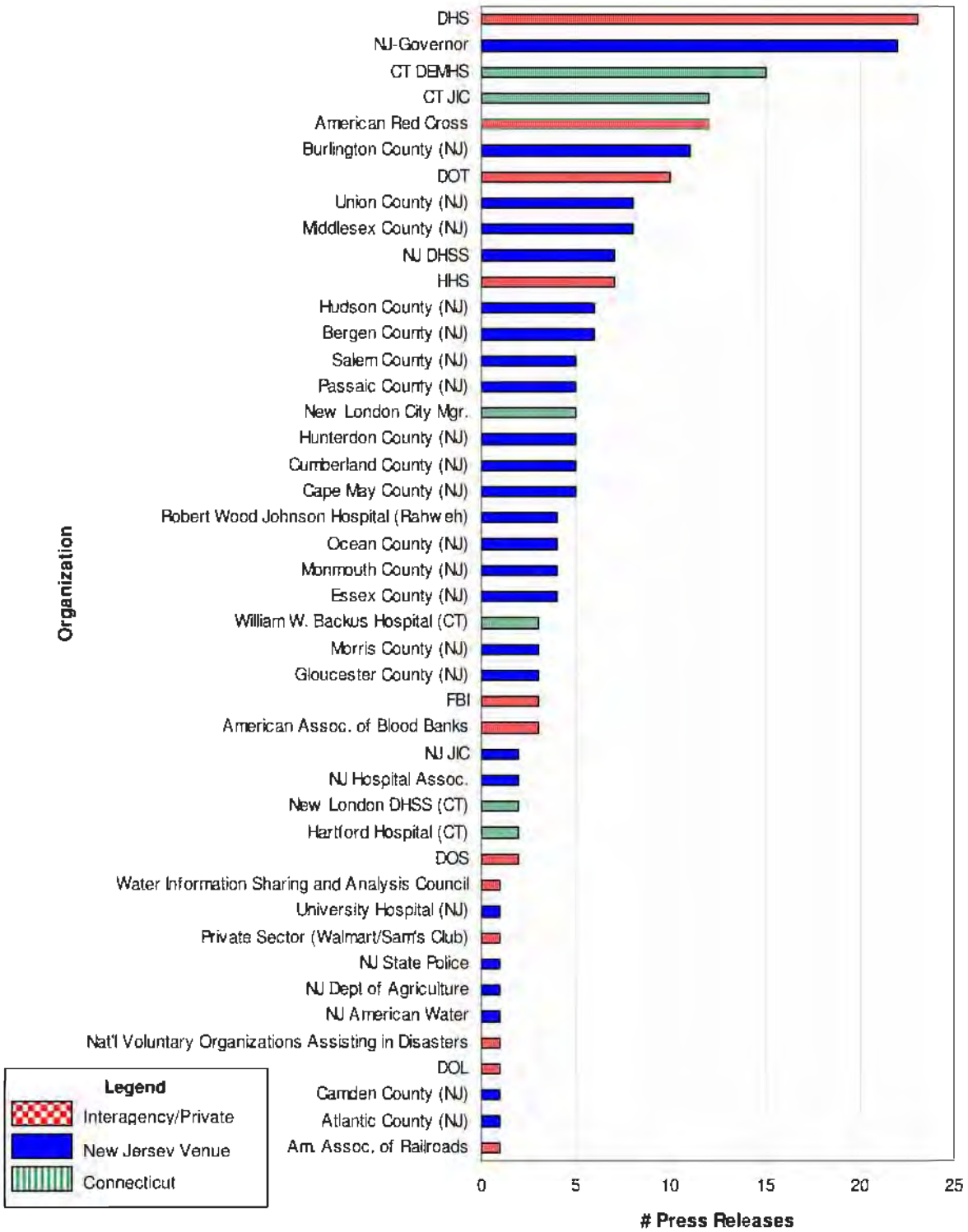
In Connecticut, the Department of Emergency Management and Homeland Security (DOEMHS) provided the most public messages overall, followed closely by the JIC, which was more active than its counterpart in New Jersey.[26] Top local officials, namely the New London City Manager and Mayor and the Governor, led televised public messaging. Health officials were less visible in televised messaging in Connecticut.

The differences in the approaches in New Jersey and Connecticut likely reflected the differing implications of the incidents—a distributed biological attack in New Jersey versus a localized explosion and chemical attack in Connecticut. There were instances of

[25] T2 FSE After-Action Report.
[26] See later section on the JICs.

inconsistent messages among organizations within each venue, particularly regarding protective action guidance, which will be discussed in a later section. However, the distribution of public messages overall reflects NRP incident communications guidance and indicates that the guidance is flexible enough to accommodate varying implementations.

Figure II-3. Press Releases Issued



4. Top Officials' Difficulty in Providing Protective Action Guidance to the Public

Despite the changes implemented since the T2 FSE, top officials in T3 still were not able to provide timely, accurate, and consistent lifesaving protective guidance to the public. FSL top officials in both venues did not provide a clear and consistent message on recommended protective actions for the public to reduce risk in the early hours and days after the attacks. In many instances, this information was provided only when asked for by a reporter. The inconsistencies and delays in such guidance could have had significant implications on the number of casualties in both venues.[27] Early and consistent guidance could minimize the exposure rate and/or degree of exposure to WMD agents.

a. New Jersey

By late morning on April 4, a presumptive diagnosis of plague was confirmed, and a bioterrorism attack was suspected. The agent suspected to be the cause of the first fatalities would have been released from one to six (or more) days earlier.[28] This would have heightened the criticality of a swift and uniform response, at least in terms of preliminary protective action guidance. Officials did not appear to convey the potential magnitude of risk that could be associated with an intentional, covert terrorist release of *Yersinia pestis* in the first day. This could have been out of a desire to not unduly alarm the public while public health strategies and resources were being mobilized. But, officials may need to assess whether the tradeoffs associated with this approach are worth the risks.

Federal officials were uniform in directing the public to consult State and local officials about specific protective action guidance. This is consistent with the NRP, which recognizes the leadership of State and local governments in directing the response to terrorist attacks. But, the potential for national casualties in the event of a contagious biological attack may call into question whether Federal officials, especially in the early hours, may need to also provide specific protective action guidance at the national level. The public, especially those in potentially at-risk areas that are not at the epicenter of an outbreak where State and local guidance may be more plentiful, may look to Federal spokespersons for uniform protective action guidance.

[27] The emphasis here is both on inconsistencies and delays, rather than just inconsistencies in messaging, because effective response to the two scenarios in T3 is so time-sensitive.

[28] This range is based on the incubation period for *Yersinia pestis*. The release time could not be precisely estimated based on a single case.

Some examples of inconsistencies and delays in protective action guidance in New Jersey are provided below to illustrate these points.

i. Criticality of the 24-hour Timeframe for Taking Antibiotics after the Development of Symptoms

Initial statements by State officials on VNN did not communicate the criticality of the 24-hour timeframe for receiving antibiotic treatment. On the afternoon of April 4, the NJ Governor mentioned that plague is treatable with antibiotics, but did not specify the criticality of treatment within 24 hours of the onset of symptoms. The DHSS Commissioner noted on VNN on April 4 that plague "has a high fatality rate," but did not clarify that this is true only if someone who is infected does not receive antibiotic intervention within 24 hours from the onset of symptoms, and that otherwise plague is highly treatable. By April 5, suhsequent press releases from State and local D/As did begin to emphasize that "early" antibiotic treatment was critical.[29]

ii. Inconsistent Respiratory Precautions

Also, FSL officials did not widely or uniformly disseminate disease prevention information, such as avoiding symptomatic individuals or wearing surgical masks, to the public on the first day. The Deputy Superintendent for the Homeland Security Branch of the NJ State Police, when asked in a VNN interview on April 4 at 15:10, stated that her office was "staying six feet away from other people." Although this was good protective action guidance, it was not widely provided by other State and local officials or mentioned by other officials on VNN on the first day.[30] In a real event, such early guidance could save lives and reduce the wave of secondary exposures. Due to the potential initial exposure time frame, this could have been critical information for some people.

iii. Uncoordinated and Unnecessary Precautions

Some organizations provided protective action guidance that proved to be unnecessary and was not coordinated through State health officials. This could have undermined the credibility of officials providing critical guidance requiring public cooperation. In one example, the NJ American Water Company issued a "boil water advisory" the evening of April 4 which was not coordinated with State health officials. The DEP initially stated that "a potential or actual threat to the quality of the water being provided currently exists." The State Epidemiologist noted in an interview on VNN on April 5 that plague is not transmissible from water and that he was unclear on the rationale for this order, but that it was "not due to plague." The NJ American Water Company ended its boil water advisory at noon on April 6, describing it as a precautionary measure due to staff shortages resulting from the emergency. The Governor issued a press release that day

[29] DHSS issued a press release on April 4 at 21:56 referencing the criticality of the 24-hour window for receiving antibiotics; however, it appeared in the 33rd sentence of the press release after updates on casualty figures, POD openings, and general information regarding plague.

[30] Union County mentioned this in a press release on April 5.

stating that there is "no threat of disease transmission from the State's water supply." In this same statement, DHSS reaffirmed that there was no need to boil tap water. These inconsistent messages could have triggered a degree of unnecessary concern among the public.

iv. Uncoordinated POD Guidance

Initial public guidance relating to the PODs and prophylactic treatment was mixed and could have had negative implications on disease spread. First, VNN anchors reported receiving conflicting information from State officials on whether and when initial PODs would be opened the morning of April 5. Officials initially instructed members of the public to report to PODs if they thought they were in the initial exposure area or they thought they were exposed to someone who was. No specific guidance was given as to how a person would know if he or she were in the exposed area (it was not specified) or exposed to someone who was. Initially, VNN reported a strategy of triaging people who were in-processing at the PODs by creating separate lines for symptomatic and non-symptomatic persons. This approach was changed the next day (at which point, symptomatic people were instructed to report to a hospital rather than a POD), but could potentially have exposed people to plague on the first day. Later, this guidance evolved—reflecting a decision by the State to conduct statewide prophylaxis rather than a targeted campaign—and everyone in the State was instructed to go to a POD unless they were symptomatic, in which case they were to report to a hospital.

There were also inconsistencies among local jurisdictions in messages relating to the PODs organized by the State.[31] Some mentioned the need to arrive with a completed registration form, whereas others did not. In an April 6 press release, Cape May County officials mentioned that the weight for children less than 100 pounds needed to be correctly recorded on the form, whereas other counties did not specifically mention this. A few counties reminded residents in press releases that if they did not speak English, they would need to bring a translator.[32] How this message would have been conveyed to those populations was not clear. Gloucester County noted in a press release issued on April 6 that if you have not been exposed and are not ill, "the best thing you can do is stay home." However, no specific guidance was provided as to how to know whether you had been exposed. Also, by this time the State had decided to implement statewide prophylaxis.

Throughput at the PODs was a critical variable in the State's ability to successfully implement its POD plan within the 48-hour timeframe it had established. Incomplete guidance to the public could have negatively affected throughput if people arrived unprepared at the PODs. State governments should develop complementary incident communications plans for Strategic National Stockpile (SNS) distribution and should work closely with all affected localities to ensure that the guidance to the public provided by localities is clear and comprehensive.

[31] See also "Strategic National Stockpile and Point of Dispensing."
[32] Cumberland and Salem Departments of Health and Somerset County, April 6 press releases.

b. Connecticut

In Connecticut, similar problems arose with the swift, accurate, and consistent provision of potentially lifesaving guidance. Delays in issuing decontamination guidance and cross-contamination warnings could have exposed more people to the agent, worsened the severity of symptoms, or contributed to the overflow of people at hospitals. Some examples of inconsistencies and delays in protective action guidance in Connecticut are provided below to illustrate these points.

i. Delayed Protective Action Guidance

An explosion was reported at the waterfront in New London around 13:20 on April 4. Data suggest first responders almost immediately suspected a chemical agent that could be sulfur mustard. VNN.com reported that, shortly after the blast, State hazardous materials (HAZMAT) workers at the city pier suspected that a chemical agent had been dispersed in the air. Rescue workers told reporters that the victims had been complaining of blistering skin rashes and trouble breathing—common symptoms of mustard exposure. The supervising emergency response coordinator with the State DEP stated, "We were immediately told of the skin blistering by the incident commander, and our workers put on their protective gear." When asked by an interviewer about live footage depicting first responders in personal protective equipment, the New London City Manager first mentioned the word "contamination" on VNN at 14:24 on April 4. The CT Governor, accompanied by the New London Mayor, mentioned the potential use of an unspecified "chemical" in her first press conference to address the attacks at 14:40. Two hours later, the New London City Manager confirmed on VNN the presence of sulfur mustard and the suspicion that it might have been released prior to the explosion, extending both the time window of exposure and the size of the potentially exposed population.

The CDC Fact Sheet on sulfur mustard indicates that the lack of immediate, widespread, self-decontamination guidance and cross-contamination warnings in the early hours of an attack could have had dramatic implications on the severity of casualties.[33] It indicates that symptoms for the skin, eyes, and respiratory tract can begin as early as one to two hours after severe exposure, increasing the criticality of swift protective action guidance within the first day. It further states that "getting the sulfur mustard off as soon as possible after exposure is the only effective way to prevent or decrease tissue damage to the body." Yet, no specific protective action guidance was offered by State and local officials in these early hours regarding decontamination procedures, no warnings were issued in terms of potential cross-contamination, and no widespread emergency bulletins were issued stating that people at the waterfront during, as well as prior to, the explosion may have been exposed.

[33] http://www.bt.cdc.gov/agent/sulfurmustard/basics/facts.asp

ii. Inconsistent Decontamination/Cross-Contamination Guidance

Officials were also inconsistent in alerting the public to the risks of cross-contamination (which may have put more people at risk) and in issuing decontamination guidance (which may have worsened the severity of the attacks and contributed to the ensuing hospital overflow problems). Shortly after this, the New London Mayor instructed people at the waterfront to "walk away from the waterfront and walk home" if people could not drive or obtain a ride home. The guidance to walk home or drive home would have exposed these individuals to greater risk as the chemical (later reported to be odorless) would have had more time to penetrate clothing and they would have unwittingly cross-contaminated other surfaces such as car seats or their homes. It was not until 16:40 on April 6 that an official (the Commissioner of the Department of Public Health) stated that sulfur mustard was "passable" from one person to another. At this time he also advised that "if you have shoes or clothing that may have contacted outside surfaces, keep [them] in [a] plastic bag outside."

The Secretary of Homeland Security instructed people in his 17:00 press conference on April 4 to "among other things, use soap and water to wash your hands if you were in the vicinity" of New London, but did not mention any other specific guidance. A VNN.com story early in the morning on April 5 quoted a New London City Police sergeant who stated that 911 dispatchers were telling callers that, if they thought they had been contaminated by mustard, "they should shower with soap and water and put clean clothes on before going to the nearest hospital emergency room." Guidance to wash with soap and water contrasted with the CDC Fact Sheet, which states that only "plain water" should be used to wash contaminated areas. Also, the guidance to report to a hospital after showering was unnecessary (showering with water was an effective decontamination procedure) and seemed to contradict the State's efforts to stem the flow of people to hospitals, which were reportedly overrun by this time.

Finally, it was not clear why the Secretary of Homeland Security highlighted this guidance, but did not mention other personal protective action guidance. Federal incident communications experts should determine whether it is appropriate for Federal spokespersons, in addition to leaders of affected States/localities, to issue such guidance. If they determine that such guidance is appropriate at this level (as mentioned earlier in the case of a biological attack), they should prepare officials to provide comprehensive guidance.

iii. Inconsistent Information on Water Risks

There were also some inconsistencies in some of the information provided on sulfur mustard which could have undermined the credibility of officials and caused some confusion for the public. In one example, the Public Health Commissioner stated (on April 7) that sulfur mustard "does not affect the water supply," and that the water supply was "secure assuming it is city water." But, the CDC Fact Sheet states that "people can be exposed by drinking the contaminated water." Also, officials were reporting that environmental testing was being done in the water, implying some potential for

contamination. Yet, other agencies were stating that water neutralized the sulfur mustard agent.[34] A health official also stated that this agent "does not cause disease." However, the CDC Fact Sheet states that it can cause chronic respiratory disease. Although this official was likely attempting to contrast this with the contagious plague epidemic, it highlights the importance of clear statements.

iv. Inconsistent Shelter-in-Place Instructions

Finally, officials did not provide comprehensive or consistent protective action guidance in Connecticut regarding the shelter-in-place order issued on the afternoon of April 4 for the New London area. First, the Governor mentioned closing all windows and doors and remaining on an upper floor without windows, as chemical mustard is heavier than air and will settle. An American Red Cross official later stated that windows and doors should be sealed with duct tape and ventilation turned off, stating that oxygen deprivation is "usually" not a problem within the (unspecified) time frames of such orders. The VNN lead anchor later strongly advised against such procedures, noting that it could be dangerous due to oxygen deprivation and citing experiences from 9-11. But, the Public Health Commissioner provided similar and additional shelter-in-place guidance in a press release on April 5, advising the public to "close doors, turn off heating or air conditioning, close fireplaces, go to interior room without windows above ground, and if available, use duct tape and plastic sheeting" to seal all openings.

Even by the next day, State and local officials were not consistent in their messages regarding the potential danger to the public from the chemical exposure. Live VNN footage of the incident scene showed first responders not wearing personal protective equipment on April 5. This led to questions on April 5 as to whether the Governor had lifted the shelter-in-place order and whether it was now safe to walk outside. She clarified on *VNN Live* on April 5 that she had not lifted this order due to the two- to three-day half-life of this chemical. But, local officials were reporting that it was safe to go outside at this time. An urban search and rescue commander stated on VNN around 11:00 on April 5 that the shelter-in-place order was "an extra precaution," but that the incident scene was safe. Shortly thereafter, the New London City Manager stated on VNN that "there is no reason to shelter in place."

Although some of these inconsistent messages were likely due to artificialities of the exercise, they illustrate a problem that can arise when jurisdictions have differing views on what constitutes "safe." In this case, for whatever reason (even if artificiality-induced), local officials felt that the area was safe and began to communicate this in their statements. This conflicted with the position and guidance of the Governor and, at best, would likely have diminished the credibility of these spokespersons. At worst, the failure by officials (primarily at State and local levels as the leaders of public information on this attack) to provide early, accurate, and consistent protective action guidance could have increased the numbers and severity of casualties from the attacks.

[34] A National Oceanic and Atmospheric Administration (NOAA) official on VNN on April 5 stated that water will "neutralize the agent."

Tables II-1 and II-2 depict the range of protective action guidance offered by officials within the first few days of the attacks. They illustrate the general lack of uniformity of initial protective action guidance across FSL public health and top officials in both venues, as well as the delays in some cases in the most crucial first hours. Although some of the early disparity was due to artificialities, they suggest that officials may be unprepared to respond quickly to time-sensitive scenarios with consistent protective action guidance. Providing swift, accurate, and consistent protective action guidance in the immediate aftermath of an attack with time-sensitive implications (such as a biological or chemical attack) is one of the highest-impact actions officials can take. Providing this guidance should be a primary focus of incident communications initiatives. Of all the actions taken by FSL governments, this relatively simple action can dramatically reduce the scale of casualties and ultimate cost of response.

Table II-2. First-Day Protective Action Guidance for the Biological Attacks in New Jersey

	DHS	HHS	HHS/CDC	HHS/FDA	NJ Governor	NJSP Deputy Superintendent of Homeland Security	NJ DHSS	NJ Attorney General	NJ DEP	NJ Department of Agriculture	Union County Health Department	Middlesex County Health Department
Follow instructions of State and local governments.	4/4, 17:25 (PR)											
Taking antibiotics if you haven't been exposed is not recommended.		4/5, 13:34 (PR)										
If you don't have symptoms and haven't been near anyone exposed, don't go to a POD.		4/5, 13:34 (PR)										
Bacteria can be transmitted by aerosol, direct contact with tissues, body fluids, or bites.										4/4, 17:56 (PR)		
You can reduce the chance of becoming sick if you receive preventive treatment within seven days of exposure.			Fact Sheet				4/4, 21:20 (FAQ)					
People experiencing respiratory symptoms should call their local hospitals prior to visiting a health care facility.					4/4, 17:58 (PR)							
Stay six feet away from people.						4/4, 15:13 (VNN)					4/5, 12:59 (PR)	
Cover mouth when coughing/sneezing.							4/4, 20:54 (PR)					4/4, 16:09 (PR+ VNN)

	DHS	HHS	HHS/CDC	HHS/FDA	NJ Governor	NJSP Deputy Superintendent of Homeland Security	NJ DHSS	NJ Attorney General	NJ DEP	NJ Department of Agriculture	Union County Health Department	Middlesex County Health Department
Wash hands frequently.												4/4, 16:09 (PR+ VNN)
Stay home/avoid contact with others if you don't have symptoms.		4/5, 13:34 (PR)	Fact Sheet				4/4, 18:15 (PR)	4/4, 17:10 (VNN)				4/4, 16:09 (PR+ VNN)
Stay away from other people if they are ill.		4/5, 13:34 (PR)	4/5, 13:29 (PR/ Fact Sheet				4/4, 20:54 (PR)					4/4, 16:09 (PR+ VNN)
Wear a tightly fitting surgical mask.			Fact Sheet				4/4, 21:20 (FAQ)					
Use a cloth to cover mouth if surgical masks are not available to avoid contracting pneumonic plague.			Fact Sheet									
If you are ill with pneumonic plague, you must receive antibiotics within 24 hours of symptoms to prevent high risk of death.		4/5, 13:34 (PR)	Fact Sheet				4/4, 21:20 (FAQ)					
If you are ill, cover mouth and nose with tissue or surgical mask when coughing/sneezing.							4/4, 21:20 (FAQ)					4/4, 16:09 (PR)
Do not touch ill or dead animals (or wear gloves).		4/5, 13:34 (PR)	Fact Sheet				4/4, 21:20 (FAQ)					4/4, 16:09 (PR)
Eliminate sources of food/nesting for rodents and seal all openings larger than 2.5 inches.			Fact Sheet				4/4, 21:20 (FAQ)					4/5, 14:38 (PR)
Treat cats/dogs/ homes for fleas.			Fact Sheet				4/4, 21:20 (FAQ)			4/4, 17:56 (PR)		4/5, 19:46 (PR)

	DHS	HHS	HHS/CDC	HHS/FDA	NJ Governor	NJSP Deputy Superintendent of Homeland Security	NJ DHSS	NJ Attorney General	NJ DEP	NJ Department of Agriculture	Union County Health Department	Middlesex County Health Department
Do not allow pets to roam outdoors.							4/4, 21:20 (FAQ)					4/5, 19:46 (PR)
Boil water for one minute. Do not drink tap water (even filtered water).							4/4, 20:54 (PR)		4/5, 08:20 (VNN)			
Thoroughly cook and wash fresh produce to reduce plague risk.										4/5, (PR)		
Advise school food providers and food banks to use biosecurity measures to thoroughly clean vehicles and equipment to avoid the spread of disease.										4/5, (PR)		
Hunting in counties affected by plague is not advised.										4/5, (PR)		
Be cautious of blood donation. (Advise blood banks and tissue donor organizations to request deferral of donations from NJ, NYC, and Allentown, PA, which routinely collect blood in NJ and quarantine of donations accepted up to three weeks ago).		4/5, 13:34 (PR)		4/5, 13:34 (PR)								
If you have symptoms of plague, report to the hospital immediately.	4/5, 20:01 (PR)						4/4, 21:56 (PR)				4/5, 14:17 (PR)	4/4, 16:09 (PR)
Apply insect repellant to skin/clothing to prevent flea bites.							4/4, 21:20 (PR)					

	DHS	HHS	HHS/CDC	HHS/FDA	NJ Governor	NJSP Deputy Superintendent of Homeland Security	NJ DHSS	NJ Attorney General	NJ DEP	NJ Department of Agriculture	Union County Health Department	Middlesex County Health Department
Wear gloves, masks, eye protection, and gowns when treating suspect animals.										4/4, 17:56 (PR)		

Table II-3. First-Day Protective Action Guidance for the Chemical Attack in Connecticut

	DHS Secretary	HHS Secretary	HHS/CDC	CT Governor	New London Mayor	New London Office of Emergency Management	CT Department of Public Health	CT DOEHMS	American Red Cross
Stay inside (shelter in place [SIP])		4/5, 13:34 (PR)		4/4, 14:40 (VNN)					
(SIP) Close windows/doors.		4/5, 13:34 (PR)		4/4, 14:40 (VNN)			4/5, 09:00 (VNN)		4/4, 15:15 (PR)
(SIP) Lock windows/doors.				4/4, 23:28 (PR)					4/4, 15:15 (PR)
(SIP) Head to interior room, without windows above ground.						4/5, 13:34 (PR)			4/4, 15:15 (PR)
(SIP) Close fireplace and damper.		4/5, 13:34 (PR)		4/4, 23:28 (PR)					4/4, 15:15 (PR)
(SIP) Make sure radio is working.									4/4, 15:15 (PR)
(SIP) Turn off all fans/ventilation.		4/5, 13:34 (PR)		4/4, 23:28 (PR)					4/4, 15:15 (PR)
(SIP) Use duct tape and plastic sheeting to seal all cracks and vents.				4/4, 23:28 (PR)					4/4, 15:15 (PR)
(SIP) Have a hard-wired phone in room.				4/4, 23:28 (PR)					4/4, 15:15 (PR)
(SIP) Bring pets inside and bring additional food and water for them.				4/4, 23:28 (PR)					
Walk/drive home from waterfront if you can.					4/4, 17:00 (VNN)				
Use soap/water to wash hands if you were in the vicinity.	4/4, 17:00 (VNN)								
Avoid any exposure.			Fact Sheet	4/4, 17:50 (VNN)					

	DHS Secretary	HHS Secretary	HHS/CDC	CT Governor	New London Mayor	New London Office of Emergency Management	CT Department of Public Health	CT DOEHMS	American Red Cross
Don't eat freshly caught shellfish.							4/5, 09:00 (VNN)		
Don't let pets stray into areas where they can contact dusty surfaces.							4/5, 09:00 (VNN)		
Do not touch anyone if you think you've been exposed.		4/5, 13:34 (PR)							
Do not touch dead animals.								4/5, 14:40 (VNN)	
Get family disaster kit.						4/5, 13:34 (PR)			4/4, 15:15 (PR)
Continue to shelter in place due to two- to three-day half-life of sulfur mustard.				4/5, 15:00 (VNN)					
Quickly remove any clothing that has liquid sulfur mustard on it. If possible, seal the clothing in a plastic bag.		4/5, 13:34 (PR)	Fact Sheet	4/6, 14:04 (PR)					
Seal any bags with contaminated clothes inside a second plastic bag.			Fact Sheet	4/6, 14:04 (PR)					
Immediately wash all exposed areas with soap/water. Then report to a hospital for additional treatment and decontamination.		4/5, 13:34 (PR)	4/4, 7:56 (PR)						
Immediately wash any exposed part of the body (eyes, skin, etc.) thoroughly with plain, clean water. Eyes need to be flushed with water for 5 to 10 minutes. Do NOT cover eyes with bandages, but do protect them with dark glasses or goggles.			Fact Sheet						
If you are showing symptoms of sulfur mustard exposure, contact your health care provider or seek medical attention.		4/5, 13:34 (PR)	Fact Sheet	4/6, 14:04 (PR)					
If someone has ingested sulfur mustard, do NOT induce vomiting. Give the person milk to drink.			Fact Sheet						
People can be exposed by drinking contaminated water or getting it on their skin.			Fact Sheet						

5. No Evident Use of a JIS

> "[The JIS] integrates incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, timely information during a crisis or incident operations."
>
> NRP

The NRP describes a JIC as "a physical location where public affairs professionals from organizations involved in incident management activities work together to provide critical emergency information, crisis communications, and public affairs support." The NIMS is supposed to integrate multiple JICs into a JIS concept, which is designed to "ensure that Federal, State, and local levels of government are releasing the same information during an incident."[35] It states that "The JIS provides the mechanism for integrating public information activities among JICs, across jurisdictions, and with the private sector and NGOs." Although there is evidence of multiple JICs and individual agency incident communications operations across multiple jurisdictions, as well as within the private sector and NGOs, there is no evidence of the use of a JIS in the T3 FSE.[36]

Substantial evidence exists of the various FSL D/As courtesy copying JICs on press releases and vice versa. This may reflect the current interpretation by many people of the "coordination" role of JICs in the NRP and NIMS. There is also evidence of numerous one-to-one attempts to coordinate or validate information points between D/As. But, there is little evidence in either Connecticut or New Jersey of a structured mechanism for the JICs to receive regular updates from D/As or for the JICs to develop and disseminate message content across all D/As. Exercise data do not reveal how the JICs in each venue coordinated with each other and with D/As to systematically produce a consistent public message. The numerous inconsistencies in some of the core public messages suggest that, if such coordination existed, it was not sufficient.[37]

There was some evidence that the mock media found that obtaining information from JICs in both venues was slow due to the time-consuming process required to locate and validate answers.[38] This caused the mock media to go directly to individual D/As in many cases when quick updates or answers were needed. Other evidence suggests that, in some cases, representatives at the various JICs focused on supporting their D/As' incident communications needs rather than the coordinated message development mission of the JIC. Media SIMCELL logs also show that JIC staffs often did not have up-

[35] DHS NIMS Fact Sheet. http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0363.xml.

[36] In New Jersey, there was the Joint Field Office (JFO) JIC and a separate State JIC. In Connecticut, there was a JFO JIC and a local JIC in addition to incident-scene public affairs support. DHS hosted a virtual national JIC through the HSOC and its Ready Room.

[37] See discussion on protective action guidance issue.

[38] Media SIMCELL logs indicate that JIC staffs would take down questions over the phone, seek answers, and return the call once a validated answer had been obtained from the appropriate representative. In many cases, the Media SIMCELL had obtained the answer more quickly by directly contacting FSL D/As.

to-date information or were generally not well informed.[39] The information problems in the JICs may have been caused by a lack of colocation with the decision makers, which increased the coordination burden.[40] This problem may make some D/As reluctant to send their most experienced people to a JIC. For the JIC to fulfill its mission as a "focal point for the coordination and dissemination of information to the public and media," it needs to be closely integrated with the decision makers who are directing incident response, recovery, and mitigation efforts. For example, at the Governor of New Jersey's request, the State EOC established a dedicated State JIC to support his incident communications needs.

Experiences in the T3 FSE and observations from subject-matter experts suggest that the current JIC and JIS concepts could benefit from further examination. The NRP is an overarching guidance document and does not describe a process for how JICs should work together within a jurisdiction or across jurisdictions. Likewise, NIMS refers to the JIS, but does not provide operational guidance for how it should be implemented; who should lead it; and how various JICs, jurisdictions, the private sector, and NGOs should interface with it. DHS is currently working to refine the JIC concept. In July 2005, the department hosted a summit to develop "enhanced JIC leadership/organizational processes."[41] The lack of any evidence of the use of a JIS suggests that the JIS concept may need more operational definition. A supporting JIS Concept of Operations could provide amplifying implementation guidance for executing incident communications in the context of the NRP and NIMS. Future FSEs, in addition to reconstructions of real-world responses, could be used to test and refine evolving JIC and JIS concepts. Further examination of JIC implementation during real-world incidents would also help to determine whether the problems seen in T3 are common or the result of an artificial exercise environment.

6. Pre-exercise Coordination between DHS and International Participants

A number of preexercise coordination actions between DHS and the governments of the United Kingdom and Canada helped to enhance public information coordination. First, senior public affairs officials from the three nations successfully negotiated a formal "Communications Agreement regarding the coordination and management of public information and media relations between United States, UK and Canada for the international counterterrorism exercise planned for April 2005." It served as a written agreement and outlined principles and a template for how these three governments would approach public information in this exercise. Although not legally binding, it did serve to formalize agreement on principles such as "sharing key messages, talking points and

[39] The reconstruction contains multiple references from the Media SIMCELL of JIC staffs not being well informed, causing reporters to turn to individual D/As for the latest information. They acknowledged relying more heavily on updates from individual D/As once they were active.

[40] Media SIMCELL logs indicate that JIC staff would take down questions over the phone, seek answers, and return the call once a validated answer had been obtained from the appropriate representative. In many cases, the Media SIMCELL had obtained the answer more quickly by directly contacting FSL D/As.

[41] DHS OPA memorandum regarding Quicklook inputs, undated.

lines to take relating to the event," and providing "early warning of developing issues which may generate media or public interest."

In addition to this, DHS initiated two pre-FSE exercises with State, local, Canadian, and UK public affairs officials to strengthen and rehearse the logistics of international collaboration on incident communications. Whereas the Communications Agreement documented the desired approach, the pre-FSE workshops enabled public affairs officials in Canada, the United Kingdom, and the United States to gain experience with the various tools that would be available to implement it, and the FSE provided an environment for these officials to practice the coordination.

International coordination on public messaging can be difficult for a variety of reasons, including differing time zones, government information sensitivities, differing approaches/philosophies regarding sharing information with the public, and the larger set of coordinating organizations. But, these initiatives represented important steps toward building relationships and generating mutual agreement on principals that the three nations could agree on.

Senior public affairs officials from Canada and the United Kingdom have indicated that participation in the T3 FSE was valuable in enhancing their real-world coordination efforts.

U.S.-UK incident communications coordination was tested dramatically by the July 2005 terrorist attacks in London. Public affairs officials in both nations credit the T3 FSE experience and the relationships developed during planning phases of the exercise with helping to facilitate incident communications coordination during this difficult time. A Canadian public affairs official stated that the relationships and lessons learned developed through the FSE have already helped to enhance Canada-U.S. communications in several recent incidents.

7. Issues from Previous Exercises

Table II-4 highlights the evolution of incident communications since the T2 FSE.

Table II-4. Comparison of T3 FSE with Previous Exercises

T2 FSE	T3 CPX	SOEs 05-2 and 05-3	T3 FSE
ISSUES/OBSERVATIONS			
• PFOs observed a lack of coordination between FSL D/As and acted to improve this.	• Public affairs coordinated public information among participating D/As based on the draft Incident Communications Emergency Plan procedures.	• Officials emphasized the need for coordinated messages.	• DHS initiatives, such as the NICCL, helped to improve coordination between FSL D/As. • DHS and HHS released some joint messages.
		• Officials emphasized the importance of including medical experts in public messages regarding bioterrorism.	• State health officials in New Jersey worked closely with the Governor and were very visible in public messaging regarding the bioterrorism attack and response.
• Protective action guidance by State/local officials was not consistent or comprehensive.		• Participants stressed the importance of providing clear, lifesaving information immediately to the public. • IIMG TTXs emphasized the role of public messaging to identify victims and limit secondary contamination. *For example, the public needs practical sulfur mustard specifics: contamination avoidance, decontamination measures, and symptoms.*	• Protective action guidance by State/local officials was still not consistent or comprehensive. This should become a top priority for public affairs staff.
• State and local governments did not appear to have pre-coordinated, off-the-shelf, agent-specific fact sheets and did not appear to use those from the CDC.		• Federal officials stated that off-the-shelf fact sheets are needed to provide immediate and, in some cases, lifesaving guidance.	• CDC Fact Sheets were more widely cited by State and local D/As in websites than in T2.
• Multiple informational phone numbers were issued, but not released as a joint set.			• Both States emphasized hotline numbers to streamline public information. • But, multiple informational phone numbers were still released in both venues.
• Local jurisdictions in Chicago (plague outbreak) issued joint press releases, which resulted in consistent instructions to the public regarding PODs.			• POD instructions for some local jurisdictions were incomplete and could have slowed throughput. • FSL leaders in both venues conducted several joint press conferences or released joint statements.

T2 FSE	T3 CPX	SOEs 05-2 and 05-3	T3 FSE
• State and local officials used language that was either too technical or too vague and interfered with clear messaging.			• FSL officials generally used clear language when referring to the pneumonic plague outbreak and the chemical attack.

J. Recommendations

- Develop the mechanisms to prepare FSL top officials to provide swift, accurate, comprehensive, and consistent potentially lifesaving protective action during a terrorist attack with time-sensitive implications, such as the scenarios used in T3. Also, while top Federal officials may direct the public to look to State and local leaders for protective action guidance for most scenarios, they (particularly DHS/HHS officials) may need to be prepared to provide comprehensive protective action guidance in the event of an attack with national reach, such as a biological attack.
- Develop a supporting JIC/JIS Concept of Operations (CONOPS) to complement ESF #15 and Public Affairs Annexes of the NRP and ICER to provide more specific operational implementation guidance for executing incident communications in the context of the NRP. Explore virtual means of exchanging information and developing joint messages.
- Consider using future exercises to further test/refine protocols (which could be documented in the CONOPS), and educate stakeholder organizations on how incident communications coordination mechanisms such as the NICCL can be used to promote a common operational picture and coordinate message content where appropriate.
- Consider expanding the NICCL to an audio/visual forum that allows collaborative tracking of the evolving facts and message points.
- Expand the DHS Public Affairs Guidance product to provide more specific message points and consider linking it to NICCL updates.
- Establish primary public information sources early in the incident, such as the State hotlines and websites established in New Jersey and Connecticut.
- State governments should develop complementary incident communications plans for SNS distribution and work closely with affected localities to ensure that the guidance to the public provided by localities is clear and comprehensive.

III. Integrating Responses to INSs: Public Health Emergency and the Stafford Act—Task # III-3: Direct and Control Response Operations

A. Summary of Issue

The issue is that neither the NRP nor HHS CONOPS provide sufficient guidance for coordinating assistance for incidents that are concurrently covered under a Stafford Act declaration and a public health emergency. During the T3 FSE, the Secretary of HHS declared a public health emergency in New Jersey under the authorities of the Public Health Service Act. As discussed in the section "Stafford Act Declarations," the President approved Stafford Act declarations for the incidents in New Jersey and Connecticut. Additionally, the T3 FSE was the first test of the recently released NRP and thus the first opportunity to examine the guidance the NRP provides in coordinating INSs.

The T3 FSE revealed that the NRP does not provide adequate guidance for coordinating Federal operations and support under a public health emergency when a Stafford Act declaration is in effect. Specifically, the processes were unclear for requesting and coordinating Federal assistance under other Federal authorities in conjunction with a Stafford Act declaration. The relationship between the public health emergency and the Stafford Act declarations was further clouded by the lack of a clearly established HHS process for coordinating Federal-to-Federal support for public health emergencies. Additionally, the funding responsibilities of State and local governments under a public health emergency were not clearly defined.

B. Background

The NRP is an all-discipline, all-hazards plan that establishes a single framework for the management of domestic incidents. It provides the structure and mechanisms for the coordination of Federal support to State and local incident managers and for exercising direct Federal coordination of Federal authorities and responsibilities. Emergency public health assistance can be rendered under at least two separate Federal acts of enabling legislation: the Stafford Act and the Public Health Service Act.

1. NRP

As the PFO for domestic incident management, the Secretary of Homeland Security declares INSs and oversees coordination efforts for Federal operations and resources.[42] The NRP is the Federal government's plan to respond to an INS. An INS is defined as an incident that meets one of the following four criteria set forth in the Homeland Security Presidential Directive (HSPD)-5 and NRP:

- A Federal D/A acting under its own authority has requested the assistance of the Secretary of Homeland Security.

[42] Homeland Security Presidential Directive/HSPD-5 Subject: Management of Domestic Incidents, February 28, 2003.

- The resources of the State and local authorities are overwhelmed, and State and local authorities have requested Federal assistance (such as a Stafford Act declaration).
- More than one Federal D/A has become substantially involved in responding to an incident.
- The Secretary of Homeland Security has been directed to assume responsibility for managing a domestic incident by the President.

For INSs that are receive presidential declarations of disasters or emergencies, Federal support to States is delivered in accordance with relevant provisions of the Stafford Act. Although all declared disasters and emergencies under the Stafford Act are considered INSs, not all INSs require a Stafford Act declaration. As a result, the NRP describes basic concepts for operating under a Stafford Act declaration as well as for INSs covered under other Federal authorities (non-Stafford Act).

2. Processes and Structures for INSs under Other Federal Authorities

The NRP discusses how to coordinate an INS that is a non-Stafford Act incident.[43] The Secretary of Homeland Security designates a Federal Resource Coordinator (FRC) to serve as the Secretary's representative in the field to manage Federal resource support. Federal agencies provide resources under interagency reimbursable agreements or under their own authorities, such as a public health emergency or the National Oil and Hazardous Substances Pollution Contingency Plan (NCP).[44] The NRP states that for an INS without a Stafford Act declaration, "the JFO serves as the focal point for coordinating Federal assistance to the requesting agency." The NRP has a Memorandum of Agreement (MOA)—Mutual Aid for Incidents of National Significance (Non-Stafford Act)—that creates a framework for interagency mutual aid for Federal-to-Federal support in an INS. Federal agencies that are signatories of the NRP are signatories to the MOA, but the MOA needs to be activated.

[43] NRP Appendix 6 Overview of Support in Non-Stafford Act Situations.
[44] See discussion in "Emergency Response Operations under a Unified Command" for more information on the NCP.

3. Stafford Act

The Stafford Act establishes the programs and processes for the Federal government to provide disaster and emergency assistance to States, local governments, tribal nations, individuals, and qualified private nonprofit organizations.[45] The provisions of the Stafford Act cover all hazards, including natural disasters and some terrorist events (explosives, fire). Relevant provisions of the Stafford Act include a process for Governors to request Federal disaster and emergency assistance from the President. The President may declare a major disaster or emergency:

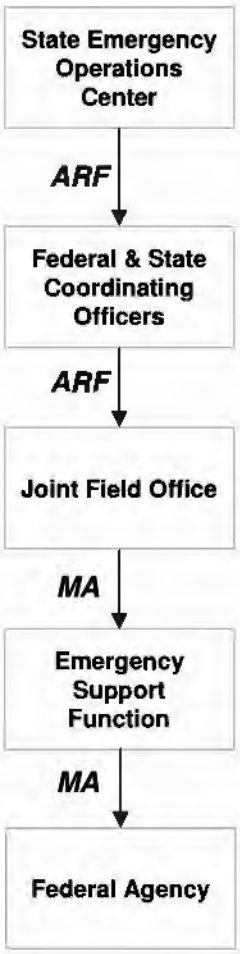
- If an event is beyond the combined response capabilities of the State and affected local governments; and
- If, based on the findings of a joint FSL preliminary damage assessment (PDA), the damages are of sufficient severity and magnitude to warrant assistance under the act. (In a fast-moving or devastating disaster, DHS/EPR/FEMA may defer the PDA process until after the declaration.)

4. Processes and Structures for INSs under the Stafford Act

The NRP discusses the processes and structures for supporting an INS accompanied by a Stafford Act declaration. A Federal Coordinating Officer (FCO), appointed by the Secretary of Homeland Security on behalf of the President, manages and coordinates Federal resource support activities related to Stafford Act disasters and emergencies. The FCO works with the State Coordinating Officer (SCO) to identify requirements and approve requests. Both are located at the JFO. The JFO manages and coordinates requests through ESFs, which provide the mechanisms for Federal support to States, for declared disasters and emergencies. The State submits requests to the JFO via action request forms (ARFs). Once the FCO determines a request is eligible for Federal support (i.e., beyond the capacity of the State to provide), the JFO Operations Section crafts a Mission Assignment (MA) and forwards it to the appropriate ESF. The ESF then coordinates with the relevant Federal agencies and tasks them with the mission assignment. Figure III-1 shows the basic ARF-MA process.

[45] Robert T. Stafford Disaster Relief and Emergency Assistance Act, 93 Pub. L. No. 288, 88 Stat. 143 (1974) (codified as amended at 42 U.S.C. §§ 5121-5206, and scattered sections of 12 U.S.C., 16 U.S.C., 20 U.S.C., 26 U.S.C., 38 U.S.C. [2002]).

Figure III-1. Stafford Act ARF-MA Process



5. Public Health Service Act

The Secretary of HHS is authorized under the Public Health Service Act[46] to declare a public health emergency. This declaration enables HHS to delegate its granted authority, release funds and resources to prevent the proliferation of a communicable disease, and plan an emergency medical response in the event of a disease outbreak. HHS is authorized to manage investigative and protective efforts, enter into contracts, assemble grants, disseminate information, and coordinate all other related actions reasonably necessary to respond to the emergency. The act gives HHS and its delegated authorities, such as the CDC and Food and Drug Administration (FDA), wide discretion and independence in the management of such efforts.

A Federal declaration by HHS allows for the release of Federal resources, including money and manpower. However, unlike the Stafford Act, which has funding already appropriated for use in the event of a major disaster or emergency declaration, funds need

[46] 42 U.S.C. 201, et seq.

to be appropriated ad hoc for use in a public health emergency.[47] These funds should supplement, rather than supplant, other FSL public funds.

HHS has no published detailed operational plan or burden-sharing agreement for coordinating assistance with States or other Federal agencies during a public health emergency. Their CONOPS does include some information on the process. The following statements are included in the HHS CONOPS:

- All requests for HHS assistance will be made to the Secretary through the Assistant Secretary for Public Health Emergency Preparedness (ASPHEP).
- If HHS requires assistance from other Federal agencies, the ASPHEP will make those requests on behalf of the Secretary.
- On behalf of the Secretary, the ASPHEP will provide specific MAs, priorities, and objectives to the Secretary's Emergency Response Team (SERT). These MAs will be coordinated and may be made at the request of other Federal entities, particularly DHS.

These statements lack sufficient detail on how requests will be submitted and coordinated with DHS and other Federal agencies.

C. Reconstruction

The Secretary of Homeland Security declared the events in New Jersey and Connecticut to be INSs on April 4 at 14:00 and 16:00, respectively.

The Governor of Connecticut asked the President for a declaration under the Stafford Act at 15:00 on April 4, which was followed by a faxed written request. At 16:30, the President verbally issued Stafford Act declarations for Connecticut and New Jersey.

The Secretary of HHS declared a public health emergency in New Jersey at 17:30 on April 4. HHS requested assistance from other Federal agencies under the authorities granted by the Public Health Service Act.

Once the Federal government declared the events in New Jersey to be an INS and an emergency under the Stafford Act, the expected Federal response organizations and processes became active. The FCO activated the ARF-MA process (see Figure III-1) and began coordinating the State's requests through ESFs.[48] Under the public health emergency in New Jersey, HHS requested direct support from other Federal agencies. HHS asked for Federal-to-Federal support from the Department of Veteran's Affairs, DHS, and Department of Defense (DoD). Most of these requests went through the NRCC or went directly to Federal agencies with little State input or coordination with the JFO.

---

[47] U.S. Department of Health and Human Services, *Concept of Operations Plan for Public Health and Medical Emergencies*, March 2004.

[48] Refer to the section on "Resource Requests and Resource Coordination" for more information on the types of resources requested by the States and the channels through which they were processed.

D. Consequence

In the T3 FSE, the terrorist attacks simulated in New Jersey and Connecticut resulted in the concurrent implementation of multiple Federal declarations to provide assistance to the States. The process for requesting and coordinating Federal-to-Federal support under a public health emergency in conjunction with a Stafford Act declaration was not understood. The guidance in the NRP was not sufficient to delineate the processes and responsibilities. Federal and State agencies had difficulty understanding how to coordinate resources and how to pay for them under the differing authorities and funding mechanisms.

The T3 FSE revealed the following:

- Neither the NRP nor the HHS CONOPS provides sufficient guidance for coordinating assistance for incidents that are concurrently covered under a Stafford Act declaration and a public health emergency.
- HHS does not have a detailed process for requesting and coordinating Federal-to-Federal assistance for public health emergencies.
- The funding capabilities of HHS and the funding responsibilities of States and other Federal agencies are unclear under a public health emergency.

E. Analysis

Data indicate that State and Federal agencies were uncertain about how to coordinate response efforts provided via the Public Health Service Act with those provided under the Stafford Act. Such uncertainty was due to the fact that the processes for requesting, tracking, and coordinating assistance provided by the Federal government under other Federal authorities in conjunction with a Stafford Act are unclear. This suggests that neither the NRP nor the HHS CONOPS provides sufficient guidance for coordinating Federal-to-Federal support under a public health emergency when a Stafford Act declaration is also in effect. Additionally, funding responsibilities for States under a public health emergency are unclear.

1. Insufficient NRP Guidance for Coordinating Assistance under a Stafford Act Declaration and a Public Health Emergency

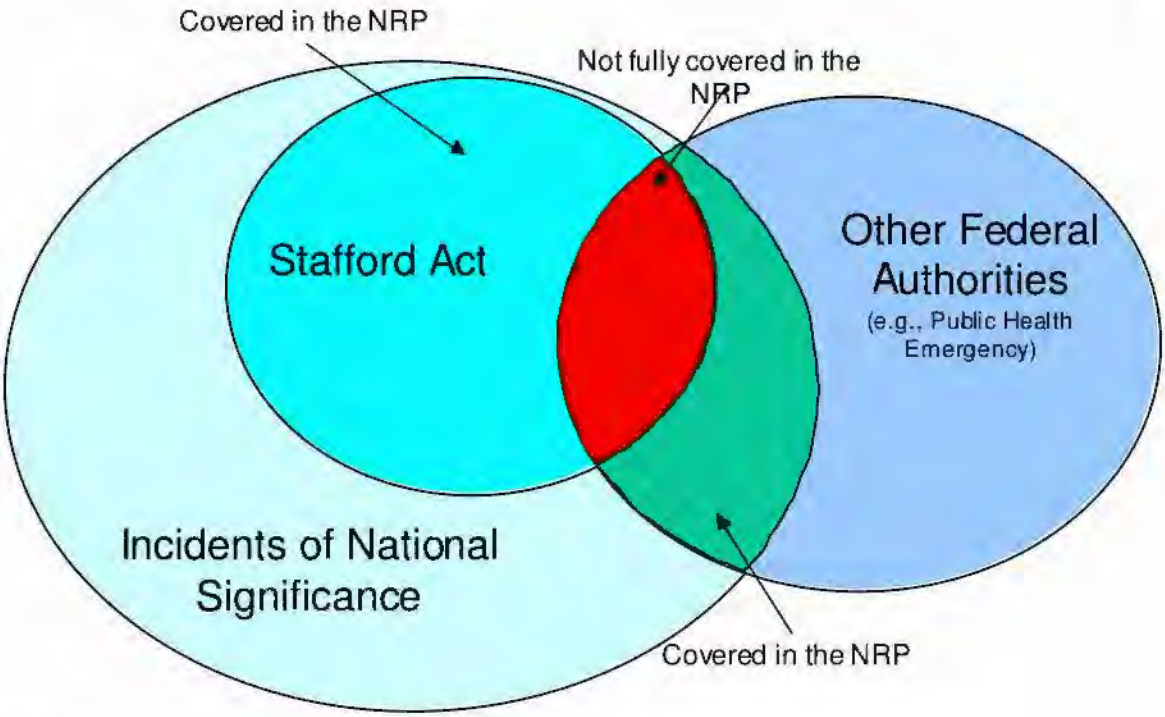
As discussed above, the NRP is intended to be the guiding document for INSs. The NRP describes the processes and structures for Stafford Act incidents and the processes for Federal-to-Federal support for INSs that are covered under other Federal authorities, such as a public health emergency. However, the NRP states that:

> *In the context of Incidents of National Significance, these supplemental agency or interagency plans may implemented concurrently with the NRP, but are* subordinated to the overarching core coordinating structures, processes, and protocols detailed in the NRP *[emphasis added]. In this case, the department or agency with primary responsibility for execution of the supplemental agency or interagency plan is also responsible for ensuring that all ongoing activities* conform to the processes and protocols prescribed in the NRP. *[emphasis added]*

Because the NRP describes structures, processes, and protocols for Stafford Act INSs and for INSs under other Federal authorities, the question is which of those are in effect during concurrent implementation of both Stafford Act and other Federal authorities.

Figure III-2 shows the relationship among INSs, Stafford Act incidents, and incidents covered under other Federal authorities. In the case of incidents that are covered under the Stafford Act and other Federal authorities, the NRP says little about how to request and coordinate Federal resources.

Figure III-2. Relationship Between INS and Incidents Covered Under Other Federal Authorities



The NRP says:

> *Federal departments and agencies supporting the NRP are activated and engaged using* either *a mission assignment process for events* supported by Stafford Act funding or *through interagency agreements or other direct funding sources when implemented* using other authorities. *[emphasis added]*[49]

The NRP does not specifically cover the case of an incident that is addressed concurrently by the Stafford Act *and* other Federal authorities. The NRP does not explicitly state that Stafford Act processes should be used for resources being requested under a public health emergency (or other Federal authorities) that is concurrent with a Stafford Act declaration. It also does not state that Federal agencies should submit requests for Federal-to-Federal support through the JFO for a non-Stafford Act INS. The NRP simply calls for agencies to coordinate operations through the JFO, without sufficient detail as to how that coordination should occur. The HHS CONOPS also discusses coordination without detailing how it should be done. Both documents lack sufficient guidance for coordinating assistance for incidents covered concurrently under the Stafford Act and Public Health Service Act.

[49] National Response Plan (December 2004).

2. Coordinating Federal-to-Federal Assistance Under a Public Health Emergency

This lack of guidance in the NRP led to several problems with resource requests and coordination during T3.[50] The Stafford Act process is a bottom-up approach in which requests originate at the State and local levels, are coordinated at the JFO, and then are tasked to the appropriate Federal agency. To provide resources during the T3 FSE, HHS implemented a top-down approach that was not well defined or well understood by the response organizations. Consistent with its authorities under the Public Health Service Act, HHS requested support from other Federal agencies. Some requests were made directly to the other agencies, and some requests were submitted through the NRCC, which would then forward them to the appropriate Federal agency. For example, HHS submitted a request for a 10,000-bed alternative care facility to DHS through the NRCC, while requesting a 250-bed field hospital directly from DoD.

Further complicating the process, HHS used the same top-down approach to provide resources in Connecticut, where a public health emergency had not been declared. For example, HHS requested a 250-bed alternative care facility and patient-movement assets for 1,000 patients directly from DoD and requested a 10,000-bed alternative care facility directly from DHS without coordinating with the State or JFO.

In addition to using different paths for resource requests, HHS did not have an established process to coordinate its efforts with the JFO and the other Federal support being provided. States were often unaware of HHS requests until after they had been made. Lack of notification placed an unexpected logistical burden on the States.

HHS lacked a clear process for coordinating Federal assistance under a public health emergency and did not follow the established Stafford Act process in Connecticut, where no public health emergency was declared.

3. Funding Capabilities and Responsibilities Under a Public Health Emergency

Under the Stafford Act, funds are set aside to pay for Federal assistance. The Stafford Act creates a cost-sharing agreement between the affected State and the Federal government, whereby the State is liable for up to 25 percent of the resource expenses. When a mission assignment is drafted, it includes the State's burden share, so the SCO knows what the cost liability is prior to receiving Federal assistance.

Under a public health emergency, HHS can authorize spending but has no funds set aside for such a purpose. A supplemental appropriation is needed to reimburse any funds spent in response to a public health emergency. Additionally, HHS has no process for burden sharing with States. As a result, States are uncertain of their cost responsibilities for support obtained under a public health emergency.

During the T3 FSE, Federal and State agencies were uncertain about who would be paying for requests originating from HHS. The JFOs thought HHS should pay for the

[50] These problems are discussed in the section on "Resource Requesting and Resource Coordination."

medical support it was requesting under the public health emergency. Many Federal participants erroneously believed that funds were readily available to cover Federal assistance under the public health emergency. The States were uncertain as to what part of the costs they would incur. During a conference call on the morning of April 6, representatives from HHS, DoD, NRCC, RRCCs Region 1 and Region 2, CT JFO, and NJ JFO discussed who was requesting the 10,000-bed alternative care facility and the 250-bed field hospital and who was going to pay for these resources. Connecticut did not want the 10,000-hed alternative care facility or the 250-bed field hospital if the State had to pay for it. They wanted assurance that HHS would incur the financial liability. HHS did not have a process in place to provide any information to the States on what would be their financial liability or what resources they would have to provide to support the Federal assets.

Although HHS has spending authority under a public health emergency, no funds are set aside in advanee. HHS and other Federal agencies have to use their own operating funds and/or request supplemental appropriations. State and local funding responsibilities under a public health emergency are unclear. During the T3 FSE, this resulted in hesitancy on the part of the States to accept any HHS-directed resources.

4. Issues from Previous Exercises

In the T2 FSE, no problems were noted with respect to the declaration of a public health emergency. In fact, the T2 After-Action Report (AAR) stated that "the declaration of the public health emergency in the Chicago area was enacted with little confusion or difficulty in execution."[51] The primary difference between the two exercises was that during the T2 FSE, tbe NRP was not in effect. Additionally, HHS initially acted alone during the T2 FSE, because the public health emergency in Illinois was declared about 20 hours before the Stafford Act declaration was made. The Stafford Act declaration was approved with only 20 hours remaining in the exercise (Table III-1).

[51] T2 Full-Scale Exercise After-Action Report, September 30, 2003, draft.

Table III-1. Comparison of T3 FSE with T2 FSE

T2 FSE	T3 FSE
SIGNIFICANT DECISIONS	
• **After consulting with State officials and receiving confirmation of pneumonic plague, the Secretary of HHS declared a public health emergency in Illinois.** *The declaration came approximately 24 hours after the first disease clusters became apparent in the State.* *This declaration was made 20 hours before the Stafford Act declaration for the State was made.*	• **After a presumptive diagnosis of pneumonic plague, the Secretary of HHS declared a public health emergency in New Jersey.** *This declaration came approximately nine hours after the initial clusters of patients began presenting to NJ hospitals.* *A Stafford Act emergency declaration was issued shortly before the public health emergency declaration was made.*
ISSUES/OBSERVATIONS	
• **No problems or difficulties with the public health emergency declaration were evident.** *However, it is not clear whether any entity actually tried to request resources through this act.* *Potential problems resulting from concurrent implementation of a Stafford Act declaration and a Public Health Emergency Act declaration did not arise because of the timing of the declarations.*	
	• **Neither the NRP nor the HHS CONOPS provide sufficient guidance for coordinating assistance for incidents that are concurrently covered under a Stafford Act declaration and a public health emergency.** • **HHS does not have a detailed process for requesting and coordinating Federal-to-Federal assistance for public health emergencies.** • **The funding capabilities of HHS and the funding responsibilities of States and other Federal agencies are unclear under a public health emergency.**

F. Recommendations

- Clarify the process for Federal-to-Federal support for non-Stafford Act assistance in conjunction with a Stafford Act declaration. Determine whether the ARF-MA process can be used to request resources under other Federal authorities and how to coordinate those requests with the JFO.
- Develop a transition plan for coordinating incidents that start under non-Stafford Act authorities but later grow to include a Stafford Act declaration.
- Clarify the process for Federal-to-Federal support under a public health emergency. Include how HHS should coordinate with other Federal agencies, determine who is best suited for coordinating and tracking requests (e.g., HHS or FEMA), and determine what responsibilities other Federal agencies have to report to HHS.
- Clarify the funding capabilities and responsibilities of States, HHS, and other Federal agencies under a public health emergency.

IV. The Strategic National Stockpile (SNS) and Points of Dispensing (PODs)—Task # III-8: Direct and Control Distribution of Supplies and Equipment

A. Summary of Issue

The issue is that the plan to conduct statewide prophylaxis evolved during the course of the exercise and did not appear to reflect a pre-planned and carefully integrated Federal and State response. It is not clear that the Federal government has a strategy or plan for implementing its own system of PODs or for rapidly identifying and supplying staff to support State efforts in the event of a large-scale requirement.

The release of *Yersinia pestis* in New Jersey prompted State officials to request SNS support. The release also prompted Federal and State officials to notionally activate nearly 400 PODs throughout New Jersey for the purpose of providing prophylaxis to every resident of the State.[52] Analysis of T3 FSE data suggests that this plan was not executable. Distribution of prophylaxis to every State resident was complicated by the short incubation period of plague, a fragmented Federal-State planning process, and resource management issues. The announcement that 8.8 million residents had received prophylaxis during the exercise overlooks these issues and is based on other factors such as unrealistic POD throughput rates and activation timelines. Staffing was the primary resource constraint in successfully executing the proposed mass prophylaxis plan.[53] To operate hundreds of notional PODs, officials had to identify and process thousands of workers. Observations made during the exercise indicate that such large numbers of workers are not presently available.

Without the current capability to provide prophylaxis to every State resident, senior officials will have to focus on targeted prophylaxis (i.e., determining as quickly as possible the potentially exposed population). Under this scenario, the possibility exists that some residents who need prophylaxis may not receive it. The alternative is to develop an infrastructure (one component of which would include increasing the number of available and trained workers) that can support statewide prophylaxis; however, this approach could require a significant investment.

[52] The State announced a plan to supply prophylaxis within 48 hours to all residents of the State plus those who had worked in New Jersey since March 28. This announcement was made by the Governor's office at 17:45 on April 5.

[53] Other constraints that potentially could have affected execution, such as transportation and parking, could not be examined.

Comparatively few problems were observed during the delivery and distribution of the SNS. There was some initial uncertainty about the SNS request, and there were problems integrating Federal plans for SNS deployment with the State; however, the T3 participants successfully resolved these issues. Major observations from the exercise include:

- New Jersey successfully received, broke down, and transported components of the SNS to PODs.
- New Jersey set up and operated 22 real PODs using the guidelines of the *New Jersey Mass Prophylaxis Manual* and was able to assess issues of throughput, as well as setup and logistics.
- In response to the outbreak of pneumonic plague, New Jersey attempted prophylaxis on a very large scale—effectively trying to reach 8+ million people under the very short epidemiological time frame associated with the disease. The State opened and operated an additional 200 notional PODs.
- The Federal government established its own system of PODs—opening more than 160 notional sites at postal facilities, Veterans Affairs (VA) hospitals, and Health Resources and Services Administration (HRSA) community centers. This action was meant to support the rapid expansion of prophylaxis undertaken by the State, but also appeared to reflect Federal government efforts to get out in front of the developing epidemic.
- The Federal government did not appear to consider at least one of the approaches being considered in the HHS Cities Readiness Initiative (CRI)—i.e., delivering medicine to people instead of having people come to the medicine—but instead relied entirely on fixed PODs.

B. Background

1. SNS

The SNS is an extensive inventory of medical supplies (e.g., antibiotics, vaccines, bandages, and ventilators) configured for rapid deployment in response to a potential or actual mass casualty event. The SNS is managed by the CDC for the DHS.

The SNS is divided into two components: push packs and managed inventory. Each of the 12 push packs contains a wide range of medical supplies designed to meet a variety of scenarios. The push packs contain approximately 50 tons of medical supplies and are staged at transportation hubs throughout the United States. In response to a mass casualty event, the CDC can deploy a push pack to an affected area within 12 hours of the request. If additional medical supplies are required, the CDC can deploy additional push packs or ship managed inventory within 24 to 36 hours. Managed inventory refers to large stockpiles of medical supplies that can be used to augment the contents of the push packs. Instead of deploying additional push packs that may contain supplies that are not needed, the CDC uses the managed inventory to meet the specific medical needs of an affected area.

For example, the CDC could respond to a State request for SNS support during an anthrax outbreak by deploying a push pack, because push packs can be delivered rapidly and contain the antibiotics needed to treat the infection. If the contents of the deployed push pack were not sufficient to meet the needs of the affected population, the CDC could use managed inventory. The managed inventory would arrive later, but the shipment would contain large quantities of the medical items needed to treat anthrax victims (e.g., antibiotics and ventilators). In this example where the medical needs are clear, turning to managed inventory would be preferable to deploying additional push packs, because the latter contain many items that are not typically used to treat anthrax infections (e.g., bandages and splints). Unlike the prepackaged push packs, shipments of managed inventory can be configured to meet the specific medical needs of the affected population.

The Technical Advisory Response Unit (TARU) accompanies SNS deployments and provides guidance on its use. The TARU consists of subject-matter experts (e.g., logisticians and emergency responders) familiar with the contents of the SNS and procedures that govern its employment. For example, the TARU has exercised the distribution of SNS medications to PODs and can provide details of the push pack contents.

2. PODs

Health officials can use PODs to rapidly distribute medical supplies from the SNS to large numbers of potentially exposed but asymptomatic people. During a public health emergency, people can be directed to a local POD where health care professionals would screen them to determine if the medication is appropriate and safe for them to take. If prophylaxis is warranted, individuals receive the medication or vaccine that will prevent them from becoming ill.

The total number of people who can receive prophylaxis is a function of three factors: length of time the PODs are active, throughput rate, and the number of active PODs. The window of opportunity for distributing prophylaxis to an affected population begins when the disease and the potentially exposed population have been identified and ends when people living in the hazard areas are no longer likely to contract the disease. Other considerations of great importance not examined in this exercise include such issues as transportation access to the POD and available parking.

Throughput rate refers to the number of patients that a POD can process in a fixed period of time (typically about an hour). This rate can be affected by the size of the staff and the standard of care provided by the staff. A larger staff will support a higher hourly throughput rate (if the physical space is large enough); however, locating large numbers of medical, security, and support staff on short notice during a public health emergency is challenging. "Standard of care" refers to the services provided at the POD.

Whereas the minimum standard of care service would be to simply distribute medication to patients, the NJ plan, like others, prescribes a higher standard of care that includes:

- education about the disease (e.g., plague) and the antibiotics (e.g., doxycycline);
- medical assessment to identify those requiring additional treatment;
- transportation of symptomatic patients to a hospital;
- translation services;
- medical screening to identify people for whom the treatment is contraindicated (e.g., a person who is allergic to antihiotics); and
- mental health counseling.

Increasing the standard of care without implementing corresponding increases in staffing and logistical support will reduce the throughput rate and increase the required logistical support. Each service requires additional staff, a larger physical space, and additional materials (e.g., forms, masks, and rubber gloves), and it increases patient time in the POD. Patients remaining for longer periods of time may create backlogs inside the facility and traffic jams outside, further reducing the throughput rate.

Increasing the number of PODs can increase overall throughput, but doing so would create additional logistical challenges. Each POD would need to have an identified site and would have to be supplied, secured, publicized, and staffed. Each of these steps would have to be completed before prophylaxis distribution could begin.

In preparation for the T3 FSE, the NJ DHSS developed the *New Jersey Mass Prophylaxis Manual*. In this document, NJ DHSS highlights key elements of its mass prophylaxis plan, including the following:

- PODs will be supplied with FSL supplies.
- A mass prophylaxis effort will require several types of workers, including nurses, pharmacists, counselors, security, translators, administrators, and support personnel.
- PODs that distribute oral medication require a staff of 183 personnel for each eight-hour shift.
- POD throughput rates will be 1,000 people per hour for oral prophylaxis.
- It is recommended that PODs operate 16 hours per day (24-hour operations are possible).
- The standard of care in New Jersey will include an education and screening process to identify individuals who should receive the prophylaxis and those who are contraindicated.

During the T3 FSE, New Jersey planned to activate 22 real PODs throughout the State. One POD would be activated in each of the following counties and municipalities:

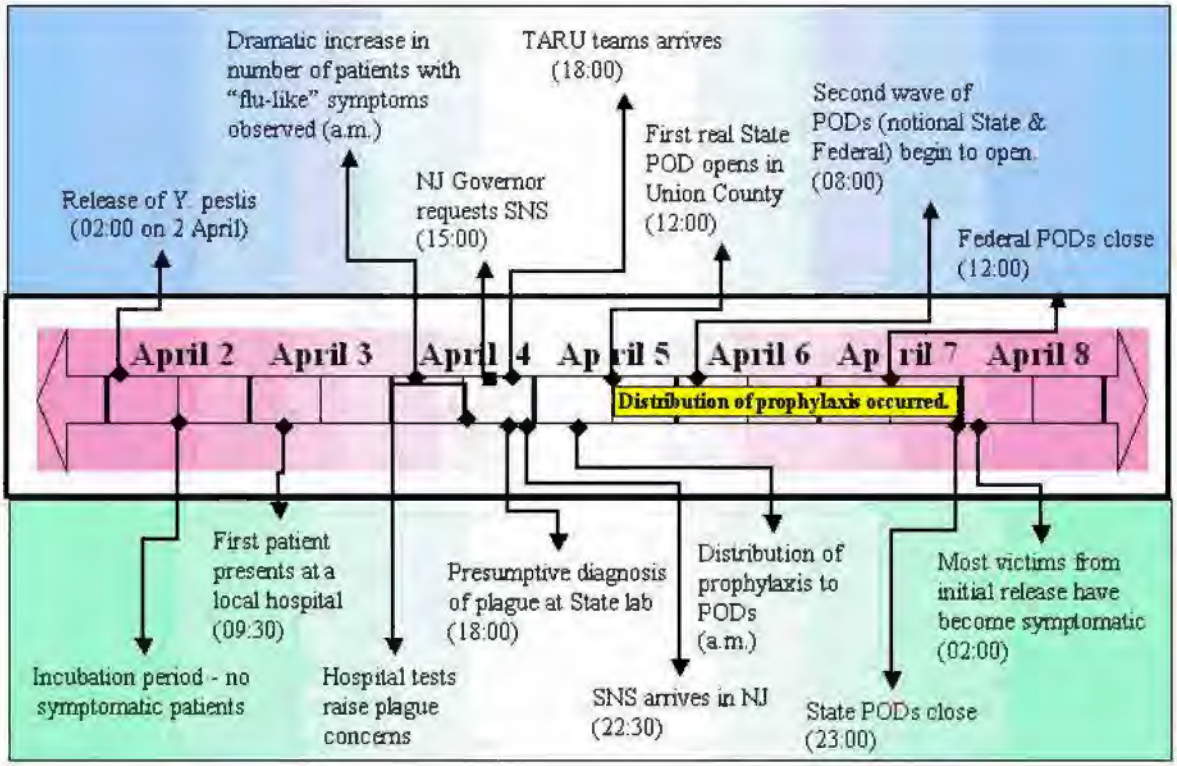
Atlantic County	Essex County	Ocean County
Bergen County	Gloucester County	Passaic County
Burlington County	Hudson County	Somerset County
Camden County	Hunterdon County	Sussex County
Cape May County	Mercer County	Union County
City of Newark	Middlesex County	Warren County
City of Paterson	Monmouth County	
Cumberland/Salem Counties	Morris County	

As part of the exercise, each of these 22 PODs was scheduled to operate for approximately four hours during one day of the exercise. During these hours of operation, the PODs would function as they would during a real public health emergency. Law enforcement officers would provide security, and staff would process volunteers simulating patients. Notionally, these 22 PODs could operate throughout the duration of the public health emergency and additional PODs could be opened as needed. Representatives from the NJ DHSS indicated that, in an actual event, the State could operate a maximum of five PODs per county for a statewide total of approximately 100.

C. Reconstruction

The release of *Yersinia pestis* in New Jersey prompted a request to the Federal government for the SNS and eventually the decision to activate a large number of PODs throughout the State. Figure IV-1 depicts the sequence of activities discussed in this section.

Figure IV-1. Timeline of NJ SNS and POD Activities



As part of the exercise scenario, terrorists notionally released the bacteria along sections of the Garden State Parkway, U.S. Route 1, and NJ Route 18 in northern New Jersey during the early morning hours of April 2. The release began at 02:00 on April 2 and ended shortly thereafter. Approximately 24 hours later on the morning of April 3, the first patient presented at a local hospital complaining of "flu-like" symptoms.

During the day on Monday, April 4, evidence began accumulating that New Jersey was facing a public health emergency caused by the deliberate release of a biological agent. At 10:20 on April 4, hospital officials notified the NJ DHSS that they had patients with symptoms consistent with plague. A presumptive diagnosis of plague was made based upon initial lab tests of patient samples. In response to this information, the NJ Governor requested the SNS from the CDC and ordered the activation of PODs throughout New Jersey. Despite some initial uncertainty about the request, the Secretary of HHS authorized the deployment of the SNS to New Jersey at 15:15.

The first SNS shipments, the managed inventory, arrived at the NJ State receipt, stage, and store (RSS) site at approximately 21:30 on April 4. The second SNS shipment, the push pack, arrived approximately five hours later.[54] The two shipments contained a total of 10 million courses of treatment (primarily of doxycycline). Overnight, the RSS staff

[54] During a real emergency, push packs are more likely to arrive first; however, an exercise artificiality caused the managed inventory to arrive before the T3 push pack.

and TARU team began preparing the SNS shipments for distribution to the county RSS site and PODs.

POD operations involved both real and notional sites. The first real POD opened in Union County at 12:00 on April 5. Additional real PODs opened on the following days, and each operated for several hours. During the day on April 5, NJ officials began planning to greatly expand the number of distribution sites in the State. At 17:45 on April 5, the NJ Governor announced that the State had decided to distribute prophylaxis to all residents and those who had worked in the State. Initially, the Governor announced that New Jersey would open 456 more notional PODs (400 at high schools and 56 at colleges). This number was subsequently reduced to approximately 200 notional PODs later in the planning process. These notional sites were reportedly operational at 08:00 on April 6.

To augment the State's efforts, the Federal government decided to open a large number (more than 160) of notional PODs in the four hardest hit counties: Middlesex, Union, Hudson, and Essex. These PODs would be located at U.S. Postal Service (USPS) facilities, VA hospitals, and HRSA Community Centers. In a series of conference calls during the night of April 5, NJ, FEMA, and HHS representatives discussed the Federal plan. HHS indicated that Federal PODs would begin operations by 08:00 on April 6; all were reported open four hours later at 12:00. The Federal PODs would be under the direction of the NJ PFO and would be staffed by USPS volunteers and other personnel provided by the Federal government. State and Federal sites operated continuously until they closed, with the Federal sites closing at 12:00 on April 7 and the State sites closing 11 hours later. At that time, officials announced that all 8.8 million residents had received prophylaxis.

D. Consequence

The T3 experience highlights the dilemma that decision makers may face when dealing with the deliberate release of a biological agent on a large scale. In real-world public health emergencies, as in the exercise, political leaders will have to choose between focused or widespread distribution of prophylaxis. Both policies carry risks for these leaders. A more focused, or targeted, approach is less resource intensive, but requires accurate determination of the potentially exposed population and a carefully crafted public message. It carries the risk that some individuals who need prophylaxis may not receive it, but it exposes fewer people to potentially adverse effects. A much wider-scale effort, like the one attempted in New Jersey, may encounter logistical and resource limitations that constrain the number of PODs the State can operate, increase the time it takes to distribute prophylaxis, expose a higher number of people to the potentially adverse effects of antibiotic treatment, and possibly leave some residents in the most affected area without prophylaxis. The T3 FSE experience highlighted the difficulties of not having the planning and resources at the Federal and State levels to rapidly execute a large-scale prophylaxis plan.

E. Analysis

The T3 FSE exercised both the deployment of the SNS, as well as the POD setup and distribution processes. Relatively few issues were noted during the delivery and distribution of the SNS; however, the exercise did highlight significant issues with the decision to provide prophylaxis to all of the residents of New Jersey.

1. SNS

At 15:00 on April 4, the Governor of New Jersey made a public statement in which he requested deployment of the SNS. However, this verbal request was not immediately followed up with a written request from the State to the CDC.[55] The first indication of a formal request from New Jersey did not appear until several hours later at 18:30. The lack of supporting documentation appeared to create ambiguity about the request. State and Federal officials were not certain if the State had actually requested the SNS or how the CDC would react to a verbal request without supporting documentation. In the exercise, the CDC deployed managed inventory to New Jersey prior to a formal request at the direction of the Secretary of Health and Human Services. .

Observations made during the deployment of the SNS indicate that State officials were not fully integrated into the planning efforts and had to react to deployment decisions made by Federal officials. For example, State officials were not aware of the arrival of the TARU or the requirement to transport the unit to the RSS site until shortly before the TARU arrived in New Jersey. In addition, the arrival times of the managed inventory and push pack changed with little notice. NJ planners successfully reacted by rescheduling escorts and RSS staffing to accommodate the changes. Despite these disconnects, the deployment proceeded because State officials were able to replan and reschedule the State's support for deployment of the Federal asset.

2. PODs

The plan to distribute prophylaxis to every resident in the State was complicated by the short incubation period of plague, a fragmented Federal-State planning process, and resource management issues. These observations indicate that the plan to distribute prophylaxis to the entire population of New Jersey was not executable.

a. Time: A Limiting Factor

Most individuals exposed to an aerosolized release of *Yersinia pestis* will become symptomatic within one to six days.[56] This provides a theoretical window of five days or

[55] The governor's comments were made under the assumption that the press conference would be taped and broadcast later in the day.

[56] The exact timeline depends in part on the dose an individual receives and the physical condition of that individual.

fewer to provide antibiotics to exposed individuals.[57] This window of opportunity is reduced by the time it takes to determine that the initial cases are actually plague and that the infection is a public health threat rather than an isolated case. The time available to distribute prophylaxis is further reduced by the need to request and receive the SNS and execute the State/local prophylaxis plan. These factors may reduce available time for distribution to less than three days.

Figure IV-1 depicts the timeline of the NJ response. Some of these times were affected by exercise artificialities and would vary from event to event. For example, the length of time between the first patient arriving at a hospital and the request for SNS could be affected by many factors, including the following:

- length of time the patient has to wait to be seen by a physician;
- diagnostic skills of the physician;
- workload of hospital and State labs;
- level of suspicion of health care providers and public health personnel;
- speed with which State health officials determine that the initial case is not an aberration; and
- State leadership's familiarity with the SNS process.

The timing observed in the T3 FSE was artificial, because participants were aware of the exercise and many knew that pneumonic plague was the disease. Observation of the timeline in Figure IV-1 suggests that the first notional PODs could have opened at approximately 08:00 on April 5, leaving a total of 66 hours (08:00 on April 5 through 02:00 on April 8 when most originally exposed individuals would have become symptomatic) to distribute prophylaxis to 8.8 million residents. As the exercise evolved, the stated goal was to complete the distribution by 23:00 on April 7.

b. Fragmented Federal and State Planning

Over the course of the exercise, two separate POD systems developed: State and Federal. At times, the existence of the two systems created confusion among the participants, possibly reducing the effectiveness of the plan to physically exercise 22 PODs while planning for the activation of additional notional PODs resulting from player action..

As the scope of the public health emergency in New Jersey widened, NJ officials became aware that HHS and DHS were concerned that the State plan to distribute prophylaxis would not cover enough residents. In discussions with the PFO cell, the NJ DHSS reported that New Jersey could operate as many as five PODs per county if conditions warranted that number; however, New Jersey officials felt that the number of victims as of April 5 at most warranted two to three PODs per county.

[57] This timeline assumes that the detection of the release occurs because sick patients arrive at hospitals, rather because the terrorists releasing the pathogen are caught.

Officials from HHS and DHS preferred a more aggressive prophylaxis program and began the process of establishing PODs at Federal facilities in New Jersey. HHS planned to supplement New Jersey's prophylaxis plan by opening more than 160 notional PODs. The Federal goal was to distribute prophylaxis to 2.8 million individuals in the four most affected counties.

In response to the Federal government's concerns and the growing number of plague victims, the NJ Governor announced a plan to expand the distribution of prophylaxis to include every resident and everyone who visited the State during a specific period of time. During the afternoon of April 5, New Jersey began executing plans to increase the number of PODs to 478 (i.e., 22 real and 456 notional ones). The number of notional State PODs was subsequently reduced to approximately 200. These additional State sites would operate under the guidelines of the *New Jersey Mass Prophylaxis Manual* and would be staffed by a mix of State personnel and personnel provided by the Federal government.

Federal and State prophylaxis efforts were not closely coordinated. Implementation of the Federal plan surprised many State officials. Likewise, the State decision to activate additional PODs did not appear to have an observable impact on Federal planning. State and Federal officials also disagreed on standards of care and staffing levels. NJ officials insisted that distribution sites follow the *New Jersey Mass Prophylaxis Manual,* which provided a higher standard of care (e.g., education, screening, and counseling) and required a larger staff (i.e., 183 personnel per shift) than the Federal plan for New Jersey. Federal officials opted for a lower standard of care (i.e., literature and medication distribution, rather than personal screening) and a smaller staff (i.e., as few as 10 per shift). When Federal and State officials reached an impasse, Federal officials indicated that they would operate the Federal system separately.

Additionally there is no plan in place to deliver medical supplies to Federally operated PODs. The State's Receipt, Store and Stage (RSS) site did not have the capability to handle the volume of medical material required to supply both the State and Federal operated PODs, nor did they have the transportation assets to deliver the material. To supply the Federally operated PODs with prophylaxis would have required a sufficiently equipped and staffed warehouse, adequate trucks and drivers and a logistics management system to maintain the supply chain.

With two systems operating, reliable information about either one was difficult to obtain. Many NJ officials were unaware of the Federal sites until after they began operations. For example, the State Epidemiologist stated on VNN that 46 PODs were open at 09:33 on April 6. Moments later, a NJ DHSS Deputy Commissioner, also being interviewed on VNN, stated that 40 were operational. According to the Federal plan, the 163 Federal sites were beginning operations during these two interviews.

c. Inconsistency in the Reported Number of PODs

Planning issues extended beyond sharing information about the operation of the two systems. Among the State and Federal participants, there was little consistency on a basic, but essential fact—the number of PODs operating in New Jersey. The timeline described in Table IV-1 provides insights into this issue.

Table IV-I. Insights into the Level of POD Awareness Among Participants

Date	Time	Event
April 5	16:52	NJ PFO is notified that the State will activate 456 additional PODs (at 400 high schools and 56 colleges) for a total of 478 PODs.
April 5	18:46	Governor's Office announced that New Jersey has taken control of 400 high schools and 56 colleges to be used as PODs. They open by April 6 at 08:00.
April 5	21:30	In a POD planning teleconference call that brought together RRCC, NJ Public Health, NJ Office of Emergency Management (OEM), HHS, PFO, DoD, and the Governor's Office, it was announced that the postal PODs would begin opening at 08:00. All 163 would be open by noon on April 6. New Jersey announced an increase in the number of PODs from 22 to 104.
April 5	23:00	HHS announced its plan to augment the 200 State PODs with 163 Federal PODs.
April 6	09:33	VNN report: The State Epidemiologist stated that 46 PODs were open.
April 6	09:45	VNN report: Deputy Commissioner Blumenstock (NJ DHSS) reported that 40 PODs are operational.
April 6	14:50	NJ EOC shift-change brief notes that there are 160 PODs operating in Essex, Union, Middlesex, and Hudson counties.
April 6	15:15	According to the NJ PFO, there are currently 280 PODs active in New Jersey.
April 6	16:30	SERT announces that 300 PODs are active in New Jersey.
April 6	18:57	Displays in the Emergency Response Team – Advance Element (ERT-A) indicate that there are 285 active PODs in New Jersey, including 163 USPS sites.
April 6	21:15	NJ DHSS states that, as of 18:30 on April 6, 456 State and Federal PODs were operating (211 at high schools, 56 at colleges, and 189 by HHS).
April 6	21:30	The NJ State Police-OEM situation report (SITREP) #12 stated that 456 PODs are active in New Jersey.
April 7	08:30	State EOC briefing noted that 129 USPS PODs are active.
April 7	10:15	Briefing from the Governor's Office indicated that 267 (211 high schools and 56 colleges) and 189 Federal PODs are active.
April 7	10:40	Health Command Center (HCC) reports that the following PODs were open: 163 post offices, 7 VA hospitals, 19 HRSA community health centers, 20 community Local Information Network and Communications System (LINCS) (Federal total = 209). A total of 248 State PODs were open.
April 7	10:58	OEM and Governor's Office are using the following POD figures: 189 Federal and 267 State (from NJ Health Operations Tracking System

Date	Time	Event
		[HOTS] log).
April 7	12:00	All Federal PODs were demobilized (other reports indicate that the Federal PODs closed at 02:00 on April 7).
April 7	14:00	HCC list of active PODs included: 248 schools, 163 post offices, 7 VA hospitals, and 19 HRSA community health centers (total = 437).
April 7	18:30	NJ governor's office reported that New Jersey had opened PODs at 211 high schools and 56 colleges. HHS had opened 189 PODs at post offices (total = 456).
April 7	19:30	Defense Coordinating Officer (DCO) brief at the JFO reported that 248 State and 189 Federal PODs were active.

Table IV-1 clearly indicates that uncertainty about the number of active PODs was common and widespread. This inconsistency suggests that the planning process was incomplete and that information about the two systems was not being shared among Federal and State agencies. For example, representatives from the JFO were unable locate the list of State PODs. In addition to the evidence in Table IV-1, there are no indications that a complete list of PODs existed. The list assembled by the NJ State EOC contained the location of 124 post offices and 456 State PODs operating at NJ high schools and colleges. However, it omitted the 22 real PODs and 39 notional PODs (13 post offices, 19 HRSA facilities, and 7 VA hospitals). Ready access to accurate information from such a list is critical to the response, because this information would be used to inform SNS delivery staff, POD workers, and residents on where to go.

d. Management of Staff Resources

The POD plan developed during the exercise was incomplete and did not address the staffing needs required to provide prophylaxis to every State resident. Officials in New Jersey did not establish a staffing requirement or develop a mechanism for integrating the additional workers into the two POD systems. Without these elements, Federal and State officials could not develop an executable plan for the two systems. In many respects, these problems reflect problems associated with attempting to carry out this scale of prophylaxis for the first time right in the middle of the public health emergency.

Uncertainty about the number of workers per shift and the number of PODs needing to be staffed frustrated efforts to define the staffing requirement. Estimates of the number of personnel varied from 10 per shift at the USPS PODs to 183 per shift as prescribed in the *New Jersey Mass Prophylaxis Manual*. Without an agreement on the staffing levels at the PODs or the number needing to be staffed, it was difficult to establish a requirement or track progress made toward staffing them.

The existence of State and Federal systems created additional problems for those responsible for staffing the PODs. When officials would identify a group of medical

professionals or security personnel staff, it was sometimes unclear whether these resources would be used to staff Federal locations, State locations, or both. The State submitted one ARF in which the State EOC requested security personnel for both State and Federal PODs. Table IV-2 documents the ad hoc search for workers that occurred during the exercise.

Table IV-2. Uncertainty Surrounding the Staffing of NJ PODs

Date	Time	Event
April 5	17:00	HHS is looking into a memorandum of understanding (MOU) with the USPS about delivering medications. HHS indicated that 3,300 health care workers are available. HHS determines USPS MOU is not feasible.
April 5	19:50	ESF-8 directs SERT and DoD to provide all available personnel to staff PODs with VA, DoD, DHS, National Disaster Medical System (NDMS), and Medical Reserve Corps (MRC). The requirement is to provide 15,000 personnel.
April 5	20:30	In a teleconference between State officials and HHS, HHS indicates that it has 1,400 personnel ready to staff PODs (five public health officers per shift to support USPS staff).
April 6	09:50	NJ officials state that 15,000 POD workers will be trained Wednesday morning (April 6) and then be assigned to PODs.
April 6	10:14	The FEMA ERT-A is trying to arrange security for 400 NJ PODs.
April 6	10:37	At the morning brief, the ERT-A Ops chief, FCO, and SCO note that 163 Federal PODs will be open today and staffed by the MRC.
April 6	12:00	The RRCC reports that Federal PODs are almost completely staffed, and the Federal Protective Service is providing security (potentially augmented by NJ National Guard).
April 6	15:01	In an e-mail, the IIMG and DHS staffs were observed attempting to resolve confusion over which organization (e.g., Federal Protective Service, NJ National Guard, or U.S. Postal Inspectors) would provide security at the Federal PODs.
April 6	16:10	FEMA has received an official request from New Jersey for 4,000 POD security personnel and 200 POD logistic elements.
April 6	16:55	There is a request to provide 2,000 POD workers from the American Red Cross.
April 6	18:11	There is an ARF for armed security at the PODs. The ARF is a request to provide 10 armed security personnel per Federal POD, for a total of 1,680.
April 6	21:15	In a LINCS e-mail, NJ DHSS states that staffing at the State PODs included school nurses, NJ National Guard (three to four soldiers per shift), Emergency Management Assistance Compact (EMAC) from 20 States, 15,000 State workers, local law enforcement, and 4,200 community emergency response team members.
April 6	21:30	The NJ State Police-OEM SITREP #12 states that Oklahoma will send two 16-

Date	Time	Event
		person teams to assist PODs with distribution of pharmaceuticals.
April 7	09:10	The FEMA Emergency Services Branch Chief is in contact with NJ State Police to backfill 4,000 officers for POD security.
April 7	09:45	NJ National Guard needs clarification on a request to provide security to 248 PODs.
April 7	09:54	An MA from FEMA to DoD to provide POD medical personnel is pending.
April 7	13:00	The NJ Department of Military and Veterans Affairs (DMAVA) informs the State EOC that it will assign four soldiers on two shifts to provide security at the State's 267 PODs.
April 7	13:02	HHS plans to release 1,200 Public Health Service staff from supporting PODs and use them to help fulfill the NJ request for 12,000 health care professionals.
April 7	14:15	Federal POD prophylaxis has been completed. The personnel (1,200 U.S. Public Health Commissioned Corps and 3,000 MRC) were reassigned to State PODs.
April 7	16:30	ARF 20 (requesting 4,000 law enforcement officers for POD security) is still being worked by JFO Emergency Services.

The impromptu nature of the staffing process highlighted in Table IV-2 illustrates the difficulty of staffing hundreds of PODs with thousands of workers within a short period of time without the benefit of a detailed pre-incident Federal-State plan covering this possibility.

The data also suggest that State and Federal officials were still identifying staffing sources (e.g., American Red Cross, MRC, and NJ National Guard) on the last full day of the exercise. For example, the Federal Protective Services (FPS), which was responsible for coordinating security forces for ESF #13, received confirmation of a NJ request for 4,000 security personnel to support operations at 11:50 on April 7 (11 hours before the State PODs were scheduled to close). It is unlikely that the FPS could have processed such a request and provided the requested level of support by the time that all State PODs would have closed.

The conclusion that statewide prophylaxis was completed by midnight on April 7 is based upon the operation of a large number of notional PODs; however, the data in Table IV-2 indicate that an executable staffing plan for these PODs had not been developed by this deadline. Even if a staffing requirement had been established and a mechanism to integrate Federal and State resources was available, the lack of readily available workers would have adversely affected activation timelines and throughput rates.

Theoretically, it was possible to meet the stated goal of distributing prophylaxis to every NJ resident by 23:00 on April 8. Table IV-3 summarizes the potential throughput of the NJ PODs during the exercise.

Table IV-3. Notional Statewide Prophylaxis

PODs	Maximum Hours of Operation			Assumed Throughput (per Hour)	Total Throughput (Notional)
	Begin	End	Hours		
State PODs [58]					
22 Planned PODs	08:00 Apr. 5	24:00 Apr. 7	64	1,000	1.4 million
200 High Schools/Colleges	08:00 Apr. 6	24:00 Apr. 7	40	1,000	8.0 million
Federal PODs [59]					
137 Post Offices	08:00 Apr. 6	12:00 Apr. 7	28	750	2.9 million
19 HRSA Centers	08:00 Apr. 6	12:00 Apr. 7	28	1,000	.5 million
7 VA Hospitals	08:00 Apr. 6	12:00 Apr. 7	28	1,000	.2 million
Notional Total					13.0 million

Table IV-3 indicates that the plan adopted by New Jersey and the Federal government made it theoretically possible to process 13 million residents through the State and Federal POD systems. This outcome would have depended upon the rapid activation of POD sites and throughputs of 750 (at USPS sites) and 1,000 (at all other PODs) people per hour among numerous factors.

Activation timelines depicted in Table IV-3 were unrealistic. The personnel needed to staff the 385 PODs had not been identified by the end of the exercise; therefore, they could not all have opened by the stated times. To meet the stated timelines, both the State and Federal POD activation processes had to be completed less than 18 hours from the point at which the decision to open the sites was made. Activation requires site preparation, staffing, delivery of supplies, and public notification. The staffing process includes identifying, notifying, and transporting qualified personnel. As noted earlier, the necessary workers were not in place when PODs were scheduled to open. Some Federal resources, such as the MRC, may not be currently available.

The *New Jersey Mass Prophylaxis Manual* states that a staff of 183 is required to process 1,000 people per hour (the plan also assumes an eight-hour shift). Using this standard, State and Federal planners would have to identify, notify, and transport more than 210,000 workers to operate the 385 PODs 24 hours per day.[60] Operating them with only

[58] The actual number of State PODs was never definitively established. Available data suggest that approximately 222 (200 notional and 22 real) State PODs were activated.

[59] The list of PODs provided by the NJ State EOC contained 124 POD postal facilities; however, the numbers used in this table were widely cited during the exercise.

[60] This also assumes that the right mix of skills is present and that the staff has been properly trained.

10% of the planned staffs (e.g., 27 staff members per 12-hour shift) would have required approximately 21,000 workers. It is not clear that the Federal and State governments could have even met the 10 percent threshold.

Identifying sources of staffing is just the first step in a process that could take several days. After identifying the source, the organizations have to be tasked and the workers have to be notified. Once notified, the workers may have to travel significant distances. For example, workers from EMAC were drawn from 20 States. These observations suggest that many of the notional PODs did not have the required staffs and could not have opened. Many of those that could open would have been minimally staffed. These understaffed PODs would have been unlikely to process 1,000 POD visitors per hour.

e. POD Throughput Rates Lower than Target Goals

Observations made during the exercise at the 22 real PODs suggest that the target throughput rate of 1,000 people per hour greatly overestimated the actual rate. Table IV-4 summarizes the throughput observations made during the exercise by data collectors assigned to these PODs. In some instances, the data collectors counted the number of patients processed.[61] They also noted numerous instances in which "bottlenecks" and "backups" slowed the processing of POD patients.

Table IV-4. T3 FSE POD Throughput Observations

Locale	Hours of Operation	Total Throughput	Hourly Throughput	Data Collector Observations on POD Throughput
Atlantic	3.0	935	311	"Overwhelmed," "jammed-up," and "very backed-up"
Bergen	2.5	No data	No data	No comments
Burlington	1.0	No data	No data	"[The POD is] … too small for 500 patients per hour."
Camden	2.5	282	113	No comments
Cape May	3.0		300	"Long lines" and "stalling"
Cumberland/ Salem	3.0	784*	261*	"Backing up"
Essex	3.5	No data	No data	"Long lines," "backing up," "excessive numbers in line," and "little movement"
Gloucester	3.0	388*	129*	"Long lines," "backup," and "backlog of more than 50"
Hudson	2.5	1,949*	780*	"Huge bottlenecks" and "backlog"
Hunterdon	4.5	No data	No data	"Backing up" and "bottleneck"

[61] Data about the staffing levels at the PODs were not available.

Locale	Hours of Operation	Total Throughput	Hourly Throughput	Data Collector Observations on POD Throughput
Mercer	4.5	545*	121*	"Long lines," "back-upped," "overwhelmed," and "much confusion"
Middlesex	3.0	420	140	No comments
Monmouth		No data	No data	No comments
Morris	2.0	No data	No data	No comments
Newark	4.5	655	146	"Bottleneck"
Ocean	2.0	No data	No data	"Congestion" and "backup"
Passaic	1.0+	No data	No data	No comments
Paterson[62]	2.0	120	60	"Confusion" and "problems"
Somerset	2.5	No data	No data	"Backlog"
Sussex	2.5	No data	No data	"Overwhelmed" and "backed-up"
Union	3.0	1,223*	408*	"Backlog" and "backing up" "Patient flow slowed to nonexistent."
Warren	2.5	No data	No data	"Backup" and "bottleneck"

* These numbers indicate the patients that received medication. Some individuals would have been sent home without medication or sent to a hospital for treatment.

Throughputs observed at the PODs were significantly lower than the planning factor of 1,000 people per hour that was used to model prophylaxis progress in the exercise. However, the rates observed in the T3 FSE are not inconsistent with throughputs observed at exercises designed to test throughput at a POD. An exercise in which residents of Washington, D.C., were exposed to the plague found that a POD staff of 57 (not including security) could process (i.e., screen patients and distribute antibiotics) approximately 111 patients per hour.[63] In April 2003, Arlington County, VA, in conjunction with HHS, tested the CDC model smallpox mass vaccination clinic and found that a staff of 47 (not including security) could process approximately 104 patients per hour.[64] The results from these studies and others,[65] as well as the observations,

[62] Paterson POD experienced a real-world bomb scare during exercise play which may have affected throughput numbers

[63] Monica Giovachino, Thomas Calhoun, Neil Carey, Briant Coleman, Gabriella Gonzalez, Bernard Hardeman, Brian McCue. Optimizing a District of Columbia Strategic National Stockpile Dispensing Center. *Journal of Public Health Management and Practice*, 2005, 11(4), 282–290.

[64] Brian G. McCue and Monica J. Giovachino, *A Field Test of the CDC Smallpox Vaccination Clinic Model*, The CNA Corporation, IPR 10847, April 2003.

[65] See additional studies cited in Brian G. McCue and Monica J. Giovachino, *A Field Test of the CDC Smallpox Vaccination Clinic Model*, The CNA Corporation, IPR 10847, April 2003.

indicate that the planning throughput of 1,000 people per hour probably overestimates the number that could be processed.

f. Weighing Trade-offs When Making Prophylaxis Decisions

During the exercise, the decision was eventually made to distribute antibiotics to the entire population of New Jersey. NJ public health officials preferred targeted prophylaxis that would concentrate distribution efforts in areas most affected by plague. Public health officials were concerned that the State could not staff the number of PODs needed to distribute prophylaxis to New Jersey's 8.8 million residents. These officials also noted that distributing prophylaxis to everyone in areas where there were few cases of plague would have a marginal impact on the spread of the disease. Finally, they were concerned that prophylaxis distribution on this scale would divert resources away from areas heavily impacted by the disease and would endanger some residents (e.g., those living in areas with few plague cases) who were allergic to antibiotics. Despite these concerns, the political leadership pressed ahead with this decision.

The T3 FSE cannot be used to assess the technical details concerning which prophylaxis approach (i.e., widespread or target distribution) was the correct choice; however, the exercise did illuminate important issues associated with the decision.

Logistical and resource requirements associated with a more targeted prophylaxis would have been significantly less than the requirement for statewide prophylaxis. Choosing targeted prophylaxis would have simplified the POD planning process and applied the available resources to areas with the greatest need. The decision to pursue statewide prophylaxis increased the complexity of the planning process and created resource demands that could not be satisfied by the combination of State and Federal agencies.

Although targeted prophylaxis requires fewer resources to execute, it does require significant data collection and analysis capabilities. When the release of a biological agent is suspected, response personnel and decision makers use epidemiological models, perhaps coupled with physical dispersion models, to determine the likely exposure location and to identify the at-risk population. Building accurate dispersion models requires information about the weather conditions, type of agent, method of dissemination, type and purity of the agent, time of the release, and extent of contamination (e.g., ground sampling results) for the case of an outdoor release of an aerosolized agent. These data are collected by several different organizations and are often incomplete during the initial phases of the response.

Epidemiological models require a case definition and information from patients who present at health care facilities. During major disasters (e.g., terrorist incidents or public health emergencies), health officials assemble individual case definitions to identify clusters of victims. Patient data may be held by different organizations (e.g., multiple hospitals and private physicians) and are often incomplete during the initial stages of a public health emergency. To construct an accurate epidemiological model, public health officials must collect and analyze these data.

Dispersion models that are consistent with clusters of victims provide strong evidence that response officials have identified the release area. With dispersion models and epidemiological case information, officials can identify the release area and identify populations that are most in need of prophylaxis. In contrast, the primary pieces of information needed to support the decision to distribute prophylaxis to everyone are the identity of the agent and a definition of the target population (i.e., what constitutes a "resident").

Targeted prophylaxis has different public information requirements. In their public messages, officials must differentiate between the at-risk population and those who do not need prophylaxis. Furthermore, the public message must allay the concerns of those who should not receive prophylaxis. Otherwise, PODs may be overwhelmed by the arrival of too many individuals. The public message needed to support statewide prophylaxis can be less sophisticated; it simply needs to direct everyone to visit a POD as soon as possible.

Early-warning biological detection systems, such as BioWatch,[66] are intended to notify public health experts of the presence of a biological release and then assess the geographic extent of the contamination. Such information would aid officials in identifying the population most at risk and in determining which prophylaxis policy to pursue. Biological sensor systems could provide indications of the presence of plague 24 to 36 hours sooner than relying on symptomatic case identification.

Although a more focused prophylaxis effort may increase the possibility that some residents who need prophylaxis do not receive it, it can also reduce the distribution of prophylaxis to people for whom it is contraindicated. A prophylaxis effort of the scale notionally exercised in New Jersey will unnecessarily expose many more of these persons to potentially adverse effects, particularly if the standard of care is reduced in response to staffing shortages.

3. Issues from Previous Exercises

Like T3, T2 also exercised the SNS requisition process and the distribution of prophylaxis. Participants also raised related concerns during SOEs 05-2 and 05-3. Table IV-5 highlights issues across these exercises.

[66] http://www.milnet.com/wh/DoHS/BioWatchFactSheetFINAL.pdf (downloaded July 17, 2005)

Table IV-5. Comparison of T3 FSE with Previous Exercises

T2 FSE	SOEs 05-2 and 05-3	T3 FSE
SIGNIFICANT DECISIONS		
• HHS directed CDC to pre-deploy SNS push packs (prior to formal requests for SNS) to Illinois. • The State also requested follow-on managed inventory supplies. • After issuing medications to first-responder population, SNS sites opened to target population by Day 4. • After some discussion over the ability to conduct mass prophylaxis, local jurisdictions agreed on a common, targeted prophylaxis strategy.	N/A	• NJ Governor requested SNS on Day 1 upon awareness of a plague outbreak. • NJ Governor decided to execute a statewide prophylaxis strategy, though State health officials recommended a targeted approach. • First State POD opened in one of the two most-affected counties by noon on Day 2. • The Federal government, concerned about the State's ability to execute its plan swiftly enough, decided to supplement the State PODs with more than 160 of its own sites located at postal facilities and private HRSA centers.
ISSUES/OBSERVATIONS		
• Multiple requests for SNS from local jurisdictions; uncertainty about request procedures (via FEMA or CDC)	N/A	• Single request from Governor directly to CDC
• Significant uncertainty about amount of medications in SNS	• Lack of consistent understanding among Federal D/As regarding capabilities (limitations of current national medical health care resources)	
• Concerns expressed by local jurisdictions regarding tradeoffs of targeted or mass prophylaxis strategies *Some counties favored the targeted approach because they lacked the resources for mass distribution; those favoring a mass approach were concerned about being flooded with people from jurisdictions using a targeted approach.*	• Concern regarding ability to securely and swiftly breakdown and distribute the SNS on a massive scale (i.e., statewide prophylaxis strategy)	• Throughput of real State PODs fell short of assumed rate of 1,000 people/hour, a key assumption behind the mass prophylaxis decision adopted by the State. • Resources required to staff the nearly 400 State and Federal PODs were not identified and were probably unavailable in the time frame of interest. • The plan to conduct mass prophylaxis evolved during the exercise and did not appear to reflect a preplanned, carefully integrated Federal-State response. • Not clear that the Federal government has a strategy for implementing its own system of PODs or for rapidly identifying and supplying staff to support State efforts for large-scale requirement
	• Concern regarding emergency authorizations for new drugs or use of drugs for non-approved use	

F. Recommendations

- States need to work with the Federal government to develop scalable prophylaxis plans that contemplate a requirement to reach very large numbers of people. T3 indicates the difficulty of doing this while an event is unfolding.
    - These plans will most likely require a combination of approaches, including fixed sites and delivery of prophylaxis directly to individuals.
    - There may be a requirement for flexible standards of care associated with different levels of prophylaxis.
    - States will need to clearly identify what Federal resources, if any, would be required to support these plans.
- Careful integration of Federal and State planning processes is required to ensure that mass prophylaxis plans will be executable if needed.
    - The new HHS Regional Emergency Coordinators who report through the Office of the Assistant Secretary for Public Health Preparedness are well situated to facilitate this process.
    - Prophylaxis/planning practices and tools developed under the CRI should be expanded to include regions and cities not currently covered.
    - Options (including the appropriate mix of PODs plus other prophylaxis delivery techniques) for conducting large-scale prophylaxis should be studied, and guidelines should be developed.
- The Federal government should decide whether it will establish and operate its own POD systems in the event of a major public health emergency like the one that occurred during T3.

Even if it is not the intention of the Federal government to establish and operate its own POD systems in the event of a major public health emergency, plans should be made to quickly identify and provide staffing resources to States facing a need to carry out prophylaxis on a large scale, should their own resources prove inadequate.

IV. Agent Confirmation and Hazard Area Definition— Task # IV-6: Direct Agent Release Mitigation Efforts

A. Summary of Issue

The issue is that specialized response units did not exhibit a clear understanding of each other's roles, authorities, and standard operating procedures. Additionally, the lack of a formally defined information flow process from the incident site resulted in premature public messages and decision making about the identity of the chemical agent.

In a chemical, biological, or radiological attack, early identification of the lethal agent, combined with clear definition of the hazard area and the potentially exposed population, can save lives, speed effective treatment of symptoms, and prevent injury to medical responders. These essential elements of information drive decisions made by top officials at FSL levels. Information critical to rapid and effective response activities includes understanding what lethal agents were released, where they were released, and where the contamination is likely to spread. Scientists have developed plume models, which make use of available data to predict atmospheric transport of pollutants and to define spread of the agent. Models may also provide information that can help identify the timing and initial location of the agent release. Until recently, there was no single Federal source for collecting data and producing the modeling products used by decision makers. The T3 FSE provided the opportunity to observe progress that has been made in creating a single authoritative Federal source for plume modeling, while highlighting issues that remain in coordinating data and information to confirm the agent and define the hazard area.

The T3 FSE highlighted the potential for tension when many organizations participate in the sampling process and when information about the agent is not systematically distributed among the response organizations. The response in Connecticut exercised the use of the Interagency Modeling and Atmospheric Analysis Center (IMAAC) as the sole Federal source of plume modeling during INSs. Observations indicate that the single-source IMAAC approach resolved much of the confusion about plume models noted during previous exercises. IMAAC products provided authoritative plume predictions that were used by all the response organizations to define the hazard area and make associated decisions; however, problems with version control as well as lack of consolidation and confirmation of model inputs were evident during the exercise.

Although the T3 FSE provided opportunities in New Jersey and Connecticut to learn about agent confirmation and hazard area definition during a major disaster, this analysis focuses on the observations and issues in Connecticut. Whereas plume modeling would be an important element of a real-world response to a plague release, exercise designers chose not to include it as part of the NJ exercise program; therefore, the IMAAC processes were not exercised in New Jersey and the IMAAC did not produce any official products for the plague release.

B. Background

During WMD events, identification of the agent and definition of the hazard area provides information that governmental agencies can use to tailor the response and protect at-risk populations. Without ready access to this information, response organizations must make guesses about the type of agent and the boundaries of the hazard area, thereby reducing the effectiveness of the response and possibly endangering the responders and residents.

1. Agent Identification and Confirmation

Various FSL agencies have the capacity and responsibility to test for the presence and identity of WMD agents. Fire department personnel, specialized HAZMAT units, environmental agencies, and law enforcement personnel may perform environmental sampling. Medical personnel may collect samples from individuals to provide additional data about the agent. The overarching goal of all agencies is to identify the agent used in the attack and the extent of its spread. However, these agencies represent three different areas of interest: (1) first responders, (2) law enforcement, and (3) environmental remediation. Each interest group uses the results from the sampling differently and largely operates during different response phases: initial response to the emergency, criminal investigation, and clean up. Although the term "response phase" indicates a change in focus as a response progresses, there really are no clear lines of demarcation between the phases. Rather, overlapping and integrated operations occur across phases, with the understanding that priorities change over time.

Fire and emergency medical services (EMS) personnel use the testing results to determine immediate treatment protocols and the appropriate personal protective equipment to use during the response period. Health care officials use the identification information to determine the best treatment for patients. Law enforcement uses results of the tests to support the investigation and prosecute suspects. Environmental agencies use sampling to determine the extent of contamination and the best methods for remediation. Fire/EMS/medical personnel and environmental specialists could be grouped together based on their public health focus, with the former being concerned with immediate health effects, and the latter with a long-term perspective on the issue. To support their missions, all interest groups have developed and fielded the ability to collect samples and identify unknown agents.

2. Hazard Area Definition

When the presence of a chemical, biological, or radiological agent is suspected, response personnel and decision makers may use plume modeling and case definitions to determine the likely hazard areas and identify at-risk populations. With this information, responders can tailor their response to the scenario and decision makers can begin to craft policies that best address the circumstances of the release.

Plume models provide scientific predictions of how an agent will disperse given weather conditions and other factors. Initial plume predictions may be of limited value due to lack of knowledge about the means of dispersal, amount of agent released, and composition of the agent. However, these products still give decision makers some baseline information from which to craft a response. As more evidence is collected and field measurements are obtained, models are refined with this empirical data to produce more accurate analyses of the extent and spread of contamination. Model products are displayed via Geographical Information Systems (GIS) with affected population counts and detailed maps. With these products and reach-back support from modeling experts, top officials can make informed decisions about protective actions and response needs.

At the Seattle, WA, RDD site during T2, the collection and analysis of data by multiple agencies at all levels of government resulted in inconsistent and potentially conflicting plume products. That experience prompted DHS and the HSC to create the IMAAC as the single source of Federal plume modeling and analysis in the event of an INS. The IMAAC is intended to be the center or facility where all agencies who support hazard area modeling for different consumers can co-locate representatives to participate in analysis and reach consensus on products. Under the MOA that established the IMAAC, agencies with particular customers, such as the Defense Threat Reduction Agency (DTRA), continue to deliver products to their customer(s) but coordinate with the other agencies in the IMAAC to reach a consensus on the assessments during an INS. The National Atmospheric Release Advisory Center (NARAC) at Lawrence Livermore National Laboratory (LLNL) in California currently functions as the interim IMAAC facility. The IMAAC accepts inputs and product requests from any of the Federal agency signatories to the MOA, any State or tribal organization, and any FSL emergency response organization. End users can download the IMAAC products from the NARAC secure website or can request receipt over e-mail. The goal of the IMAAC agreement is to reduce confusion and uncertainty among response organizations about the plume models. By providing an authoritative, single source for plume predictions, IMAAC can contribute to a shared situational awareness among response organizations.

The IMAAC policy was codified in the NRP and in an MOA sponsored by DHS. The signatories to the MOA include the Department of Energy, Department of Commerce, DoD, Department of the Interior, National Air and Space Association (NASA), Nuclear Regulatory Commission (NRC), Environmental Protection Agency (EPA), and DHS.

C. Reconstruction

The T3 FSE provided an opportunity to learn about the response mechanisms that officials use to identify and confirm unknown WMD agents and define hazard areas during an incident response. In Connecticut, officials were responding to the release of a fast-acting sulfur mustard agent, from which victims exhibited symptoms within hours of exposure. The terrorists used two methods to disseminate the mustard agent in Connecticut. First, at approximately 11:30 on April 4, a small aircraft flew over the New London City Pier on the Thames River releasing mustard in a gaseous form over the waterfront area. Roughly two hours later, at 13:20, a VBIED, hidden in the back of a

truck that also carried sulfur mustard detonated at the head of the pier. Most of the mustard agent present in the truck bomb was destroyed during the explosion, limiting contamination to the immediate vicinity of the detonation, where a pool of mustard agent had collected prior to the explosion. The aircraft release contaminated a much larger area and had a greater impact on the people attending the festival at the pier.

1. Agent Identification and Confirmation in Connecticut

The New London Fire Department first responders arrived within five minutes of the blast, and recognized immediately that the victims at the pier were suffering from more than just the effects of a truck bomb. Their initial monitoring and metering revealed the presence of a chemical agent. From there, the Incident Commander (IC) coordinated all the HAZMAT and specialized units that arrived on scene to test for the agent. With the FBI WMD Coordinator advising, the IC developed a testing plan that increased in sophistication as it progressed while limiting contamination of evidence and duplication of effort. First, the CT State Police Emergency Services Unit (ESU) entered the scene to conduct paper tests, which revealed the area to be positive for a blister agent. Next, the CT National Guard Civil Support Team (CST) was sent to the perimeter of the site to monitor air and wind movements to make sure the wind did not shift and contaminate the first responders. Based on the paper tests, air monitoring, and victim symptoms, a presumptive positive assessment of mustard agent was made at 15:37 and passed to operating centers and decision makers. At this time, there was no scientific evidence of mustard agent.[67] The next test, by the CT DEP HAZMAT Unit, used a gas chromatograph mass spectrometer (GCMS) to survey the clothing of one of the victims. This test came back negative, an artificiality of the exercise that may have changed the course of the testing plan if not for the controller intervention. Fourth, the National Guard CST used a second, more advanced GCMS to test a clothing sample. Per the Master Scenario Event List (MSEL), this test at 20:17 was positive for mustard. Although the equipment used by the DEP and CST is virtually identical to that used in a sanctioned laboratory, the environment is not considered pristine enough for definitive testing, particularly for a criminal investigation. Field tests are usually considered preliminary results, with definitive testing occurring in a laboratory. Very early on in the response, the CT State Police ESU collected a sample for the FBI to send to the Edgewood Chemical Activity (ECA) in Aberdeen, MD, for definitive testing. At 08:40 on April 5, the ECA confirmed that the samples contained mustard.

Concurrent with the efforts at the incident site, the CT Department of Public Health (DPH) initiated its own line of testing to confirm the identity of the chemical agent. CT DPH received notification of the preliminary mustard identification, but questioned the source and accuracy of the information. Not knowing about the airplane dispersal, which occurred two hours prior to the explosion, CT DPH and the treating hospitals reasoned that the contaminant could be lewisite, rather than mustard, because of the apparently

[67] Although it is possible that the initial tests and victim symptoms would have led responders to suspect mustard, it is unlikely that they would have been as certain in their diagnosis if not for the artificiality of the exercise. All participants knew ahead of time that the agent being simulated was mustard.

short time span between victims being contaminated via the truck bomb and victims becoming symptomatic. Using skin and blood samples from patients, the CT DPH laboratory confirmed the presence of mustard at 01:34 on April 5.

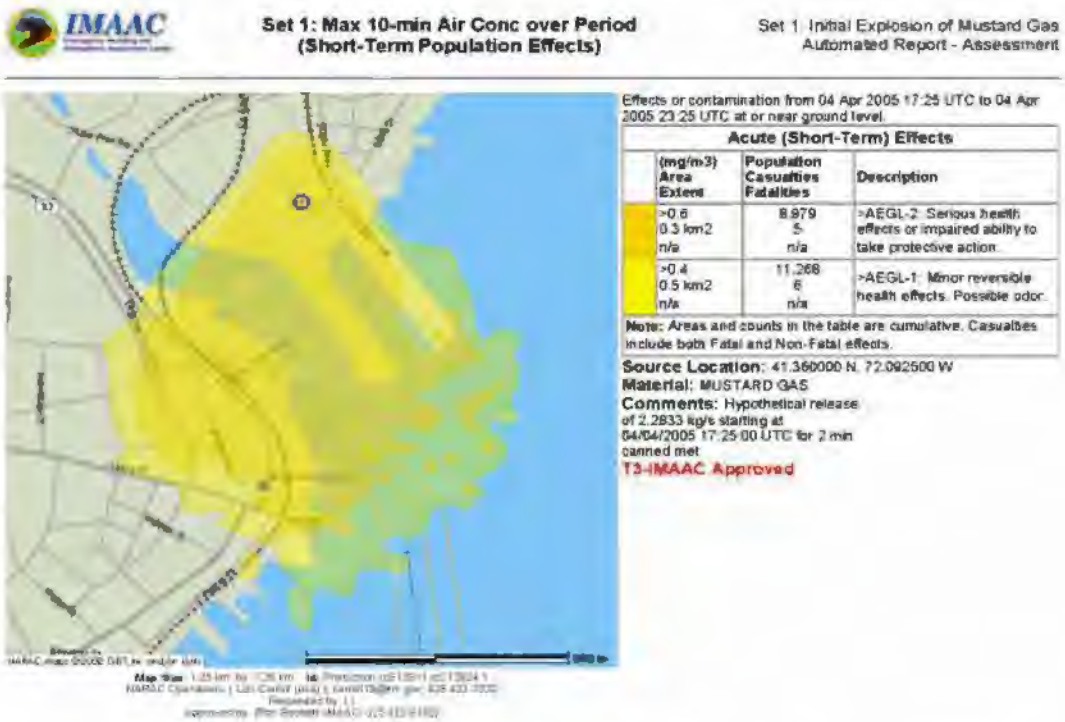
2. Hazard Area Definition in Connecticut

Even before the agent was identified, officials in Connecticut implemented two approaches to define the hazard area: plume modeling and environmental sampling.

The IMAAC was alerted to the explosion by VNN shortly after the bomb detonated. Once alerted, the IMAAC began modeling the potential effects of a chemical release in the event that such a release had occurred concurrent to the explosion. At 13:40, the IMAAC Operations cell began conducting sample runs of a plume model using mustard as the agent.[68] The DHS Science and Technology (S&T) Division watch officer at the HSOC activated the IMAAC at approximately 13:53. IMAAC was asked to produce an initial set of plume products based on VNN reports, with more detailed information to be included as it became available. The IMAAC released the first plume product via the NARAC website at 14:36. Figure V-1 shows the initial plume prediction.

[68] Although the fortuitous use of mustard in the earliest run model was likely an artificiality of the exercise, the fact that IMAAC began modeling even before formal notification is not unusual. IMAAC operations personnel report that learning of any bombing, accidental release or spill, or national emergency would activate an informal IMAAC modeling response in the event that formal activation occurred.

Figure V-1. Initial IMAAC Plume Model Released at 14:36 on April 4

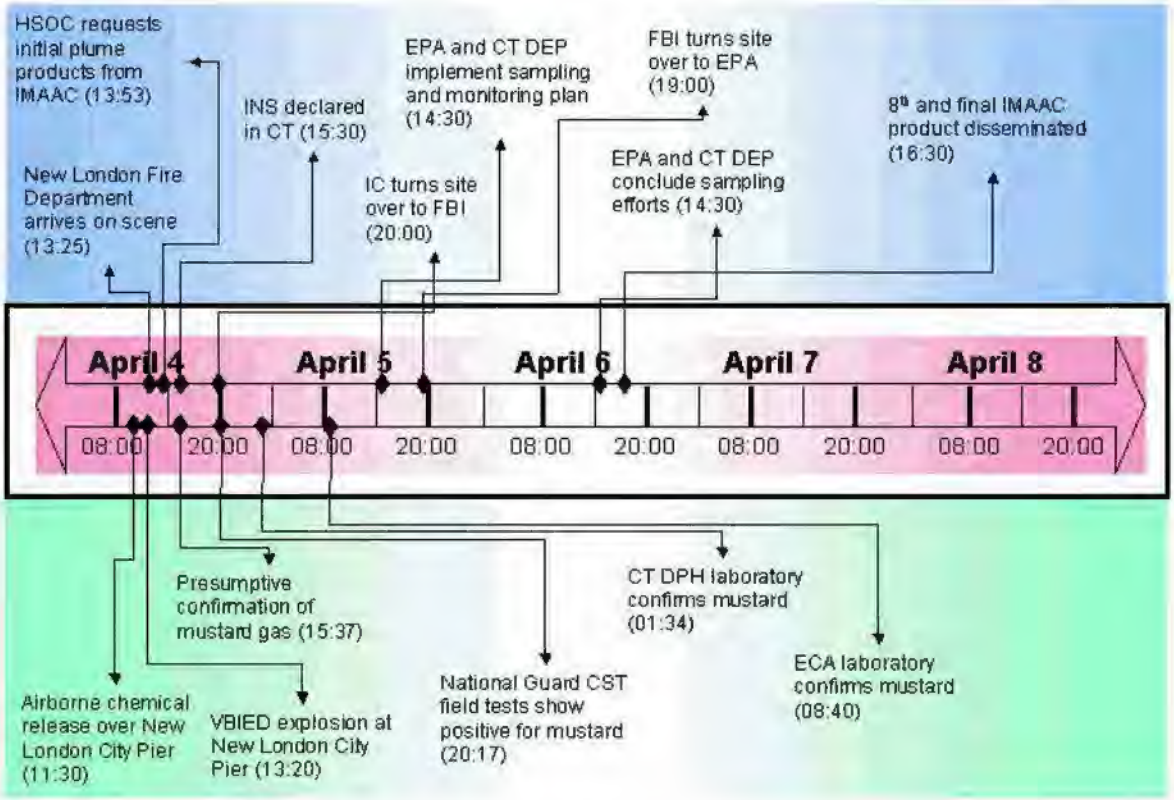


At 15:30 on April 4, the Secretary of Homeland Security declared the events in Connecticut an INS and by default identified the IMAAC as the single source for Federal plume models of the effects. Over the next four days, the IMAAC released seven additional sets of plume products, as well as some revisions to specific model runs within the sets.

Under the authority of the NCP, the EPA, U.S. Coast Guard (USCG), and Connecticut DEP developed a sampling and monitoring plan to detect the continued presence of mustard agent and delineate the extent of contamination. On April 5, sampling and air monitoring teams comprised of personnel from the Connecticut DEP HAZMAT Team, EPA Region 1 HAZMAT Team, EPA Superfund Technical Assessment and Response Team (START), and USCG National Strike Force/Atlantic Strike Team (NSF/AST) implemented the plan in the areas immediately surrounding the incident site. Early evening on April 5, the teams received access to the hot zone at the incident site for testing purposes. Field operations concluded at 14:36 on April 6, with a total of 36 samples taken. The results from these field samples were sent to the IMAAC and contributed to the development of more accurate plume products.

Figure V-2 shows key events in the Connecticut incident and response.

Figure V-2. Key Events for Agent Identification and Hazard Area Definition in Connecticut



D. Consequence

Exercise play in Connecticut presented response organizations with an opportunity to exercise the coordination processes required for identification of the chemical agent and definition of the hazard area. Overall, these activities appeared more coordinated, efficient, and successful than in T2. In particular, the T3 FSE also showed how much improvement has been made since T2 in coordinating and developing analysis products to support top officials' decision making about the hazard area and the effects of contamination on the population. Despite these success stories, T3 showed that room for improvement still exists.

T3 illustrated the potential for tension when many organizations participate in response activities without a clear understanding of the roles, standards, and operating procedures of other responders on site. This tension is neither new nor unexpected. However, such issues take on added weight when they have repercussions that reverberate up the entire response chain. In Connecticut, these tensions manifested themselves onsite in disagreements between different chemical sampling units and communities. Among the

results was a delay in top officials receiving essential elements of information to help with decision making and the contamination of evidence that could be needed for criminal prosecution.

Play in T3 duplicated that of T2 in terms of a breakdown in information flow from the incident site to the other organizations and operating centers in the response chain. In T3, this was evidenced by many incorrect and unconfirmed reports of the agent being mustard. T3 showed that a systematic process for releasing information from the site does not exist. The result is presumptive and potentially incorrect information being used by decision makers and given to the public. In the T3 FSE, responders were fortunate that the rumors and preliminary reports were accurate. In the future, responders may not be so fortunate. Information about the contaminating agent, and any other essential elements of information that may drive FSL actions as well as public responses, needs to come from a single authoritative source that is acknowledged as such by the entire response chain.

The use of the IMAAC in T3 as the single authoritative source for Federal plume products resulted in dramatically less confusion regarding such products than in previous exercises. The few problems that occurred involving version control and non-IMAAC analyses were insubstantial and could be attributed to technology issues. That being said, the IMAAC processes for receipt and review of other modeling products may need to be reclarified, and a protocol may need to be established for other modeling agencies to distribute to their consumers on the purpose of their products and the guidelines for redistribution.

Events in T3 indicate that the creation of IMAAC as the single source for plume products was a good decision. Now, however, processes associated with providing data and requesting products may need to be reexamined. The IMAAC is not equipped to consolidate the inputs it receives and resolve discrepancies among them. Serious consideration should be given to the decision to allow multiple agencies at FSL levels to have direct access to the IMAAC operations cell. The response flexibility granted by such access should be weighed against the potential for conflicting inputs or requests. Procedures need to be developed on how the IMAAC should handle discrepancies in data inputs and requests that do not align with previously provided inputs or scientific evidence. Finally, the IMAAC needs the authority and access to more effectively inject its evidence into top officials' decision-making processes.

E. Analysis

The T3 FSE play in Connecticut provided an opportunity to learn about agent identification and hazard area definition during a major disaster. The exercise highlighted the potential for challenges when many organizations participate in the sampling process and when information about the agent is not systematically disseminated among the response organizations. The exercise also provided an opportunity to exercise the IMAAC MOA and observe its impact on the response. Although room for improvement exists, the use of the IMAAC appeared to reduce the amount of conflicting plume information received by decision makers in previous exercises.

Response agencies and organizations in Connecticut accurately identified mustard as the agent used by terrorists. The actions taken and decisions made with respect to the agent identification and confirmation process revealed areas of concern associated with:

- the coordination of emergency responders, law enforcement, and environmental responders at the incident site; and
- the flow of information about the contaminating agent.

The use of the IMAAC as the single source for plume models successfully reduced the number of conflicting products provided to decision makers and contributed to a common picture across the various response organizations and command centers. Although T3 showed significant improvement over T2 in this respect, there remains room for more improvement, particularly with:

- continued availability of additional plume products and analysis;
- managing contradictory requests for the IMAAC products; and
- coordination of emergency responders, law enforcement, and environmental responders on scene.

1. On-Scene Coordination of Emergency Responders, Law Enforcement, and Environmental Responders

Events at the Connecticut incident site highlighted the potential for confusion or tension when many organizations participate in the sampling process without clear understanding of each other's roles, authorities, and standard procedures.

First responders in Connecticut quickly recognized that there was a potential WMD component to the attack. They appropriately made note of the symptoms they were seeing, and recognized that victims complaining of garlic smells and exhibiting blisters were beyond the expected repercussions of a simple explosion. Based on these reports, WMD-specific responders arrived on the scene quickly, and testing of the agent progressed at a rapid pace.

Multiple State and Federal agencies dispatched HAZMAT units to the scene shortly after it was identified as a WMD event. Data show that the local FBI requested that agency's specialized units and the State Police ESU, and the Governor activated the National Guard CST. The HAZMAT units from the USCG, Connecticut DEP, and EPA arrived under their NCP authorities. Within two hours of the explosion, at least five specialized units were on site with the capability of testing for contamination and supporting agent identification efforts. Over the course of the four-day exercise, nine specialized units, with different primary responsibilities, supported efforts on scene associated with agent confirmation and hazard area definition. Table V-1 identifies the agencies and units that responded to the scene, the day they arrived, and an assessment of their focus based on T3 observations.

Table V-1. Agencies Supporting Sampling at the Incident Site in Connecticut

Responding Agency/Unit	Focus	Date of Arrival
New London Fire Department	Emergency response	April 4
CT DEP HAZMAT Team	Emergency response and remediation	April 4
National Guard CST	Emergency response	April 4
U.S. Navy Groton Submarine Base HAZMAT Team	Emergency response	April 4
FBI WMD Coordinator	Law enforcement/criminal investigation	April 4
CT State Police ESU	Law enforcement/criminal investigation	April 4
EPA Region 1 HAZMAT	Remediation	April 4
USCG Atlantic Strike Team	Remediation	April 4
FBI Boston HAZMAT Response Team (HMRT)	Law enforcement/criminal investigation	April 5
FBI HAZMAT Response Unit (HMRU)	Law enforcement/criminal investigation	April 5
EPA START	Remediation	April 6

The initial emergency response phase of the operation, during which responders focused on immediate situational assessment and victim recovery, lasted just seven hours—from the time the VBIED detonated to 20:00 on April 4, when the IC turned over control of the site to the FBI. The investigation phase lasted until early evening on April 5, or approximately 24 hours, when the FBI concluded its evidence collection efforts and turned the site over to the EPA and Connecticut DEP for sampling. Initial remediation efforts, predominantly sampling and monitoring to determine the extent of contamination at the site and in surrounding areas, began almost immediately and lasted through the end of the exercise. Long-term remediation and recovery efforts would have continued beyond the T3 FSE conclusion.

As Table V-1 indicates, most of the specialized units that responded to the scene arrived on the first day of the response effort. Although it was clear that efforts on April 4 were focused on emergency response and victim recovery, there were some instances of tension among sampling units concerned with public health concerns and those concerned with the criminal investigation. Some of this tension may have been a result of the artificiality of the exercise, but a lack of understanding appeared to exist across all the

units about standards and operating procedures followed by other responders and interest groups carrying out their own respective duties and responsibilities.

For example, law enforcement HAZMAT specialists, represented in Connecticut by the FBI and the State Police ESU, have two primary concerns during the initial emergency response phase. First, they seek to minimize damage to or contamination of evidence on scene. To this end, the FBI WMD Coordinator worked with the IC and first responders to identify the least damaging routes in and out of the site and oversaw collection of a small number of pristine evidence samples before emergency personnel entered the detonation area. Second, law enforcement personnel strive to maintain control of all potential evidence or data for future prosecution of the perpetrators. To this end, the FBI WMD Coordinator attempted to influence the type of field tests performed and the order in which they were conducted to minimize the possibility of contradictory results that could be used later by a defense counsel. Law enforcement personnel are also concerned with the chain of evidence and maintaining positive control of evidence at all times. In suspected terrorist incidents, all samples are evidence, even those being used by HAZMAT personnel, medical workers, and environmental units to assist with medical treatment, decisions about protective gear, or definition of the hazard area. To support this responsibility, the WMD Coordinator assigned CT State troopers to accompany all samples that went for testing. This practice became problematic when the National Guard CST collected samples for testing in its mobile field unit. Although the test the team performed on the sample is standard, the mobile unit itself is classified, and the State trooper did not have the clearance required to enter. This disrupted the evidence chain, from a control standpoint and in terms of having someone available to testify to the results later.

The T3 experience leads to questions regarding the presence of multiple assets with duplicative capabilities at the site, particularly those without specific responsibilities or authorities. Although the speed with which they all arrived in the T3 FSE is likely unrealistic, the fact remains that the presence of multiple units with similar capabilities can easily lead to duplication of effort, lack of understanding of different units' responsibilities or authorities, and counterproductive jurisdictional issues. The onsite presence and early activities of so many testing and sampling assets may be redundant in the first 12 hours of the response. However, some experts argue that having more assets available to support testing efforts gives the IC and senior law enforcement officials more flexibility in designing a test plan to support the needs of public health and the criminal investigation. In the exercise, that flexibility allowed the test plan to build in sophistication from paper testing indicating a blister agent to the use of advanced GCMSs that are virtually identical to the equipment used by accredited laboratories.

A second issue was associated with access to the incident site itself. The FBI took control of access to the site shortly after arriving early in the afternoon on April 4, though the IC still controlled operations. This allowed law enforcement to admit units or deny access to units. The National Guard CST, under orders from the Governor to report to the incident scene and support the IC, was denied access to the site and the Incident Command Post (ICP) for approximately two hours on April 4, when responders were still in the

emergency phase of the response. The data do not provide details on why the CST was initially denied access or why the decision was eventually reversed. Additionally, on April 5, there was poor coordination about when the remediation units would receive access to the site for field measurements, an issue of key interest to officials at all levels of the response. The initial sampling plan called for remediation units to begin testing on site the morning of April 5. However, that morning, the FBI informed the rest of the FSL agencies present that law enforcement's control of the site would continue for most of the day, and that sampling units would not he allowed to hegin their on-scene efforts until evidence collection had concluded. For most of the day, the remediation units were limited to sampling outside of the FBI's perimeter.

The discussion over access progressed all the way up to the JFO Coordination Group and the PFO for deliheration during a 14:30 meeting on April 5. At that level, the communities are largely divided into two groups: law enforcement and public health, with the latter also including environmental assessment and remediation. Although the law enforcement community recognizes the priority of emergency response over the investigation, the same is not true of remediation efforts, which are considered lower priority than the investigation. However, the sampling conducted by the USCG, EPA, and CT DEP was aimed at more than just long-term cleanup. The sampling results contributed to the IMAAC plume models and were essential for decisions about sheltering-in-place, school and business closings, and mass care needs. The delay in getting complete results did not seem to be well understood by decision makers at the State and Federal levels.

2. Flow of Information About the Contaminating Agent

Information that mustard was the chemical agent used in the attack did not filter up to decision makers and out to the public in an organized and controlled process. Instead, top officials began making decisions and statements to the public based on unconfirmed information and did not consider alternative hypotheses. For example, initial data from the Connecticut DPH showed that other agents, such as lewisite, could have been the source of victims' symptoms. If the early rumors about mustard had proved false, this could have had significant impact on response operations, including decontamination efforts, victim treatment, and public guidance. Immediate acceptance of presumptive confirmations of the agent in T3 may have been due, in part, to exercise artificiality. Exercise participants had advance knowledge of the agent being simulated, and as a result, may have been more inclined to accept unconfirmed hypotheses as fact. However, data still show the lack of a clear process for communicating and controlling such key pieces of information, and the potential for rumor to quickly become accepted as fact during a crisis.

In Connecticut, the first test-based confirmation that a mustard agent was released at the incident site occurred at 20:17; however, reports on the presence of mustard occurred well before that preliminary confirmation. As previously noted, first responders in Connecticut quickly recognized that there was a potential WMD component to the attack. Initial assessments of the situation were based on victim reports and symptoms.

Therefore, before conclusive testing, responders suspected a chemical blister agent like mustard. These suspicions quickly took on the appearance of fact as the information left the incident site. Table V-2 lists all the mustard agent reports prior to the 20:17 field test and an assessment of whether the report was based on information available at the time.

Table V-2. Reports of Mustard Agent Prior to the 20:17 Confirmation on April 4

Time of Report	Report of Mustard Agent	Based on Available Information?
14:20	FBI WMD Coordinator tells IC that symptoms suggested mustard.	Yes
14:50	IC tells 911 dispatcher and New London EOC that the contaminating agent was mustard.	No
14:55	VNN broadcasts an unconfirmed report of mustard found at the incident site.	Yes
15:05	Operations Chief in State EOC briefs that mustard is suspected but awaiting confirmation.	Yes
15:13	City Manager in New London EOC confirms that mustard was used in the incident.	No
15:33	IC allows the PIO on scene to release reports of mustard.	No
16:27	State Police reports to the State EOC that the presence of mustard has been confirmed.	No
16:58	IC informs the PIO that mustard has not been confirmed, but is suspected.	Yes
17:02	On VNN, Secretary of Homeland Security announces confirmation of the presence of mustard at the CT site.	No

The only public safety agency or operating center that appears to have hesitated to accept these unconfirmed reports was the CT DPH. At the DPH Emergency Control Center (ECC), the toxicologist and other health professionals on duty discussed the rapidity of the onset of symptoms. They determined that the symptoms appeared too quickly for the agent to be mustard if the truck explosion was the means of release. These officials initially suspected that the agent was lewisite. The public health community was concerned with an accurate confirmation of the agent, because mustard and lewisite have different treatment protocols and decontamination requirements. Therefore, if hospitals were treating patients for mustard exposure, their efforts would have been less than

optimal if the contaminant turned out to be lewisite. As a result, at 15:22, the CT DPH advised the State EOC not to release information about mustard until its presence had been confirmed. Even after the preliminary confirmations of mustard by the FBI were issued, the CT DPH continued to question the result until the State laboratory or the CDC verified it, which occurred early in the morning on April 5.

Complications in the flow of information about agent confirmation highlights another seam between the public health and criminal investigation communities, and their requirements as to what it takes for an agent to be "confirmed." For the law enforcement community, "confirmation" has legal ramifications, whereas for the rest of the responder community, confirmation drives public health and continuity of operations decisions. The FBI considers all instrumented monitoring tests conducted in the field to be preliminary. They use these results as guidelines for packaging evidence and practicing the appropriate safety precautions. Onsite testing is not definitive and cannot be used to support the prosecution of those responsible for the release. As a result, the FBI was reluctant to confirm the presence of mustard until it received results from ECA. Although the other organizations that collected samples immediately confirmed the presence of mustard, the FBI waited until 18:39 to report its suspicions to the JFO Coordination Group, Unified Command, and State EOC. As late as 23:15 on April 4, the FBI JOC told the State EOC that it was still not willing to announce confirmation of mustard to the press.

In general, the language used in reference to agent identification and confirmation is not specific enough to distinguish between the nuanced definitions of "confirmed" required by different responding communities and top officials. During T3, clear guidance was not available about the differences between confirmations that were presumptive, preliminary, or definitive. Nor did there appear to be widespread efforts to appropriately label confirmations as such. Instead, there appeared to be a lack of shared understanding at different levels of the response as to the definitive nature of the early reports from the site. The result was having preemptive, and at times incorrect or contradictory, reports flow up and down the response chain and to the public.

Ambiguous language is not the only explanation for the unclear status of agent identification and the release of information before it is confirmed. In the end, the problem comes down to having clear, explicit channels for information flow—channels that responders at all levels can rely on to send and receive valid information.

The T3 FSE highlighted legitimate gaps in the process of moving information from the incident site to the various command centers. Specifically, it was never clear:

- who was responsible for official confirmation of the contaminant, both to the public as well as to FSL agencies involved in the response;
- when that information should be pushed out; and
- how that information should be disseminated.

The NRP establishes a theoretical information flow from the ICP through the local and State EOCs, up to the Federal responders in the JFO, then on to the HSOC and IIMG. But the reality in Connecticut was much more complex considering the large number of FSL agencies represented at the incident site, the activation of an off-site Unified Command with predominantly Federal membership, and the very realistic demand for information from decision makers and the media. Information was being pushed and pulled from all directions. Although much of the preemptive agent confirmations and notifications in the exercise could be attributed to the artificiality of an exercise in which everyone knows the agent ahead of time, the fact remains that the situation is rife with the potential for miscommunication, rumors, and ambiguous statements from the scene. Information not clearly and systematically disseminated with the necessary level of detail and clarification may be misused or misunderstood.

3. Presence of Additional Plume Products and Analysis

T3 showed marked improvement over T2 in the use of plume products to support definition of the hazard area in Connecticut. The single-source IMAAC approach resolved much of the confusion about plume products noted during T2; however, the existence of additional plume products in T3 still caused some problems.

a. Version Control of IMAAC Products

During the exercise, decision makers faced some challenges concerning the number of IMAAC model runs completed and products distributed during the exercise—essentially a problem of version control. These products had differences ranging from slight revisions to different driving assumptions. Early model runs were not effectively taken out of play or retired, and it was often unclear which model run was the most current. As a result, there were instances in which command centers or participants not co-located were referring to different products. Problems with version control are a common result of distribution processes and the time lag between receipt and onward distribution of updates.

The IMAAC operations cell used two methods to disseminate its products:

- Products were posted on the NARAC website. Individuals located at the New London EOC, State EOC, JFO, and HSOC, as well as various agency headquarters and operating centers, could download the plume analysis from the NARAC site and display it on a choice of GIS maps.[69] NARAC account holders in the key operating centers were identified prior to the exercise, and the IMAAC had a process in place to quickly set up new accounts as needed. Account holders received an e-mail notification whenever a new model run was posted.

[69] The broad selection of GIS maps means it is possible for users to be looking at the same IMAAC results but in different perspectives and with varying levels of underlying detail. This may have caused some confusion at times in T3.

- An electronic slide presentation of the IMAAC model results with explanatory information was sent via e-mail to all the NARAC account holders and any other individuals who requested the products over the course of the response.

Users accessing the IMAAC data via NARAC required some level of training to download the analysis and generate products using the web-based GIS maps, but once trained, they could view the results on their preferred maps. Users relying on the electronic slides sent via e-mail received ready-to-view products with an identifying set number to distinguish them from previous products. These products could not be manipulated and arrived approximately 20 minutes later than the e-mail notifying NARAC system users of new product postings. This time delay could explain some of the instances when individuals referred to different products.

Additionally, not all command centers and officials have their own NARAC accounts. In Connecticut, the Geospatial Laboratory representative at the State EOC was tasked with downloading IMAAC products and posting them to the State web portal for multiagency use. Although this worked for the most part, it could have led to delays in some State and local agencies or operating centers receiving products. For example, the posting of the second set of plume products to the State intranet did not occur until 17:30, though the product was released by the IMAAC at 16:06. Moreover, it appears that some State agencies were either unaware of this service or unable to access the portal. Data indicate that on April 4, the State Police and CT DPH were without plume products at 20:00 and 20:23, respectively, although by that time the IMAAC had released three sets of products.

Another potential explanation for version control problems is the fact that due to available technology, products are widely distributed so quickly that records do not exist for everyone who may have received past products. Therefore, there is no way to ensure that all those individuals or agencies receive updates. The IMAAC does record all outgoing e-mails so that anyone who received previous versions will also receive new products. But, once the data pass that first link in the communications chain, there is no way to manage updates and version control across the board.

b. Non-IMAAC Products

The declaration of the CT bombing as an INS made the IMAAC the single Federal source for plume models. However, this did not stop other Federal agencies from modeling the effects. Per the MOA, other agencies may continue to model for their particular consumer, but must forward their products to the IMAAC and seek consensus. With one exception, this approach worked. At approximately 11:16 on April 5, the DTRA issued a document purporting to explain some discrepancies in the IMAAC product. The DTRA report caused some confusion among players because it contradicted the single source approach to modeling, but it did not appear to drive any decision changes.

The DTRA product that made its way around operating centers in Connecticut was not disseminated by the agency itself. Rather, it appears that DTRA issued the product to its consumer, DoD Northern Command (NORTHCOM), who then distributed it to the

DCOs and other military representatives in the various operating centers. From there, as with the IMAAC products, the document was pushed outside of its distribution chain. DTRA and other agencies modeling hazard areas can only control the list to which they send products. The MOA does not cover any further distribution that may overlap with IMAAC.

During the T2 FSE in Seattle, WA, the existence of multiple plume products resulted from independent modeling efforts by various agencies at FSL levels. During that exercise, local and State EOCs and local and State public health departments generated plume predictions. These varying products, coupled with the predictions generated by four Federal agencies, complicated decision making at all levels. The MOA establishing the IMAAC as the sole source for Federal plume products largely eliminated half of the problem experienced in Washington: that of conflicting Federal predictions. The complications generated by State and local products was never an issue in T3 because there are no data indicating that New London or the State of Connecticut had initiated or had attempted to initiate its own modeling capabilities. Rather, the State went immediately to the IMAAC for plume products.

4. Managing Contradictory Requests or Inputs to the IMAAC

Over the course of the four-day exercise, the IMAAC Operations Cell produced and released eight sets of plume products, as well as some revisions to specific inputs within the sets. The IMAAC produces new model runs when one of two things happens—either the cell receives a specific request for an updated product, or the cell receives new input or data that the modelers know will impact the plume picture. Table V-3 identifies when each set of products was released, the requesting or inputting agency, and the different assumptions used in developing the set.

Table V-3. IMAAC Model Runs Produced for Connecticut

Set #	Time of Release	Requesting Agency	Input Assumptions
1	14:36, April 4	DHS S&T (HSOC)	– 55-gallon drum of mustard exploded with 100-kg HE
2	16:06, April 4	CT DEP (State EOC)	– Confirmed location at New London City Pier – Refined explosion source and details
3	19:17, April 4	NOAA (HSOC)	– Aircraft release with west to east flight path
4	23:50, April 4	T3 SIMCELL[70]	– Calibrated with 13 field measurements – Aircraft release of 300 kg of mustard – Updated festival population data
5	08:00, April 5	CT DEP (State EOC)	– Combined 60-kg aircraft release and 10-gallon ground release
2P	09:35, April 5	DHS S&T (HSOC)	– Same as set 2, but with updated festival population data
6	14:30, April 5	CT DEP (State EOC) and IIMG	– Combined 274-kg airborne pure-vapor release and 18.8-kg evaporation release from truck
7	16:00, April 5	CT DEP (State EOC)	– Added 10 gallons to airborne release – Controller-confirmed location of explosion – Ground-based sprayer source – Calibrated with 87 field measurements
7A	23:00, April 5	IIMG	– Same as set 7, but with reduced amount and assumed duration of group evaporation release
8	16:00, April 6	DHS S&T (HSOC)	– Combined airborne (droplet and vapor) release and truck spill – Calibration with 158 field measurements

[70] The T3 SIMCELL injected data representing the results of field measurements taken by the joint sampling teams. At the time of the first inject, the sampling activities were still notional, and specific teams or leaders had not been identified. Later, field measurement injects were provided directly to the sampling teams, who passed the information through their respective reporting chains, EPA and CT DEP, and onto the IMAAC.

As can be seen from Table V-3, the agencies providing inputs and requesting models were about evenly split between Federal and State agencies. All the requests made by Federal agencies were actually made by agencies' watch officers in the HSOC on behalf of the IIMG. Connecticut made its requests through the CT DEP Geospatial representative in the State EOC. The State was more active in making requests than the IMAAC operators expected. By design, the IMAAC can accept inputs and requests from any of the Federal agencies designated as Authorized IMAAC Requestors (AIRs), any State or tribal organization, and any FSL emergency response organization. For the latter group, IMAAC must request authorization from the HSOC S&T Officer, but will conduct the analysis in parallel to the authorization effort. All of this flexibility means that IMAAC is able to respond rapidly to a situation even before the rest of the Federal response apparatus is fully activated.

However, the IMAAC's ability to coordinate with response organizations at all levels and locations means consolidation of inputs and requests is only happening at the IMAAC itself. The IMAAC CONOPS document prepared for T3 states:

> *When an Incident of National Significance is declared, the IMAAC will be the single point of distribution for Federal plume products. IMAAC will support the DHS-designated PFO (if appointed) and his Joint Field Office Coordination Group or the Federal Coordinating Officer (FCO) through distribution of products and technical expertise to State and local response.*[71]

This seems to suggest that the IMAAC would work through the JFO Coordination Group to provide analytical services to the State. However, the CONOPS also states:

> *The IMAAC will work directly with Federal, State, and local agencies technical assets and regional or national incident response teams to provide the most accurate, reliable, and timely estimates of plume hazard predictions and impacts possible. The IMAAC will continue to refine products based on newly obtained data, improved input information, and the use of additional simulation tools.*

The latter statement suggests that during the T3 FSE, local and State agencies were not required to work through Federal representatives to provide inputs or request model runs. In fact, the CT DEP Geospatial representative in the State EOC had a direct line to the IMAAC and requested half of the analyses produced. This approach is consistent with the role of the Federal government in support of a State response and is part of what makes the IMAAC so flexible and responsive. The concern is what the IMAAC should do if it receives inputs and requests from one level or agency of government that vary from those

[71] Memorandum dated March 30, 2005, *Department of Homeland Security Interagency Modeling and Atmospheric Analysis Center (IMAAC) Concept of Operations for the 2005 TOPOFF3 Exercise*, from Bruce A. Davis (Interim IMAAC Director, DHS S&T, EPR) and Ron Baskett (Interim IMAAC Operations Manager, LLNL, National Atmospheric Release Advisory Center).

received from other parts of the government, or if it receives requests that will not produce a valid output based on scientific evidence.

For example, in the initial requests for a plume product, the IMAAC Operations Cell received inputs from three different sources regarding the location of the explosion—the State Pier, the City Pier, and Fort Trumbull. The third location was an artificiality of the exercise, but the confusion over the pier site is realistic. The IMAAC Director had to delay release of that initial plot while he sought clarification from his sources on this critical element of information.

In another example, the IMAAC determined from the initial set of field measurements, injected at 19:30 on April 4, that the bulk of the agent had to have been released from an airplane; this scientific conclusion supported the FBI's investigation of the crop duster in Maine and was released in set 4 of the IMAAC products. However, the next day, the IMAAC Operations Cell continued to get requests for products that did not incorporate an airplane dispersal: the CT DEP requested an updated model run based on a ground release, and the DHS S&T representative to the IIMG instructed the IMAAC to produce model runs that did not include the airplane dispersal. In the Connecticut JFO, decision makers sought plume products that assumed either an air release or a ground release, but not both. They wanted to compare the hazard areas of each because of the apparent uncertainty over the dispersal mechanism. In Connecticut and Washington, D.C., players reported being unclear on the role of the suspect plane in the chemical release. A clear statement from the IMAAC on the scientific verification of an aerial release may have helped alleviate such confusion.[72]

Variation in inputs and requests may be a function of a lack of a common operating picture across the response organizations, or may be due to a real need for a different picture or focus. The concern for future applications of the IMAAC is the lack of detailed procedures regarding how to handle discrepancies, whom should be responsible for resolution and deconfliction, what authority or responsibility the IMAAC has to discuss the rationale for requests with a requesting agency, and how the IMAAC can more effectively inject scientific evidence into top officials' discussions and decision making.

5. Issues from Previous Exercises

The most significant issue relative to agent confirmation and hazard area definition that came up in previous exercises was the presence of multiple, competing plume products. During the T2 FSE, the conflicting information provided in the many different plume predictions caused problems from the incident site all the way to the Secretary of Homeland Security. That experience led to the creation of the IMAAC and the MOA directing that the IMAAC serve as the single source for plume products. The result in T3 was a more consistent picture of the hazard area shared across different operating centers, and a common plume picture shared by responders on the ground up to the HSC in the

[72] Confusion among participating agencies and operating centers regarding the role of the airplane in the mustard attack is discussed in greater detail in the Information Sharing chapter of the AAR.

White House. However, it should be noted that competing plume products in T2 were generated by FSL agencies. Although the IMAAC agreement appeared to reduce Federal products in T3 to those generated by a single source, the T3 FSE did not test potential complications from State or local agencies producing their own predictions.

A second issue identified in T2 was minimal coordination of data collection efforts among agencies at the incident site. The result of the onsite coordination failures in T2 was that no one agency at the site had all the sampling data and that many collection efforts were repeated. Onsite coordination of sampling in T3 seemed to go much better than in the preceding exercise, with the IC and FBI WMD Coordinator directing the initial sampling efforts, and the EPA, USCG, and CT DEP developing and implementing the follow-on sampling plan. The result was minimal redundancy in actual testing activities, except when required by exercise design. This improvement in coordinating sample collection efforts did not eliminate the broader T2 finding: no one agency had a complete operational picture. The same result occurred in T3, as evidenced by the contradictory requests issued to the IMAAC and the breakdowns in the flow of information about the contaminating agent. Similarly, although the onsite sampling activities in T3 appeared more coordinated, tension resulting from competing demands for access and duplicative capabilities suggests that coordination can be further improved.

Finally, events in the T2 FSE illustrated problems with the distribution of analysis products to decision makers. Although there were some complaints during T3 about delays in receipt of products, they were not significant. For the most part, all of the operating centers and top officials had immediate access (via technical representatives and/or e-mail) to IMAAC products. Time delays could largely be explained by the chosen mode of receipt (i.e., download vs. e-mail) and how far removed an individual was from the initial distribution list.

Table V-4 summarizes the improvements observed between T2 and T3 in the areas of agent confirmation and hazard area definition. Note that the T2 issues were those identified in that exercise's AAR and may not be all inclusive.

Table V-4. Comparison of T3 FSE with Previous Exercises

T2 FSE	SOE 05-3	T3 FSE
ISSUES/OBSERVATIONS		
• Different agencies and jurisdictions used one or more plume models to generate predictions, which led to confusion and frustration among top officials in Washington State and Washington, D.C. • FSL agencies used different and incomplete data to develop plume products and deposition maps. • Decision makers did not understand the differences between predictive plume products, empirical data products, and deposition maps. • Decision makers were not well informed of the limited usefulness and lifetime of the plume predictions or the need to run updates using empirical data.	N/A	• IMAAC successfully provided a common picture of the plume for use by FSL officials. • IMAAC received inputs and requests that varied and/or contradicted with those received from other agencies or jurisdictions. • IMAAC received inputs and requests that would not produce a valid output based on scientific evidence. • FSL agencies/operating centers did not recognize the IMAAC products as a source for information beyond predictive plume products. • IMAAC did not appear to have adequate procedures in place to deal with discrepancies in inputs or contradictions in modeling requests.
• Agencies at the incident site and at off-site locations did not coordinate collection and analysis of radiological data.	• Officials agreed that rescue operations are always the top priority and predicted that there would be no conflict between law enforcement, decontamination, and public health/medical response efforts.	• Specialized incident site response units did not exhibit a clear understanding of each other's roles, authorities, and standard operating procedures. • The lack of a formally defined information flow process from the incident site resulted in premature public messages and decision making about the identity of the chemical agent.
	• Some officials expressed concern about lab shortages for a widespread chemical release. • Officials emphasized the importance of summarizing technical information in layman's terms to support decision makers.	

F. Recommendations

- Clarify and disseminate the various response organizations' roles and responsibilities at the incident site, to include the timing of those responsibilities and their contribution to the larger response operation.
- Clarify the formal information flow procedures from the incident site to the rest of the response organization and assert the authoritativeness of formal processes over informal information movement.
- Clarify the IMAAC processes for receipt and review of other modeling products and establish a protocol for other modeling agencies to distribute to their consumers on the purpose of their product and the guidelines for redistribution.
- Develop procedures on how the IMAAC should handle discrepancies in data inputs or product requests and identify a process to aid the IMAAC in deconflicting inputs.
- Clarify the responsibilities, authorities, and mechanisms for the IMAAC to formally disseminate critical information learned through its scientific analysis of the incident.

VI. Emergency Response Operations nnder a Unified Command—Task # IV-2: Establish IC Unified Command

A. Summary of Issue

The issue is that the Unified Command's scope of responsibilities was not clearly understood. Doctrinal details were insufficient regarding concurrent implementation of the NRP and NCP and regarding the resulting duplication of roles, competition for resources, and coordination of information.

The National Incident Management System (NIMS) directs the Incident Command System (ICS) as the Federally recommended organization for managing emergency responses. It allows an integrated organizational structure that can scale up or down to effectively meet the demands of an incident regardless of the complexity of the situation. Traditionally, the most senior person present from the primary agency overseeing the local response acts as IC and handles the command and coordination function. When multiple organizations or jurisdictions have responsibility over aspects of the tactical response, a Unified Command may be formed to link organizations or municipalities together, provide a forum for integrated decision making, and enable a coordinated approach to incident response.

The T3 FSE provided an opportunity to exercise the integrated ICS approach in Connecticut with the formation of a Unified Command. The exercise revealed:

- poor integration between the off-site Unified Command Post (UCP) and activities at the incident scene;
- challenges for integrating the Unified Command with other emergency response organizations and operating centers;
- concern over lack of alignment between the NCP and NRP, which plays out most significantly at the Unified Command; and
- limited understanding of the scope of Unified Command responsibilities.

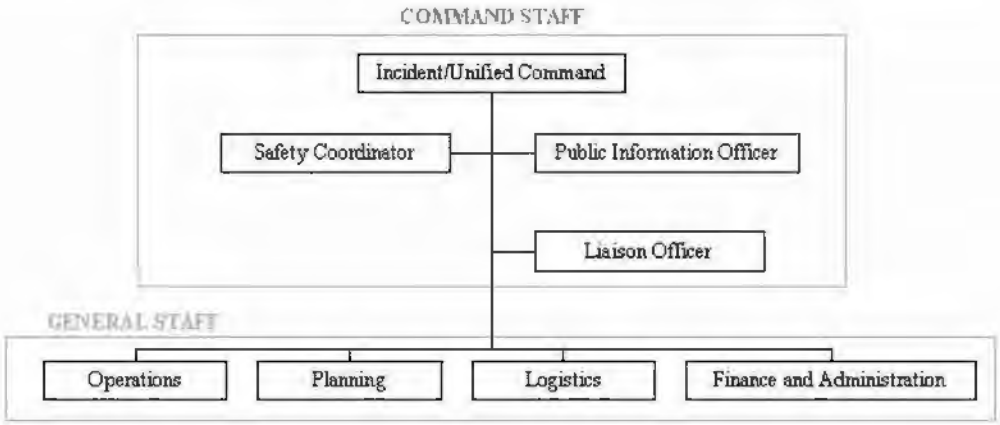
The analysis indicates that implementation of the Unified Command concept would be improved by further defining the roles and responsibilities of the Unified Command, developing standard operating procedures, and detailing these in the NRP and other supporting doctrine, such as NIMS. Additionally, the external information flow processes used by the Unified Command need to be reconsidered to ensure State and local coordination, particularly when the Unified Command's focus shifts to Federal-to-Federal support and NCP responsibilities.

B. Background

NIMS codified the concept of the ICS and the establishment of a single IC or a Unified Command to oversee response operations. Per the NIMS, a single IC is used when an incident occurs within a jurisdiction with no jurisdictional or functional agency overlap. The IC has overall incident management responsibility. A Unified Command is

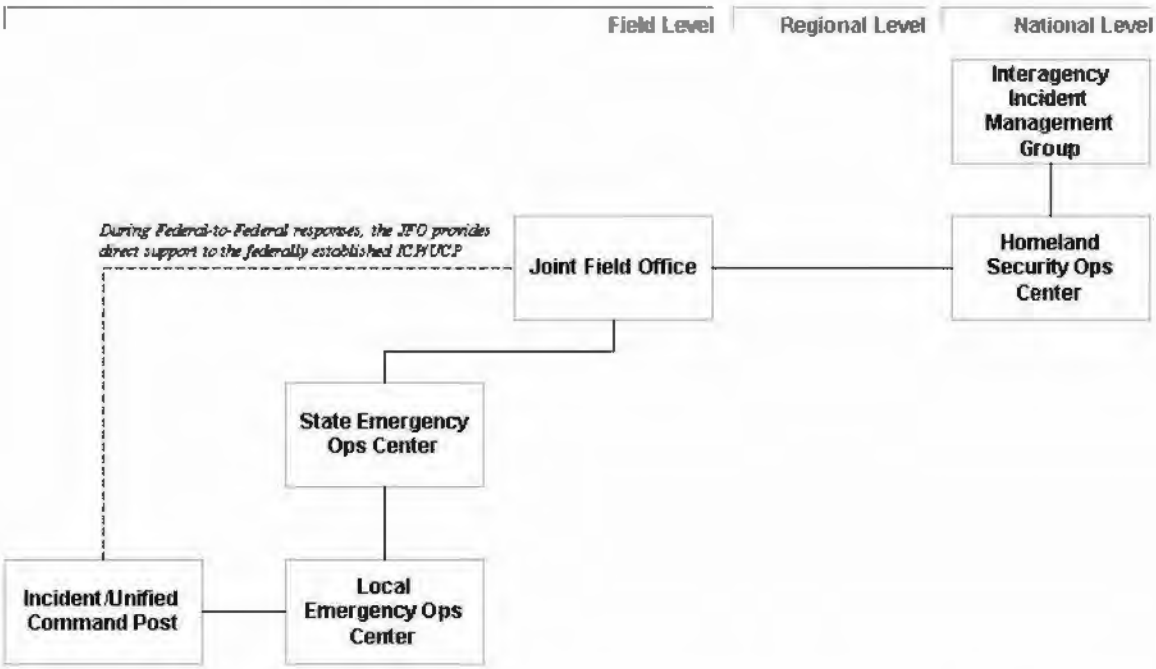
implemented when a response involves multiple jurisdictions or agencies, each with its own functional responsibilities for an aspect of the response. The Unified Command uses a collaborative approach to make decisions and establish priorities. In both constructs, the Command develops incident objectives, approves Incident Action Plans (IAPs), and approves resource requests. Figure VI-1 shows the notional organizational chart for an IC or Unified Command per the ICS.

Figure VI-1. Notional Response Organization under the ICS



Per the NRP, the IC or Unified Command coordinates its needs through the local EOC as depicted in Figure VI-2. The exception to this model is a Federal-to-Federal response situation, in which the JFO provides direct support to the Federally established ICP/UCP. In that case, the NRP permits direct coordination of information between the ICP/UCP and the JFO, as indicated by the dashed line in Figure VI-2.

Figure VI-2. Notional Coordination Flow from ICP/UCP



An IC's focus is direct control of tactical operations. As the multijurisdictional or multiagency replacement for the IC, the Unified Command's purview is also tactical operations on scene and the response efforts related to management of the incident site. Traditionally, the local EOC handles all other local concerns that fall outside the response objectives established by the IC/Unified Command.

The Unified Command concept is introduced in the NIMS as an alternative or transitional option from a single IC. It is not given much consideration in the NRP, which only defines it as an option.

The Unified Command is discussed in greater detail in the NCP, which establishes the coordinated FSL response to the accidental or intentional release of hazardous substances, oil, pollutants, and contaminants into the environment. A Unified Command is the designated response structure per the NCP. The dominant agencies in the NCP-driven response are the USCG and EPA at the Federal level, environmental agencies and health departments at the State level, and emergency responders on scene.[73] The NCP proposes the Unified Command as the:

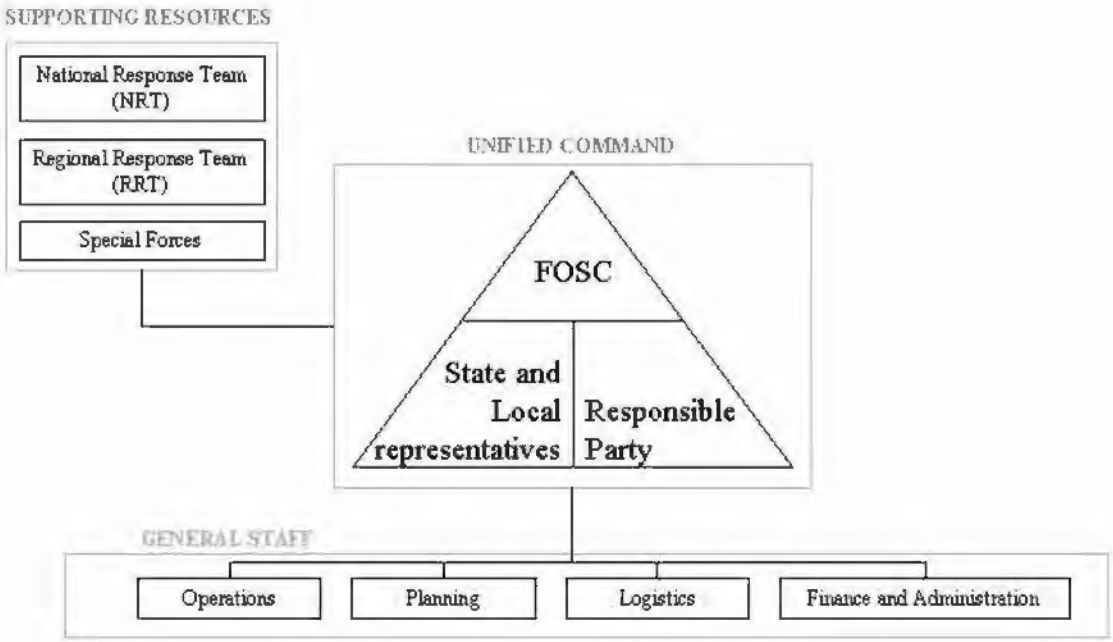
> *Basic framework for the response management structure…that brings together the functions of the Federal government, the State government, and the responsible party to achieve an effective and*

[73] In situations in which the release involves private corporations or facilities, the responsible parties will also be part of the response.

> *efficient response, where the [On-Scene Coordinator] OSC maintains authority.*[74]

In a response managed under NCP authority, the Federal On-Scene Commander (FOSC) holds primary responsibility for directing response activities and coordinating efforts related to the detection and mitigation of the release. Except in limited situations, the FOSC is a regionally based official predesignated by the EPA or USCG. The State is usually represented in the Unified Command by its environmental agency. The notional organizational structure of the Unified Command in an NCP response is shown in Figure VI-3.

Figure VI-3. Notional Unified Command in an NCP Response



The supporting resources depicted in Figure VI-3 include two permanent elements, the National Response Team (NRT) and Regional Response Team (RRT). These two elements are responsible for planning and preparedness activities, and for providing advice and support in the event of an incident. NRT membership consists of representatives from USCG, EPA, FEMA, DoD, Department of Justice (DOJ), Department of Energy (DOE), U.S. Department of Agriculture (USDA), Department of Commerce (DOC), HHS, Department of Interior (DOI), Department of Labor (DOL), Department of Transportation (DOT), Department of State (DOS), the Nuclear Regulatory Commission (NRC), and General Services Administration (GSA). RRT membership consists of designated representatives from each of the Federal agencies

[74] U.S. EPA, National Oil and Hazardous Substances Pollution Contingency Plan, §300.105(e).

participating in the NRT, as well as State officials. If agreed on by the States, local government representatives may also participate. Regional representatives from the EPA and USCG co-chair the RRT, except during activation, when the chair is a representative from the agency providing the FOSC.[75]

The RRT is the regional coordination element for NCP planning and implementation. During a response, the RRT advises and supports the FOSC by monitoring the situation, providing subject-matter expertise and recommending specific actions. The NCP calls for the FOSC to consult regularly with the RRT as appropriate. Incident-specific RRTs may be activated upon request from the FOSC, from any RRT member, or by the RRT chair. Such activation is likely if the incident exceeds the response capability of the FOSC, if it transcends State boundaries, if it poses a substantial threat to public health or the environment, or if it is a worst-case discharge as described by law.

The authorities and responsibilities referenced in the NCP are required by section 105 of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (CERCLA), 42 U.S.C. 9605, as amended by the Superfund Amendments and Reauthorization Act of 1986 (SARA), Public Law 99-499 and by section 311(d) of the Clean Water Act (CWA), 33 U.S.C. 1321(d), as amended by the Oil Pollution Act of 1990 (OPA), Public Law 101-380. Response actions undertaken via CERCLA and the NCP do not require declaration of an INS or a Stafford Act declaration, but rather have their own notification mechanism and funding stream. As a result, the FOSC has independent authority under the NCP to respond to HAZMAT incidents and initiate response activities. The FOSC has the authority to go directly to the Federal agencies identified in the CERCLA to request assistance and resources in their respective areas of expertise. To obtain support not otherwise available under the NCP, the FOSC may request Federal assistance from DHS via the Federal-to-Federal support mechanism available under the NRP.

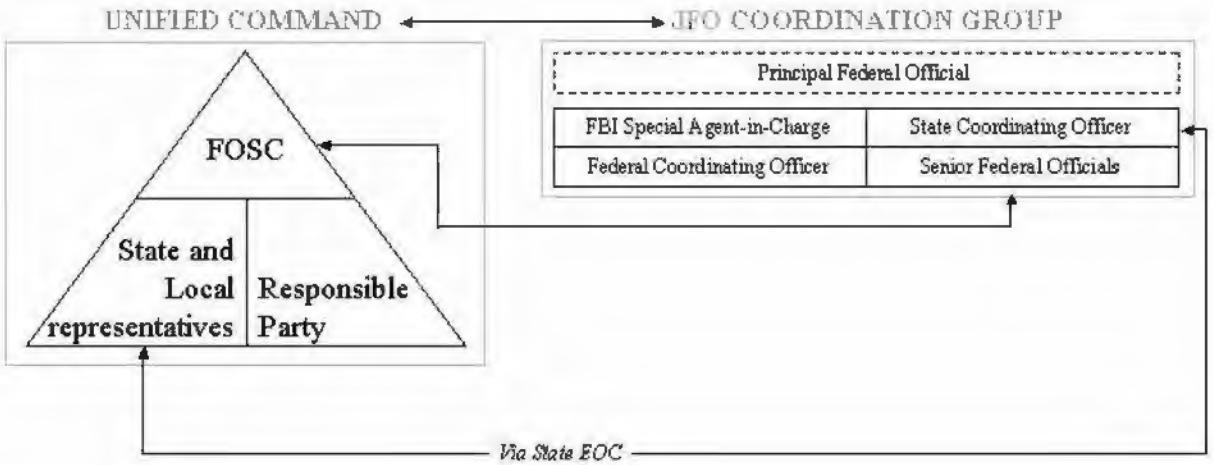
The NRP and NCP acknowledge the potential for concurrent implementation. In the event that an NRP response is underway, the plans call for the FOSC to carry out his/her responsibilities under the NCP while coordinating with the FCO to ensure consistency with other Federal disaster assistance activities. The NRP contains two annexes that address concurrent implementation of the two plans:

- ESF #10—Oil and Hazardous Materials Response Annex, which applies when ESF #10 is activated; and
- Oil and Hazardous Materials Incident Annex, which applies when ESF #10 is not activated.

[75] The FOSC is the Federal official pre-designated by the EPA or the USCG to coordinate and direct the NCP response, with EPA taking the lead for inland incidents (or those affecting inland and coastal areas) and USCG taking the lead for incidents occurring on or near the coast. In limited situations, another Federal agency may be identified as the lead and will designate its own FOSC.

Most INSs involving the release of oil or hazardous materials will include Stafford Act declarations and the resulting activation of ESF #10. In those situations, the FOSC coordinates NCP response activities with the Federal actions via ESF #10 and the ESF #10 Senior Federal Official (SFO) in the JFO Coordination Group. If the INS does not include a Stafford Act declaration, the agency leading the NCP response provides an SFO at the JFO through whom activities will be coordinated. Either way, the FOSC typically communicates with the SFO, who coordinates with the PFO and/or FCO. In both cases, the NCP-style Unified Command communicates with the JFO Coordination Group. The lines of connectivity between the Unified Command and JFO Coordination Group are illustrated in Figure VI-4. The graphic does not illustrate the coordination effort between the Unified Command's General Staff and ESF #10.

Figure VI-4. Connectivity Between UC and JFO Coordination Group During Concurrent NRP and NCP Implementation



C. Reconstruction

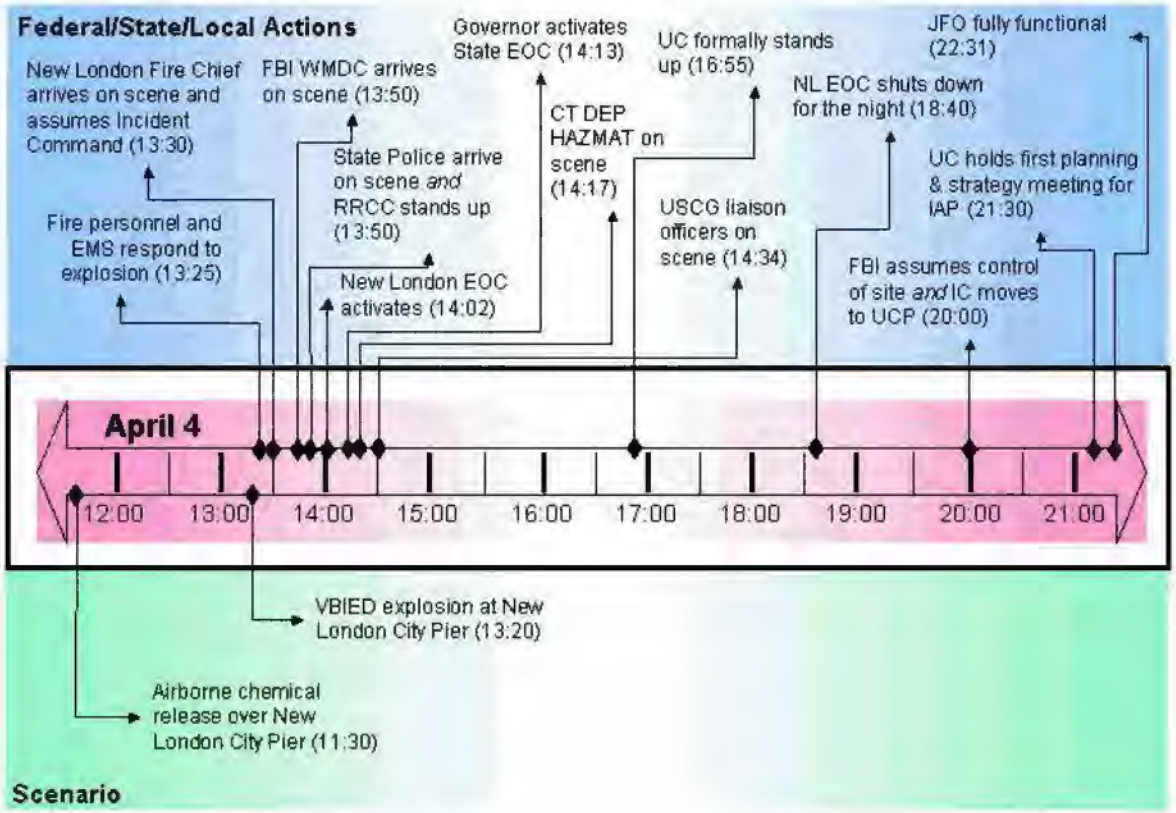
At 13:20 on Monday, April 4, a truck exploded at the City Pier in New London, CT. Local emergency personnel responded to the incident site shortly after the explosion. At 13:30, the New London Fire Chief arrived on scene and established an IC to direct a coordinated response of fire, police, and EMS personnel. As other agency representatives arrived on scene over the next two hours, they checked in with the IC to determine how best to provide support. At 14:20, the IC initiated activation of an off-site command post to be staffed according to ICS guidelines, with operations, planning, logistics, and finance and administration branches. Command and control formally shifted to a Unified Command at 16:55, and plans were made to move to the off-site UCP to be located at the National Guard Armory a few miles away from the incident site. At 19:45, the IC announced his demobilization strategy for local assets on site, determining that once all patients were treated, the initial responders would depart, the FBI would take control of the scene, and the Unified Command would transition to the off-site UCP. The last live victims were removed from the incident site at 20:00, after which EMS and local fire

personnel demobilized, and the FBI began setting up its crime scene. The Unified Command fully activated at the armory at 21:30 with a planning and objectives meeting of the principals.

Concurrent to the response and ramp-up on site, other emergency response organizations at the FSL levels were activated. The New London EOC stood up at 14:02 and established communications with police officers at the incident site and with the Area IV Coordinator for the State. The Governor activated the State EOC shortly thereafter at 14:13. The FEMA Region 1 RRCC stood up at 13:50, while the JFO assumed control of Federal response coordination at 22:31.

Figure VI-5 illustrates the key events in the ramp-up to a Unified Command.

Figure VI-5. Transition from an IC to a Unified Command



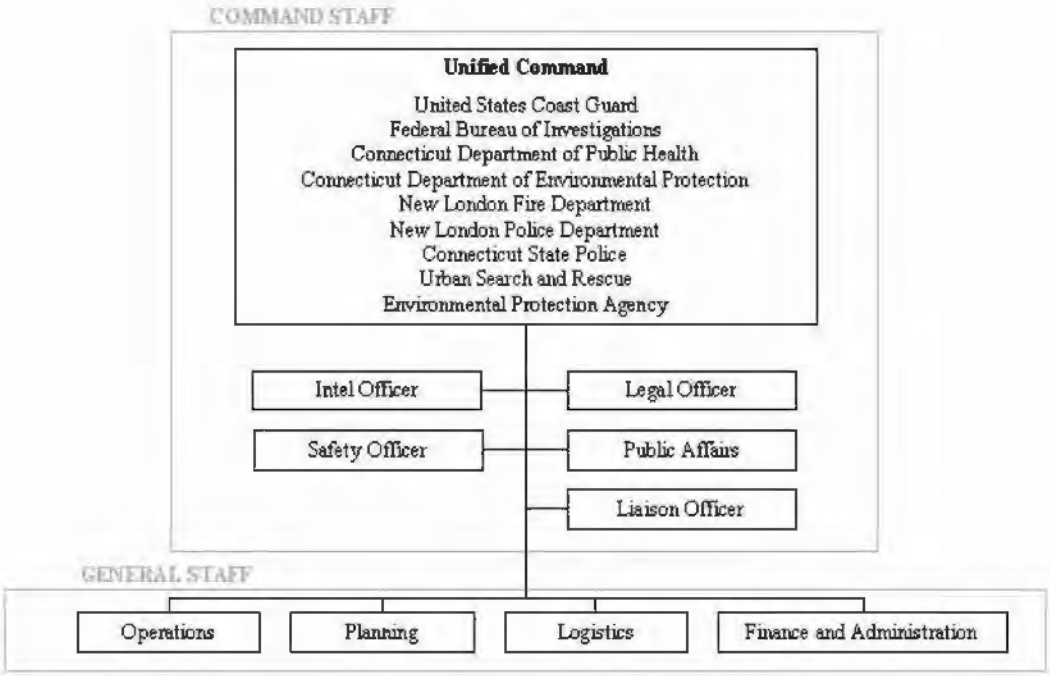
The agencies represented in the Unified Command on April 4 were:

- New London Fire Department
- New London Police Department
- CT State Police
- CT DEP
- CT DPH
- DHS/USCG
- FBI

On April 5, Urban Search and Rescue (USAR) joined the Unified Command to coordinate its recovery operations at the incident scene. EPA joined to facilitate the assumption of responsibility for remediation of the chemical release.

The Unified Command general staff was comprised of representatives from the USCG, EPA, CT DPH, U.S. Public Health, and NDMS among others. Figure VI-6 shows the organizational chart for the UCP during the T3 FSE.

Figure VI-6. CT Unified Command Organizational Chart as of April 5



Once activated, the Unified Command's focus turned to setting objectives for the response effort and planning activities for the upcoming operational period. Following the 21:30 strategy meeting, members drafted an IAP to start at 08:00 on April 5 that included an air monitoring and sampling plan to begin testing for the extent of the contamination. The IAP was approved at 06:30 on April 5, during the morning meeting

of the Unified Command. At that time, the FBI notified planners of the need to rework the sampling plan to account for site closure for evidence collection. At 14:30 that afternoon, HAZMAT units from EPA, USCG, and CT DEP notionally began executing their sampling plan in the neighborhoods around the incident site. Actual sampling efforts continued onsite until 14:36 on April 6, when the hazard area was fully understood and test results indicated greatly reduced concentrations of mustard.

D. Consequence

The Unified Command concept adds flexibility to an incident response by providing the construct for integrated decision making and coordinated operations. The response in Seattle, WA, during the T2 FSE resulted in the establishment of an onsite Unified Command; however, no detailed analysis of that organization was completed to allow comparisons with T3. Experiences in the T3 FSE suggest additional clarification of roles, responsibilities, and processes is required to make the Unified Command a more effective participant in response efforts.

The following areas were problematic for the Unified Command during the T3 FSE:

- maintaining oversight and awareness of activities at the incident site;
- integrating with the other emergency response operating centers;
- aligning response efforts pursued under the authorities of the NCP with the NRP activities and structures; and
- understanding the scope of its responsibilities.

Maintaining oversight and awareness of activities at the incident site was an issue for the Unified Command for three key reasons. First, there was no formal process in place to share information between the incident scene and the UCP. Instead, the Unified Command relied on direct reporting from senior representatives of the agencies still on the scene. Second, agency presence and participation in the off-site UCP was inconsistent, particularly among agencies still operating at the incident site. Third, there appeared to be a lack of buy-in or understanding among all responding agencies as to the purpose and operating mechanisms of the Unified Command. These explanations indicate the need for full-time agency representation in the UCP and/or specific processes for moving information from the site to the command post and vice versa. More discussion and documentation of the Unified Command concept at the Federal level may help promote support for and understanding of the ad hoc field organization.

Poor coordination between the Unified Command and the local EOC resulted in the virtual exclusion of the latter from the response effort and the use of alternate information flow processes for coordination with the State. This may have been partially due to an exercise artificiality, but there are also indications that the Unified Command's focus of effort may have contributed to the problem. During the T3 FSE, the Unified Command primarily used Federal-to-Federal coordination and its NCP authorities to meet its needs. The processes for those approaches do not require any action from or coordination with local authorities. The NRP needs to reconsider the information flow processes that are set

up when a Unified Command implements the NCP and Federal-to-Federal support. As the alternative to the local IC, the Unified Command must also communicate with the local authorities and keep them apprised of the situation at the scene, even if their resources are no longer required. In particular, when an incident progresses beyond the capabilities of the local municipality and the State, and when the UCP is comprised of predominantly Federal agencies, there may be a tendency to bypass the local and State authorities; the Unified Command and State government need to make concerted efforts to keep local authorities involved in the response process.

Although the T3 FSE did not appear to have any significant problems attributed solely to the concurrent implementation of the NCP and NRP, participants and observers expressed concern that current doctrine does not sufficiently address the potential for duplication of roles, competition for resources, coordination of information, and transition from an NCP-only response to a joint NCP-NRP effort. The NRP annexes associated with concurrent implementation of the two plans require clarification and additional detail in the areas stated above. Furthermore, experiences in the T3 FSE suggest that the relationship between the RRT and ESF #10 is unclear. Further clarification as to the role of the RRT and its relationship to ESF #10 is needed.

Finally, efforts pursued by personnel at the UCP, objectives established by the Unified Command, observations made by data collectors and subject-matter experts, and comments by participants themselves indicate that the role of Unified Command is not clearly understood or sufficiently defined. Operators require a better understanding of the Unified Command's scope of responsibilities and role in the response operation relative to the local and State EOCs and the JFO.

E. Analysis

The focus of the analysis section is the role of the Unified Command as it relates to:

- the lack of integration between UCP and activities at the incident scene;
- poor coordination with State and local operations centers;
- concern about lack of alignment between NCP and NRP; and
- poor understanding of the scope of Unified Command responsibilities.

1. Lack of Integration Between UCP and Activities at the Incident Site

Evidence suggests there was minimal coordination between the UCP and activities at the incident scene. Agency representatives to the Unified Command were not always present or available at the UCP, and communications between the UCP and the incident site were insufficient once the local IC left the scene and turned the site over to the law enforcement investigation. This led to ineffective and wasted planning efforts at the UCP and tension among some Unified Command agencies.

For example, overnight on April 4, the DHS/USCG, EPA, and CT DEP drafted a site sampling and monitoring plan as part of the Unified Command's first IAP. That plan

assumed the HAZMAT specialists would have access to the site the next morning. However, there was no FBI presence in the UCP overnight, and the agency representatives charged with drafting the plan were concerned about scheduling remediation activities without FBI input. They attempted to reach the FBI Unified Command representative at the JOC overnight, but without success. When the FBI's representative to the Unified Command reviewed the plan on April 5, he informed the rest of the FSL agencies present that FBI control of the site would continue for most of the day, and sampling units would not be allowed to begin their on-scene efforts until evidence collection had concluded. Discussions about access to the site went to the JFO Coordination Group and PFO for resolution.[76]

Analysis suggests three possible explanations for the poor coordination between the UCP and activities at the incident site. First, there did not appear to be a coordinated process in place to share information between the incident scene and the UCP. When the UCP formally activated at 21:30 on April 4, the only agencies at the incident site were FBI, State and local police, and USAR. The FBI and USAR representatives to the Unified Command returned to the UCP a few times each day to give updates and check in with the other agencies, but they were not present for most planning meetings or to support IAP development. As part of pre-exercise planning, the Unified Command developed an information flow plan for moving information from the UCP to other agencies, but it does not appear that such thought was given to the incident site. Rather, UCP members seemed to assume that those agencies with personnel still at the scene would provide sufficient representation in the UCP to facilitate coordination.

The second potential explanation for poor coordination between the UCP and site activities is that agency presence and participation in the UCP varied throughout the exercise. The local fire and police representatives stood down at 15:00 on April 5, when all emergency operations at the incident scene had concluded, and the departments had no assets still participating in the response. The State Police and FBI did not have personnel in place to staff the off-site UCP 24 hours each day. Instead, the FBI Supervisory Special Agent (SSA) for the incident site was dual-hatted as the FBI representative to the Unified Command. His responsibilities of managing the FBI efforts at the scene would not permit him to commit to a full-time presence at the off-site UCP. This was especially problematic, considering the FBI was the lead response agency once the local IC demobilized his assets and the response shifted from emergency efforts to evidence collection. Senior representatives from CT DEP, CT DPH, EPA, and DHS/USCG appeared to be present in the UCP throughout the duration of the response, and as a result, they drove the UCP efforts toward their focus areas. The UC anticipated the presence of other agencies on a full-time basis which did not occur.

Finally, the coordination problems may have been the result of a lack of buy-in by all agencies to the Unified Command concept in general and the establishment of an off-site UCP in particular. There was disagreement about the need for an off-site UCP and the

[76] Other implications of this issue are discussed in the chapter on Agent Confirmation and Hazard Area Definition.

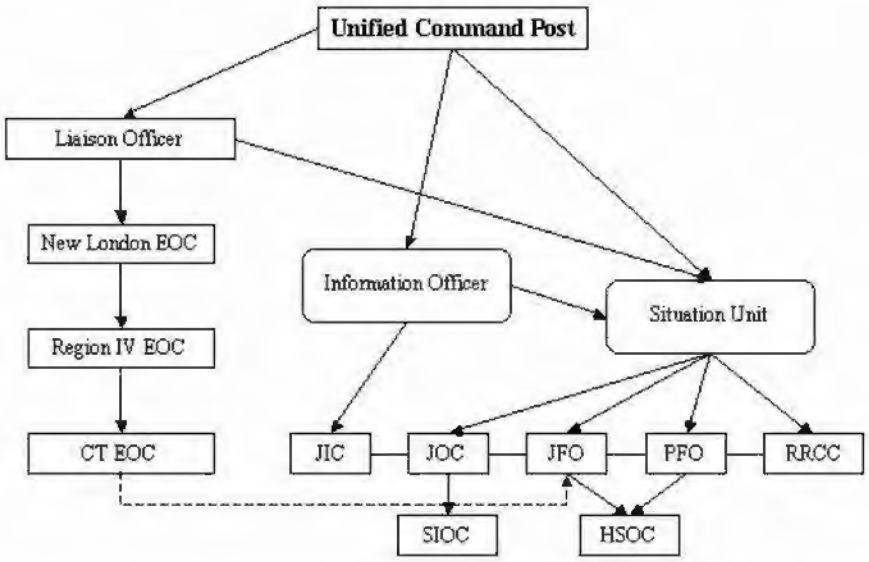
potential overlaps between its activities and those of other operating centers in the response. For example, the FBI SSA appeared to be surprised to learn of the existence of the UCP at the armory, expressing to a data collector his impression that "The UCP was at the JOC." This reveals a lack of understanding about the scope of the Unified Command and about the difference between the JFO/JOC and the Incident Command Post, which is further discussed in a later section of this chapter. The Incident Management Assist Team (IMAT) composed only of Coast Guard members, was the driving force behind the organization of the UCP and UC staff. Several other agencies were invited to participate in the UC staff, but did not send representatives.

2. Poor Coordination with Local and State EOCs

Information about plans, activities, and resource needs did not filter up from the Unified Command through the local and State EOCs, as designed by the NRP. Instead, once the Unified Command stood-up, the New London EOC was largely excluded from the response effort. Interactions and communication between the State EOC and the Unified Command appeared to be primarily through agency representatives present in both locations or through the JFO.

In accordance with the NRP, the ICP/UCP coordinate, through the local EOC, official state/local requests for Federal assistance as depicted in Figure VI-2. Prior to the start of the T3 FSE, the FOSC oversaw development of an information flow plan for the Unified Command that expanded on the NRP's structure for both Federal-to-State and Federal-to-Federal responses. That plan called for a liaison officer in the UCP to serve as the primary point of contact with the New London EOC. The plan is illustrated in Figure VI-7.

Figure VI-7. T3 Information Flow Plan, Designed by the Unified Command



Although the initial plan provided a means of communication from the UCP to the New London and State EOCs, the reality was that the New London EOC was largely shut out of the Unified Command's response efforts, and information flow to the State instead went through State agencies represented in the UCP (e.g., CT DPH and CT DEP). This may be partially because the local EOC closed at 18:40 on April 4, almost three hours before the UCP fully activated. Therefore, the UCP was forced to bypass the locals from the beginning and to find alternative ways of moving information to the State. By the time the New London EOC reopened on the morning of April 5, the alternative information flow processes were already in place.

A second potential explanation for the lack of communication and coordination between the UCP and the local and State EOCs may lie in the Unified Command's focus of effort. When the IC turned over control of the site to the FBI, field activities shifted to evidence collection, and efforts at the UCP itself shifted to remediation planning. The FBI and State Police coordinated their evidence collection onsite, and the remediation efforts fell under both the Federal-to-Federal response category in the NRP and the EPA/USCG authorities of the NCP. As was illustrated by the dashed line in Figure VI-2, in a Federal-to-Federal response, the NRP calls for the UCP to coordinate directly with the JFO. The NRP also requires direct coordination between the FOSC and ESF #10 in the JFO. Per the NCP, coordination of remediation activities with the State is meant to occur at the agency level, usually by the State environmental agency. It is not unusual, therefore, for that agency to serve as the conduit of information to the State's leadership in an NCP response. All three of these doctrinally established communication and coordination processes do not include direct links with the local EOC. This may have resulted in communication difficulties during the exercise. The result for the T3 FSE was that, while it would have been appropriate to inform the local EOC of what was going on, the Unified Command's primary efforts did not require any action from the New London authorities, and allowed for alternative information flow processes per doctrine.

It should also be noted that the New London EOC, as is likely with most local governments, does not have the personnel to provide liaisons with the State or Federal command posts/operating centers. During the initial stage of the response, the New London EOC was apprised of the situation and the actions being taken by the local police and fire department personnel on the scene and the 911 dispatcher. Once those elements left the scene and left the response effort as a whole, the locals had no formal representation anywhere in the response chain. The result was not just exclusion by the UCP, but also by the State and JFO. The situation was exacerbated in Connecticut by the lack of a direct line of communication between the local EOC and State EOC. Instead, all communications flowed through an Area Coordinator. The New London EOC made numerous resource and information requests of the State through the Area Coordinator, but responses were consistently slow or nonexistent. For example, a request for all-terrain vehicles took almost two hours to reach the State EOC, which responded that the request would take six hours to fulfill—well outside the needed response timeframe. Another example of poor communication between operating centers and the local EOC is the fact that the New London EOC learned via VNN when the Governor raised the threat level, declared a state of emergency, and issued the shelter-in-place advisory in New London.

3. Concern About Lack of Alignment Between NCP and NRP

Limited evidence from the T3 FSE exists to suggest there were problems with concurrent implementation of the NRP and NCP. This evidence largely focuses on confusion over the role of the RRT, resource request processes, and information flow. This evidence, combined with concerns expressed by exercise participants and observers over the alignment of the two plans, suggests the need for clarification and greater detail regarding how the two plans intersect, how to better integrate NCP response mechanisms with those of the NRP, and how to better coordinate the response efforts. Although ambiguities in these areas may not have caused noticeable problems during the T3 FSE, they appear to be of concern to the responding agencies and therefore merit further consideration.

a. Role of the RRT and its relationship with ESF #10

The ESF #10—Oil and Hazardous Materials Response Annex to the NRP—describes the relationships among the ESF #10, RRT, and FOSC as ones of support and coordination. But little detail is provided as to how this support and coordination would occur. The annex states:

- "During a response, RRTs deploy their respective agency response resources and provide assistance and advice to the Federal OSC(s)."
- "During an incident, the RRTs coordinate with the NRT and provide support to the Federal OSC."
- "To the extent possible, support agency representatives to ESF #10 should be those personnel also assigned to the NRT or RRT(s)."
- "Either the EPA or DHS/USCG Co-Chair of the RRT serves as the regional lead for the ESF [#10], depending upon which agency is primary agency."
- "The regional lead for ESF #10, in coordination with the OSC, consults the RRT for advice or assistance, and establishes appropriate mechanisms for the RRT to coordinate with the JFO during an incident as needed."
- "Upon identification of actual or potential releases of oil and hazardous materials, the regional lead for ESF #10 closely coordinates with the OSC(s) and the RRT (if convened) to develop and implement a response strategy."

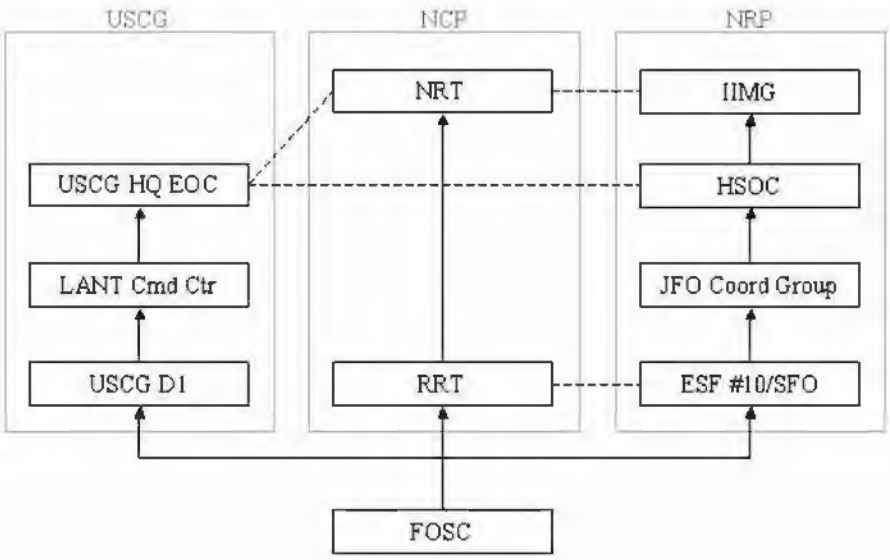
These six statements represent all of the guidance that the annex provides regarding the relationship between the RRT and ESF #10. Yet the two teams are very similar on paper. They both include representatives from EPA and USCG, as well as any other agencies with responsibilities in oil and hazardous material releases. They both provide guidance and subject-matter expertise to the FOSC. ESF #10 alone serves as the coordination point for the FOSC to align NCP response activities with the rest of the Federal efforts, whereas the RRT connects NCP efforts on the ground with policy and strategy decisions by the NRT.

The lack of understanding of and clarity on the role of the RRT caused confusion for the USCG FOSC in terms of reporting requirements and where to go to seek guidance. The FOSC was under the impression that he had to keep both the RRT and ESF #10 updated

on the situation—a dual reporting burden for his staff. Additionally, he was concerned with seeking technical advice from both organizations and potentially receiving conflicting guidance. A late afternoon conference call on April 4 between the ESF #10, FOSC, and RRT attempted to clarify the role of the RRT and the means of coordination among the three groups. The decision was made to integrate the RRT into the response process via the SFO in ESF #10. Despite this apparent resolution, uncertainty persisted. On April 6, the FOSC forwarded a request to the RRT, suggesting that it coordinates with ESF #10 to establish a panel of experts to advise the Unified Command on the environmental effects of mustard and the remediation requirements. This justification for the request was to reduce the reporting requirement and the possibility of conflicting recommendations.

In fact, the FOSC in the T3 FSE had a triple-stranded reporting requirement—his internal agency chain, the NCP reporting chain, and the NRP strand. These three reporting chains are shown in Figure VI-8. The dashed lines represent points where the NRP Annex suggests there should be coordination.

Figure VI-8. FOSC Reporting Chains During T3 FSE



The lack of understanding on the role of the RRT and its relationship with ESF #10 caused confusion. The activation of both the RRT and ESF #10 appeared redundant, which increased confusion, raised concerns over conflicting advice, and appeared to add to the FOSC's reporting burden.

b. Overlapping Funding Streams and Resource Requests

The NCP implements the response authorities and responsibilities granted by the CERCLA. Agencies leading NCP response efforts have access to CERCLA funding and the authority to request additional Federal support as needed. NCP actions do not require

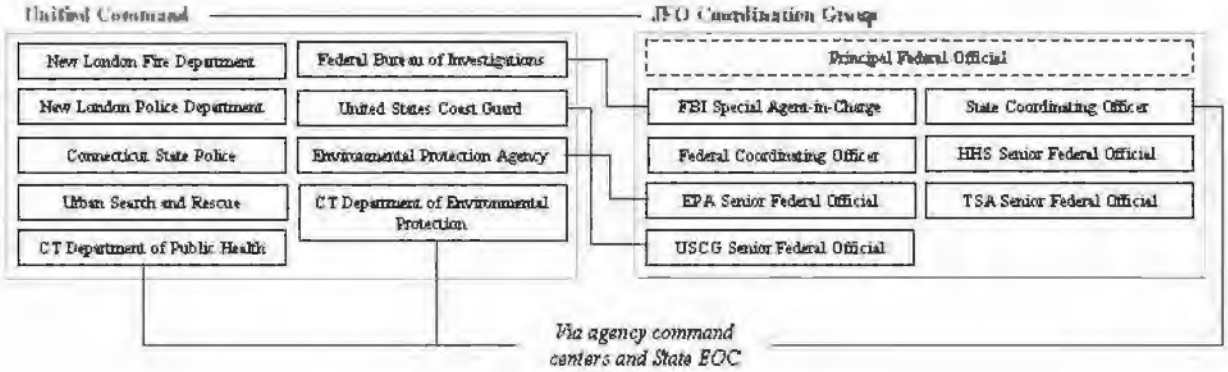
Stafford Act funding or approval by the FCO via the FEMA ARF-MA process. As a result, there is the potential for duplicate resource requests from the NCP agencies at the UCP and from the FEMA structure at the JFO, as well as the potential for the FOSC to direct Federal resources controlled by the FCO. The process in place to prevent such overlaps is UCP coordination via ESF #10, as discussed in the NRP annexes and referenced previously. The T3 FSE data reveal no specific examples of competition for resources between the FOSC and FCO or dual requests. However, requests for resources by the Unified Command under NCP authorities and under the Federal-to-Federal request process of the NRP did add to the confusion among the various operating centers regarding what assets were being requested, who was requesting these assets, and the status of those requests.[77] This suggests that coordination of resource requests by the Unified Command via ESF #10 either did not occur or was insufficient. Internal AARs, exercise observations, and comments to data collectors note the potential for problems and indicate that additional clarification of authorities and coordination mechanisms are needed for FOSCs and FCOs to avoid conflicts in directing Federal resources and to maintain awareness of each other's resource requests.

c. Coordinating Mechanisms and Information Flow

The way the NCP was implemented in this exercise changed the information flow and coordination processes established in the body of the NRP. Figure VI-2 highlighted the basic principle of NRP information flow from the IC or Unified Command through the local EOC, to the State EOC, and on to Federal agencies at the JFO. Activation of the NCP inserts a different information flow process into the mix, from the Unified Command directly to the JFO.

Figure VI-9 applies the connectivity construct developed in the NRP annexes to the UC and JFO in Connecticut during the T3 FSE.

Figure VI-9. Connectivity Between the Unified Command and JFO Coordination Group in Connecticut



[77] This issue is discussed in greater detail in the Resource Allocation chapter of the AAR.

The NRP annexes associated with NCP implementation with and without ESF #10 activation are the only location in the former document where it indicates that the Unified Command should be coordinating and communicating directly with the JFO and JFO Coordination Group. The information flow process implemented during concurrent NRP and NCP implementation has too many points of connectivity between the UC and the JFO Coordination Group, while potentially excluding the local and State EOCs. For example, on April 5, the UCP made a direct request of ESF #10 to assist in the relocation of small businesses affected by the incident. This request did not go through the State EOC or the normal JFO route. The presence of so many nodes can lead to poor information control and could confuse the operating picture.

4. Limited Understanding of the Scope of Unified Command's Responsibilities

The focus of an IC is direct control of tactical operations. As the multijurisdictional or multiagency replacement for an IC, the common assumption is that the Unified Command's purview is also tactical operations on scene and the response efforts related to management of the incident site. Traditionally, all other local concerns fall to the local EOC. Neither NIMS nor the NRP specifies any change in the Unified Command's purview in WMD responses; when a "site" may not be clearly defined or identified; when tactical operations may rapidly conclude; or when State and Federal organizations may play a larger role.

Per the ICS and NIMS, IC/Unified Command are responsible for establishing priorities and objectives for the incident response. The IC's focus in Connecticut was on treating victims and securing the scene. The response by emergency personnel involved medical triage, victim recovery and transport, verification of the presence and identity of a contaminating agent, and decontamination of victims and personnel. The New London Fire Chief supervised and directed local emergency responders and State and Federal assets in the relevant activities to meet these objectives. Once the emergency response concluded the night of April 4, the focus of the Unified Command shifted from emergency response to evidence collection and remediation. The Unified Command laid out its objectives in IAPs covering the planned activities over the next operational period (24 hours).

Many of the response activities and support pursued by Federal and State agency representatives at the UCP appeared to go beyond tactical operations at the incident site. UCP representatives from the U.S. Public Health Service Commissioned Corps and the NDMS were involved in tracking victim numbers, resolving bed availability issues, and facilitating requests for Disaster Mortuary Operational Response Team (DMORT). Members of the UC developed a risk communications plan in case of an evacuation, and issued recommendations for the public to the State EOC and JFO with regards to outdoor activities. On April 6, the Unified Command established a new team in the Operations Section to evaluate Maritime Security (MARSEC) measures on commercial shipping and develop responses to adverse effects.

In general, the role of the Unified Command is not well understood in an NRP response effort. The Unified Command concept is introduced in NIMS as an alternative or transitional option from a single IC. But it is not given much consideration in the NRP, which simply defines it without explaining the transition from IC to Unified Command, the determination of membership, the coordinating functions, the avenues for conflict resolution among members, or the scope of its responsibilities. The lack of a clear definition of the Unified Command's scope was apparent in the UCP activities in T3 and in comments from participants during and after the exercise.

5. Issues from Previous Exercises

Table VI-1 summarizes the observations from SOEs and the T3 FSE with regard to emergency response operations under a Unified Command. Note that the T2 AAR did not identify any issues with respect to response operations under a Unified Command.

Table VI-1. Comparison of T3 FSE with Previous Exercises

SOEs	T3 FSE
ISSUES/OBSERVATIONS	
• Officials expressed general concern about the concurrent implementation of the NRP and NCP.	• Doctrinal details were insufficient regarding concurrent implementation of the NRP and NCP, and the resulting duplication of roles, competition for resources, and coordination of information. • Activation of both the RRT and ESF #10 appeared to be redundant and complicated matters for the FOSC.
	• The Unified Command did not maintain clear oversight and awareness of activities at the incident site to ensure effective planning. • Agencies in the Unified Command did not have full-time representation at the UCP, which hampered integrated planning and coordination of operations. • Response operations pursued by the Unified Command bypassed the established information flow process through the local and State EOCs. • The Unified Command's scope of responsibilities was not clearly understood.

F. Recommendations

- Encourage members of the Unified Command to provide full-time representation in the UCP.
- Establish clear procedures for information sharing and coordination between the UC at the Incident Command Post, the JFO Coordination Group, and state/local EOCs (separate from procedures for processing resource requests)
- Develop standard operating procedures for concurrent implementation of the NRP and NCP that expand on the coordination methods identified in the NRP annexes. Include how to transition between an NCP-only response and a concurrent NCP-NRP effort.

- Clarify and document the role of the RRT and its relationship with ESF #10.
- Expand the NRP to include discussion of the Unified Command, its scope of responsibilities, and interactions with other emergency response centers.
- Expand NIMS to include more detail on the Unified Command.
- Develop standard operating procedures for the Unified Command that detail the transition from a single IC, the determination of membership, the coordinating functions, the avenues for conflict resolution among members, the determination of location (e.g., offsite or on-site), and the scope of its responsibilities.
- Develop criteria for an IC to use to determine the circumstances under which it is appropriate to stand-up a Unified Command.
- Recommend position-specific Incident Commander training for all potential Incident Commanders.
- Discuss the development of a National IMAT made up of interagency members, instead of a Coast Guard-only IMAT.

Part 6: Conclusions

This section summarizes the primary issues or observations and recommended courses of action associated with each of the ten analysis topics. Next to each recommended course of action is a designation of whether this is a National Response Plan (NRP)-related issue, policy issue, procedural issue, planning issue, organizational issue, information-sharing issue, or public information issue.

I. Homeland Security Advisory System (HSAS), State Threat Conditions, and Associated Protective Measures

Issues/Observations
• Real-world and exercise elevations of the HSAS level to Orange and Red indicate that implementation of the HSAS is not systematic. • There does not appear to be a formal mechanism for coordinating, reporting, and tracking changes to HSAS and State threat levels and implementation of associated Federal, State, local (FSL), and private sector protective measures. • The absence of a mechanism for coordinating the implementation of protective measures can contribute to an uncoordinated response. • Unintended consequences of implementing HSAS Red protective measures are not well understood. • Officials in the T3 Full-Scale Exercise (FSE) used the HSAS and State threat conditions as a means of facilitating emergency response operations more than as a threat advisory system. • Inconsistent messages and little specific puhlic guidance limit the value of the HSAS as a warning/advisory system.
Recommended Courses of Action
• Develop a formal process for coordinating and tracking implementation of severe (or Red-level) protective measures across FSL government agencies and the private sector. (Procedural) • Provide more specific guidance regarding actions recommended under the different color-coded threat conditions and link the levels to specific protective measures. (Information Sharing) • Re-examine and refine the potential purposes of the HSAS: (1) public warning and advisory, (2) attack prevention, and (3) emergency response. (Policy)

II. Joint Field Office (JFO) Operations

Issues/Observations
• Lines of authority and coordination among the Principal Federal Official (PFO), Federal Coordinating Official (FCO), and JFO sections were unclear and hampered the efforts of the JFOs in Connecticut and New Jersey. • The relationship between the PFO and FCO is not formalized, and final authority over the JFO cell was unclear. • In Connecticut, the PFO cell duplicated many of the capabilities and much of the expertise resident in the JFO sections, but lacked its own clear purpose or it delineated responsibilities. This often resulted in overlapping or competing activities occurring in the PFO cell and the JFO sections. • The JFOs did not follow standard processes for sharing information internally.
Recommended Courses of Action
• Clarify the relationship between the PFO, PFO cell, and FCO, including the scope of their operational responsibilities and their authorities within the JFO. (NRP) • Develop a checklist to manage the integration of the PFO cell with the JFO sections once the latter is fully activated. (Procedural) • Implement formal information-sharing processes and procedures within the JFO to improve internal situational awareness. Identify, train, and authorize an individual to manage the JFO and information-sharing processes. (Procedural)

III. Resource Requests and Resource Coordination

Issues/Observations
• The use of multiple resource processes created uncertainty and adversely affected situational awareness. • State and Federal officials struggled with the implementation of the Federal resourcing process. • The role of the Department of Health and Human Services (HHS) Secretary's Emergency Response Team (SERT) was not well-defined or understood by participants. At times, the SERT duplicated functions performed by Emergency Support Function (ESF)-8 in the JFO. • Information about the status of resources was not readily available, and the process lacked transparency.
Recommended Courses of Action
• Develop a unified Federal emergency resourcing process that supports resource requests from the State under the Stafford Act and resource requests for Federal-to-Federal support under other Federal authorities. (NRP) • Provide States with a team of subject matter experts who are knowledgeable on Federal capabilities and the resource requesting process. (Organizational) • Document the mission assignment process more thoroughly in the NRP. (NRP) • Clarify the role of the SERT during emergencies. Consider using the SERT to augment ESF-8 at the JFO or deploying the SERT to the State Department of Health to provide subject matter expertise in identifying and requesting Federal medical support. (Organizational) • Make information about resource requests readily available, including what resources or capabilities were requested, who made the request, how the request is being funded, and its current status. (Information Sharing)

IV. Information Sharing

Issues/Observations
• Information systems used in T3 were largely stovepiped within agencies and/or response communities. • The vast number of operating centers negatively affected information sharing by increasing the scope and complexity of the problem. • The use of informal or alternate channels for sharing information caused problems by enabling circular reporting and bypassing authoritative sources. • The T3 FSE revealed a lack of uniform reporting guidelines and procedures for validating information received from secondary or tertiary sources. • Agencies and operating centers acted and made decisions on different information. • Situational awareness was not effectively shared across operating centers and agencies.

Recommended Courses of Action
• Support the development of interoperable information systems and/or a suite of emergency response/management applications that can be used across response communities. (Information Sharing) • Consider development of a DHS field operations guide that lists radio frequencies/preferences of federal, state and local responders to expedite the development of communications plans. (Information Sharing) • Assess the roles and responsibilities of each Federal operations center and consider reducing the number of operating centers, consolidating them, or co-locating personnel. (Organizational) • Require that reports of casualty numbers include a clear description of the information being conveyed. (Information Sharing) • Identify key terms that are likely to appear during a Weapons of Mass Destruction (WMD) response, standardize their definitions, and disseminate the information across the entire response network. (Information Sharing) • Establish mechanisms to update and disseminate new definitions during response operations. (Information Sharing) • Identify and define the overlapping essential elements of information (EEIs) required by all the response communities. (Information Sharing) • Establish specific reporting protocols and guidelines for all levels of government. (Procedural) • Identify the authoritative sources for EEIs and what EEIs should be included. (Organizational) • Identify an operating center at each level of the response to act as the "keeper of the critical information." (Organizational) • Develop protocols for horizontal and vertical coordination (i.e., horizontally across one level of government and vertically between levels) to align the operational pictures developed and maintained by different operating centers and agencies. (Procedural)

V. Stafford Act Declarations

Issues/Observations
• It remains unclear whether an incident with a non-explosive biological, chemical, or radiological weapon would fit the definition of a major disaster under the Stafford Act. • Other Federal programs may provide assistance in lieu of a major disaster declaration. • The Stafford Act provides for the possibility of exceeding the $5 million limit set for an emergency declaration; therefore, reaching that limit is unlikely to result in significant impacts on response spending. • Lack of detailed information to agency staffs on verbal approvals of presidential declarations caused initial uncertainty at the National Response Coordination Center (NRCC), Regional Response Coordinating Centers (RRCCs), and State Emergency Operations Centers (EOCs) in Connecticut and New Jersey.
Recommended Courses of Action
• Determine the applicability of a Stafford Act major disaster declaration to non-explosive incidents involving WMD, particularly those involving a large-scale bioterrorism incident. (Policy) • If these types of incidents do not fit the definition of a major disaster declaration, determine whether exemptions within the Stafford Act for Emergency Declarations and other Federal programs can result in an equivalent level of assistance. If they can, ensure that States are aware of them. (Policy) • If the Stafford Act major disaster declaration does not cover these types of incidents and equivalent Federal assistance is not available through other means, pursue legislation to address this problem. (Policy) • Until legislation is passed that would allow these types of incidents to receive the full range of Federal assistance provided under a major disaster declaration, identify other Federal programs that may be able to provide assistance, and ensure that States are aware of them. (Procedural)

VI. Emergency Pnblic Information

Issues/Observations
• Numerous tools, prompted by lessons learned during the T2 FSE, were implemented in T3, including a Ready Room, National Incident Communications Conference Line (NICCL), and public affairs guidance. • FSL agencies used a variety of means to reach the public; made joint public statements; and actively worked to combat rumors, consistent with the NRP and Incident Communications Emergency Reference (ICER) guidance. • In New Jersey, public messaging occurred largely at the State level with little coordinated local visibility. Local top officials were more visible in Connecticut. • FSL agencies may still not be prepared to provide swift, accurate, consistent lifesaving protective action guidance to the public. • The operations of multiple Joint Information Centers (JICs) were not always coordinated, and there was no evidence of use of a Joint Information System (JIS). • DHS' pre-exercise coordination with international participants may be a model for coordinating international incident communications in a terrorist attack.

Recommended Courses of Action
• Develop the mechanisms to prepare FSL top officials to provide swift, accurate, comprehensive, and consistent potentially life-saving protective action in a terrorist attack with time-sensitive implications such as the scenarios used in T3. • Develop a supporting concept of operations (CONOPS) to complement ESF-15 and Public Affairs Annexes of the NRP and the ICER, and to provide more specific operational implementation guidance for executing incident communications in the context of the NRP. • Consider using future exercises to further test/refine protocols (which could be documented in the CONOPS), and educate stakeholder organizations on how incident communications coordination mechanisms, such as the NICCL, can be used to promote a common operational picture and coordinate message content when appropriate. • Expand NICCL to an audio/visual forum that allows collaborative tracking of the evolving facts and message points. • Expand DHS Public Affairs Guidance product to provide more specific message points, and consider linking it to NICCL updates. • Establish primary information sources early in the incident, such as the State hotlines and websites in New Jersey and Connecticut. • State governments should develop complementary incident communications plans for SNS distribution and work closely with all affected localities to ensure that the guidance to the public provided by localities is clear and comprehensive.

VII. Integrating Responses to Incidents of National Significance: Public Health Emergency and the Stafford Act

Issues/Observations
• Neither the NRP or the HHS CONOPS provides sufficient guidance for coordinating assistance for incidents that are concurrently covered under a Stafford Act declaration and a public health emergency. • HHS does not have a detailed process for requesting and coordinating Federal-to-Federal assistance for public health emergencies. • The funding capabilities of HHS and the funding responsibilities of States and other Federal agencies are unclear under a public health emergency.
Recommended Courses of Action
• Clarify the process for Federal-to-Federal support for non-Stafford Act assistance in conjunction with a Stafford Act declaration. Determine whether the action request form-mission assignment (ARF/MA) process can be used to request resources under other Federal authorities and how to coordinate those requests with the JFO. (NRP) • Develop a transition plan for coordinating incidents that start under non-Stafford Act authorities, but later grow to include a Stafford Act declaration. (NRP) • Clarify the process for Federal-to-Federal support under a puhlic health emergency. Include how HHS should coordinate with other Federal agencies, who is best suited for coordinating and tracking requests (e.g., HHS or the Federal Emergency Management Agency (FEMA)) and what responsihilities other Federal agencies have to report to HHS. (Procedural) • Clarify the funding capabilities and responsibilities of States, HHS, and other Federal agencies under a public health emergency. (Policy)

VIII. Strategic National Stockpile (SNS) and Points of Dispensing (PODs)

Issues/Observations

• The throughput of the real PODs fell short of the goal of 1,000 persons per hour, which was established in the *New Jersey Mass Prophylaxis Manual*. That goal was an important assumption behind the massive prophylaxis campaign adopted by the State.
• Timelines for establishing and staffing additional (notional) State and Federal PODs were most likely not achievable.
• The resources required to staff the nearly 400 State and Federal PODs were not identified and were probably unavailable in the given timeframe.
• Proposed locations of the notional Federal PODs were problematic. Postal facilities do not appear to be good candidates, and the Health Resources and Services Administration (HRSA) Centers are privately owned, not government owned.
• The plan to provide prophylaxis statewide evolved during the course of the exercise and did not appear to reflect a pre-planned and carefully integrated Federal and State response.
• It is not clear that the Federal government has a strategy or plan for implementing its own system of PODs or for rapidly identifying and supplying staff to support State efforts in the event of a large-scale requirement.
  ○ Efforts to coordinate the Federal and State distribution systems were ineffective.
  ○ Federal and State PODs followed different standards of care, with State PODs using more rigorous and resource-intensive standards.
• The use of fixed distribution sites as the sole approach to providing prophylaxis for a large number (millions) of people may be impractical.
• Some combination of fixed sites and other means of distribution, such as those being developed for the City Readiness Initiative (CRI), could be necessary to reach large numbers of people.

Recommended Courses of Action
• Develop joint Federal and State scalable prophylaxis plans that address a requirement to reach very large numbers of people. Plans need to include a combination of approaches, including fixed sites and direct delivery of prophylaxis. (Planning) • Expand the prophylaxis/planning practices and tools developed under the CRI to include regions and cities not currently covered. (Planning) • Develop options and guidelines for conducting large-scale prophylaxis. (Planning) • Determine whether the Federal government should be prepared to operate its own POD system in the event of a major public health emergency. (Policy) • Develop Federal plans for quickly identifying and providing staffing resources to States to support large-scale prophylaxis implementation. (Planning)

IX. Agent Confirmation and Hazard Area Definition

Issues/Observations
• Specialized incident site response units did not exhibit a clear understanding of each other's roles, authorities, and SOPs. • The lack of a formally defined information flow process from the incident site resulted in premature public messages and decision making about the identity of the chemical agent. • The Interagency Modeling and Atmospheric Assessment Center (IMAAC) successfully provided a common plume picture for use by FSL officials. • The IMAAC did not appear to have adequate procedures in place to deal with discrepancies or contradictions in inputs or modeling requests from various agencies.
Recommended Conrses of Action
• Clarify the various response organizations' roles and responsibilities at the incident site to include the timing of responsibilities and their value to the larger response operation. (Organizational) • Clarify the formal information flow procedures from the incident site to the rest of the response organization and assert the authoritativeness of formal processes over informal information movement. (Information Sharing) • Clarify the IMAAC processes for receipt and review of other modeling products and establish a protocol for other modeling agencies to distribute to their consumers on the purpose of their product and the guidelines for redistribution. (Information Sharing) • Develop procedures on how the IMAAC should handle discrepancies in data inputs or product requests and identify a process to aid the IMAAC in deconflicting inputs. (Procedural) • Clarify the responsibilities, authorities, and mechanisms for the IMAAC to formally disseminate critical information learned through its scientific analysis of the incident. (Information Sharing)

X. Emergency Response Operations under a Unified Command (UC)

Issues/Observations
• The UC did not maintain clear oversight and awareness of activities at the incident site to ensure effective planning. • Agencies in the UC did not have full-time representation at the Unified Command Post (UCP), which hampered integrated planning and coordination of operations. • Response operations pursued by the UC bypassed the established information flow process through the local and State EOCs. • Doctrinal details were insufficient regarding concurrent implementation of the NRP and National Oil and Hazardous Substances Pollution Contingency Plan (NCP) and the resulting duplication of roles, competition for resources, and coordination of information. • Activation of both the Regional Response Team (RRT) and ESF-10 appeared to be redundant and complicated matters for the Federal On-Scene Coordinator (FOSC). • The UC's scope of responsibilities was not clearly understood.

Recommended Courses of Action
• Encourage members of the UC to provide full-time representation in the UCP. (Organizational) • Discuss the development of a National IMAT with interagency membership, as opposed to a Coast Guard-only IMAT. (Organizational) • Establish processes for regular sharing of information with personnel at the incident site when an off-site UCP is established. (Information Sharing) • Rework information flow processes involving the UC to include the local and State EOCs, even when using Federal-to-Federal support or NCP authorities. (Information Sharing) • Develop standard operating procedures (SOPs) for concurrent implementation of the NRP and NCP that expand on the coordination methods identified in the NRP annexes. Include how to transition between an NCP-only response and a concurrent NCP-NRP effort. (NRP/Procedural) • Expand the NRP to include discussion of the UC, its scope of responsibilities, and interactions with other emergency response centers. (NRP) • Expand NIMS to include more detail on the Unified Command. (NIMS) • Develop SOPs for the UC that detail the transition from a single Incident Commander, determination of membership, coordinating functions, avenues for conflict resolution among members, determination of its location, and scope of its responsibilities. (Procedural) • Develop criteria for an Incident Commander to use to determine the circumstances under which it is appropriate to stand-up a UC. (Policy)

THIS PAGE INTENTIONALLY LEFT BLANK

Homeland Security

Top Officials 3 (TOPOFF 3) Full-Scale Exercise (FSE)

Executive Overview of Preliminary Findings and Assessment

(Classification consideration derived from *DHS SCG SLGCP-001, January 2005*)

July 8, 2005

Annex A: Executive Overview

I. Introduction

Top Officials 3 (TOPOFF 3) was a congressionally mandated, national counterterrorism exercise designed to identify vulnerabilities in the nation's domestic incident management capability by exercising the plans, policies, procedures, systems, and facilities of Federal, State, and local response organizations against a series of integrated terrorist threats and acts in separate locations in the northeastern United States.

The United Kingdom (ATLANTIC BLUE) and Canada (TRIPLE PLAY) conducted simultaneous, related exercises with overarching international exercise objectives to improve mutual response and preparedness against global terrorism. The three domestic scenarios were enhanced by incorporating events from the other two countries. The planning and execution of the three national exercises provided an excellent opportunity for international cooperation, networking of key responders, and sharing of information on each country's concepts of emergency operations.

The following report summarizes the preliminary findings/lessons of TOPOFF 3 and suggests remedial actions to address identified shortfalls. An official TOPOFF 3 After-Action Report (AAR) will be promulgated on September 30, 2005, providing a more extensive analysis of exercise actions against information recorded by exercise data collectors located at key emergency operation centers and exercise sites.

Major sources supporting this review included:

- Master Control Cell Interagency Hotwash
- Connecticut and New Jersey Venue Hotwash Comments
- United Kingdom and Canada Comments
- After-Action Conference (AAC) Out-Brief (Player and Planner)
- HSC Comments
- DHS I-Staff AAR
- IIMG/HSOC Comments
- DoD Comments
- T3 Quick-Look Report
- Large-Scale Game (LSG) Quick-Look

Exercise design, exercise play, and exercise review—the three major components of TOPOFF 3, were all cast in deference to the four major objectives of the Full-Scale Exercise (FSE):

- Incident management: To test the full range of existing procedures for domestic incident management of a weapons of mass destruction (WMD) terrorist event and to improve top officials' capabilities to respond in partnership.

- Intelligence/Investigation: To test the handling and flow of operational and time-critical intelligence between agencies in response to a linked terrorist incident.
- Public Information: To practice the strategic coordination of media relations and public information issues in the context of a WMD terrorist incident.
- Evaluation: To identify lessons learned and promote best practices.

The issues presented here are divided into four broad categories:

- topics related to Federal, State, and local coordination;
- topics related to the execution of procedures detailed in the National Response Plan;
- topics related to environmental considerations resulting from a WMD incident; and
- topics related to international communications, coordination of response, and role responsibilities resulting from a WMD incident in the United States.

All have been validated as concerns worthy of remedial action/effort by the sources above and, in most cases, multiple sources.

The format used herein is:

- ***Issue*** (presented in abbreviated, but recognizable, form)
- ***Discussion*** (circumstances surrounding the issue)
- ***Recommendation*** (actions suggested as remediation for identified problem)

The collective of most of the resources listed above are posted on the DHS ESP portal in the T3 library documents section. Additional information can be gained though review of these sources or by contacting the SLGCP Exercise Director.

II. Executive Summary Overview

A. Federal, State, and Local Coordination Process

1. Emergency Declaration Process

Issue: Stafford Act declarations require comprehensive review.
Discussion: Entitlement differences between "emergency" and "major disaster" are inconsistent when applied against a multiple WMD attack.
Recommendation: Impose the more encompassing "major disaster" declaration for all significant terrorist events.

2. Coordination of Strategic National Stockpile

Issue: There was a perceived lack of coordination between FSL mass prophylaxis plans.
Discussion: Rapidly rising casualty numbers required officials to develop an ad hoc process to augment State prophylaxis plans.
Recommendation: Initiate interagency effort to examine existing SNS distribution plans.

3. Coordination of Federal and State Medical Response Plans

Issue: Perceived limitations exist relating to medical provider surge capability in response to WMD incidents.
Discussion: Gaps in organizational plans related to deployment of medical personnel affected the response to the incidents.
Recommendation: Initiate review of Federal, State, and local plans to validate medical surge capabilities.

4. Homeland Security Advisory System (HSAS)

Issue: Elevation of HSAS levels raised persistent questions, triggering critical time-consuming coordination hurdles.
Discussion: Operational consequences of the elevation of HSAS conditions need to be balanced against general public perception/public good.
Recommendation: DHS, in coordination with the HSC, should study the implications of revising the HSAS to align it more directly with the operational requirements surrounding the implementation of protective measures.

5. Private Sector Integration

Issue: Concerns were raised regarding communication between governmental and private sector organizations.
Discussion: Reported informational disconnects between FSL governmental entities and private sector suggests a need to accelerate recognition of the private sector in U.S. HLS effort.
Recommendation: Consider a more robust private sector integration strategy to facilitate full use of private sector resources in the national HLS effort.

6. Critical Infrastructnre/Key Resources

Issue: Concerns surfaced over compatibly of Federal and State efforts in applying protective measures for land, sea, and air infrastructure and transportation resources.
Discussion: There appears to be inconsistency between Federal and State responses to the HSAS elevation as it affects Critical Infrastructure/Key Resources.
Recommendation: Revalidate Federal and State protection plans, especially regarding the transportation sector.

B. National Response Plan Issues

1. Statutory Authority

Issue: Concerns were raised regarding alignment of statutory authorities that predate DHS and the NRP.
Discussion: Uncertainty exists whether NRP guidance has been fully integrated into Federal procedures that predate DHS.
Recommendation: Conduct a review of all Federal statutes and agency response plans related to terrorist incidents and ensure the NRP guidance is fully integrated.

2. JFO/PFO Decision Making

Issue: The level of effectiveness of the PFO in facilitating coordination between Federal and State government in question.
Discussion: After-action assessment of exercise suggests a lack of understanding of the role of the PFO by key response personnel at all levels.
Recommendation: Direct enhanced NRP training for critical staffs (i.e., IIMG, HSOC).

3. JFO Integration

Issue: The PFO cell appeared isolated within the JFO.
Discussion: Full functionality of the PFO within the JFO was not realized in the area of coordinated Federal/State/local (FSL) messaging and deconfliction of interagency policy.
Recommendation: Further refine the definition of PFO roles and responsibilities. As necessary, review and revise the structure supporting the PFO and JFO. Develop/implement expanded staff training.

4. PFO Selection Process

Issue: The selection of a PFO already holding a key position within an affected region can prove detrimental to the response effort.
Discussion: The PFO selection process must compare the ramifications of having a qualified leader with existing relationships selected from the affected region with assigning a qualified individual from outside the region.
Recommendation: Develop a decision matrix that weighs all the pros and cons associated with the PFO selection.

5. Incident Reporting Requirements

Issue: The incident reporting process lacks standardization across the interagency realm.
Discussion: The misalignment and/or misinterpretation of the vital information being passed among "top officials" provides senior leadership with an ill-defined operational picture.
Recommendation: DHS to refine internal reporting process and lead a Federal coordination effort.

6. Information Management Systems

Issue: Shortfalls were evident in the information management processes used to support the response effort.
Discussion: The Homeland Security Information Network (HSIN) was clearly underused.
Recommendation: HSIN should be reviewed to consider its intuitiveness and user distribution.

C. Environmental Issues

1. Bio Watch Detection Timeline

Issue: The Current Bio Watch assessment process is labor-intensive.
Discussion: Improved Bio Watch monitors could possibly accelerate confirmative agent identification.
Recommendation: Initiate an evaluation of existing technologies for automated bio agent detection.

2. Bio Watch Monitor Coverage

Issue: Coverage for high-risk areas is limited by the number and placement of monitors.
Discussion: Bio Watch coverage is incomplete in areas evaluated as high-risk.
Recommendation: Consider expanding the number of monitors and review placement strategies.

3. WMD Contamination Management

Issue: Common WMD decontamination and cleanup standards have not been adopted across the Federal, State, and local realm.
Discussion: States and local jurisdictions affected will likely request Federal guidance/assurance.
Recommendation: DHS should accelerate development of consensus-based standards.

D. International Perspectives

1. International Incident Management Communications

Issue: Challenges were noted related to integrating domestic and international incident communications.

Discussion: The exercise demonstrated the importance of having the U.S. embassy serve as the focal point for international discussions, especially during a crisis response.
Recommendation: Clarify the role of the State Department in support of the context of incident management, enhancing international incident management communications.

2. Alert and Advisory Systems

Issue: Uncertainty existed regarding each nation's alert/advisory system.
Discussion: The impact of U.S. HSAS changes has a cascading effect on many international issues.
Recommendation: Establish a working group to review and integrate international alert/advisory systems.

3. International Aviation Issues

Issue: Exercise incidents resulted in numerous aviation issues related to transportation and commerce.
Discussion: "*How clean is clean?*" remains a challenging question given dissimilar international protocols and procedures, especially with regard to aviation issues.
Recommendation: Establish common international standards of "cleanliness" related to aviation during incidents of WMD terrorism.

III. Executive Overview Issues

A. Federal, State, and Local Coordination

1. Emergency Declaration Process

Issue: The authorities, processes, and assistance eligibilities associated with Stafford Act declarations require a comprehensive review in the context of terrorism incidents, specifically bioterrorism. (Recommendations about amending the Stafford Act were offered in the evaluations of the TOPOFF 2000 and TOPOFF 2 events. Although slightly different in nature, a fundamental shortfall in the Stafford Act has been identified for remedial action.)

Discussion: The Stafford Disaster Relief and Emergency Assistance Act provides for two types of declaration, "emergency" or "major disaster." These declarations result in different levels of Federal relief/assistance to State and local governments. Emergency declarations are available in any instance in which the President determines Federal assistance is necessary to supplement State and local efforts to save lives and protect property, public health, and safety, or to lessen or avert the threat of a catastrophe. Both the Connecticut and New Jersey T3 Full-Scale Exercise events met this definition.

"Major disaster" assistance is available only for natural catastrophes or, regardless of cause, any fire, flood, or explosion, per 42 USC 5122. The Connecticut exercise scenario involving a vehicle-borne improvised explosive device met the requirements of a major disaster. The New Jersey biological exercise scenario did not meet this definition. During TOPOFF 3, after Stafford Act declaration requests were received from both governors, the president, following the statutory guidelines of the Stafford Act, declared a "major disaster" for Connecticut and an "emergency" for New Jersey.

As a result the legal constraints associated with each declaration acted to define the support limits available to State and local governments. For example, New Jersey businesses were ineligible for the Small Business Administration's disaster loan program until the Presidential Declaration of Emergency was amended. Other Federal disaster programs remained unavailable to New Jersey residents. The declaration in New Jersey actually made incident management more cumbersome for authorities and led to a public perception that New Jersey's crisis was less important than the event in Connecticut. New Jersey's public reaction was captured by the media and preceded official government messaging regarding this issue.

Further, the authorities of the Secretary of Health and Human Services (HHS) under the Public Health Services Act have not been reconciled with those of the Stafford Act in response to a WMD event.

Recommendation: Review the Stafford Act and propose an amendment to allow for a declaration of "major disaster" for all significant terrorist events.

2. Coordination of the Strategic National Stockpile

Issue: During TOPOFF 3 FSE, the effort of the Federal government and the State of New Jersey to provide mass prophylaxis to the State's entire population following the biological attack revealed notable shortfalls in effectiveness. The speed and scale of the challenge (i.e., to put medications in the hands of the affected population in a secure and timely manner) is clearly not being met fully by existing plans.

Discussion: Shortly after New Jersey initiated its five-day SNS distribution plan, rapidly rising casualty figures prompted the Federal government to rapidly accelerate and augment New Jersey's distribution plan. Staff from DHS, HHS, and New Jersey worked quickly to develop an ad hoc process to supplement New Jersey's planned distribution centers with additional Federal centers located in the most severely affected counties. This plan, relying upon the rapid deployment of large numbers of Federal health care workers and other Federal personnel with material resources, effectively reduced the distribution timeline to only two days. Some level of preliminary FSL planning occurred, yet few participants from that planning effort were completely satisfied with the outcome. Participants cited a number of concerns related to the overarching SNS. Included were:

- the adequacy of State and local jurisdiction plans to make effective distribution on a massive scale;
- the adequacy of State and local jurisdiction plans to determine which segments of the population require prophylaxis;
- whether the State and local jurisdiction plans have been exercised to ensure that mass distribution of SNS materials can be readily accomplished with State and local indigenous resources;
- whether to provide priority prophylaxis to health care workers and responders;
- the ability to provide targeted distribution strategies (e.g., intensive efforts to localize geographically by risk);
- the optimal method to provide security for the supply convoys and distribution sites; and
- whether the Public Health Security and Bio-terrorism Preparedness and Response Act of 2002 funding increased SNS distribution capability at the State and local level.

Recommendation: DHS and HHS should partner to initiate an interagency/intergovernmental effort to coordinate Federal and State plans for medical response planning for tasks related to the distribution of the SNS.

3. Coordination of Federal and State Medical Response Plans

Issue: The national health support structure was not engaged to obtain appropriate assistance in dealing with the catastrophic incident presented.

Discussion: The status of the State and organizational plans as they relate to the deployment of medical assets in support of efforts of this magnitude, translates as a limiting factor in response efforts (i.e., How can the numbers of potential personnel available to assist be maximized? and

How can their related operational readiness be assessed?). Appendix 6 of the NRP-Catastrophic Incident Supplement (CIS) defines deployment timetables and suggests template components for consideration in designing a State and local strategy to deal with large-scale crises.

Planning factors relevant to this exercise were:

- the availability of hospital beds and specialized care equipment for WMD victims;
- the capability to rapidly transport both response resources to an incident site and large numbers of victims to health care facilities;
- lack of decontamination capability for numerous victims prior to hospital intake;
- inadequate personnel to rapidly triage, shelter, and treat large numbers of victims at receiving hospitals, as well as the inability to provide enough doctors, nurses, and medical technicians on-scene.

Recommendation: DHS should initiate an aggressive effort to encourage all States to design medical surge strategies based on the templates and support mechanisms outlined in the CIS.

4. Homeland Security Advisory System (HSAS)

Issue: Reacting to changes of the HSAS Threat Condition during TOPOFF 3 presented participating international, Federal, State, and local officials with persistent critical time-consuming challenges.

Discussion: HSPD-3, amended by HSPD-5, promulgated the HSAS as the primary framework for setting and communicating risk conditions and directing or recommending protective measures. Although the HSAS Threat Condition has been elevated to *Orange* on six occasions, it has never been elevated to *Red* outside of an exercise environment. Exercise activities have not clearly defined the ramifications of an elevation of the HSAS level to *Red*.

During the initial hours of the exercise, officials spent an inordinate amount of time attempting to resolve the issue of elevating the HSAS Threat Condition to *Red* following recognition of confirmed terrorist attacks. These difficulties continued later in the exercise as senior Federal officials perceived that there could be negative effects from the State-mandated protective measures that were activated when the State's tbreat condition was raised to *Red*. These perceptions should be explored and, if negative effects are likely, they should be addressed.

Many complications surfaced during the exercise that impacted decisions about the elevation and reduction of the HSAS Threat Condition. There appeared to be insufficient understanding among the Federal departments and agencies about what actions each might take at *Red*—leading to unanticipated negative consequences when the decision to go to *Red* was made. The consensus of opinion suggests that DHS, in coordination with the HSC, should revisit the HSAS and align it more directly with the operational requirements surrounding the implementation of protective measures while assessing its utility as a public messaging tool.

Decisions surrounding HSAS Threat Condition elevation was driven by the need to send a consistent and effective message to the public rather than the need to activate the appropriate protective measures required to prevent or mitigate the effects of further attacks. For example:

- Senior Federal leaders felt obliged to raise the threat condition to *Red* despite concerns about its effect on the response due to public expectations that the highest threat condition must be appropriate following an actual terrorist attack—"If not *Red* now, then when?"
- The debate over HSAS Threat Condition elevations tended to be focused more on its public warning and public messaging purpose than on the evaluation of the appropriate protective measures required to prevent or mitigate the effects of further attacks.
- As the exercise progressed, protective measures were increasingly de-coupled from the HSAS Threat Condition (e.g., a set of proposed measures was alternately labeled "*Orange Plus*" or "*Red Minus*," without changing the proposed set, depending on an anticipated HSAS Threat Condition decision.

Recommendation: The HSAS should be reviewed to consider aligning it more directly with the operational requirements surrounding the implementation of protective measures. Its utility as a public messaging tool should be examined to determine if disseminating the level of protective measures taken is properly interpreted by the public and elicits the intended response.

5. Private Sector Integration

Issue: Although TOPOFF 3 provided private sector organizations and associations a tremendous opportunity to test emergency response and business continuity plans in conjunction with Federal, State, and local response agencies, inconsistency existed in passing information between the government and private sector participants.

Discussion: TOPOFF 3 marked a significant increase in the involvement of the private sector in the exercise process. The private sector was successful at gaining access to incident response channels, but they were less than completely successful at gaining accurate and useful information to satisfy their situational awareness requirements.

The private sector owns 85 percent of the nation's infrastructure and has the potential to play an enormous role in the response to a credible threat, or in support of the nation's critical infrastructure after a terrorist attack. The U.S. government has committed to exercise and assess its ability to successfully communicate and coordinate with the private sector. Exercises such as TOPOFF 3 provide an excellent opportunity to identify the critical links between all levels of government and Critical Infrastructure/Key Resources sector-oriented private sector organizations required during the response and recovery from a WMD incident.

Recommendation: DHS should expand communication/coordination efforts with private sector entities in future TOPOFF series exercises to include formalizing the Private Sector Cell prototype at the National Infrastructure Coordinating Center (NICC). Permanent implementation would enable private sector representatives who have responsibility for the nation's critical infrastructure and key resources to carry out their NRP-defined roles during an incident of national significance.

6. Critical Infrastructnre/Key Resources

Issue: Federal, State, and local governments and private sector entities encountered difficulties in coordinating the application of transportation sector protective measures to land, sea, and air arteries in response to changing HSAS Threat Conditions.

Discussion: Federal, State, and local governments and private sector entities have made some inroads to develop protective measures corresponding to the HSAS Threat Conditions, with a specific focus on the Critical Infrastructure/Key Resources sectors identified in HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection." The IIMG maintains detailed protective measures listings, mapped against key homeland security mission areas, which are updated following operational periods and exercise events involving a HSAS Threat Condition change. As DHS officials attempted to implement these measures in response to T3 exercise events and threat condition changes, they found themselves in conflict with the measures that State authorities had also taken in response to threat condition changes.

Protective measures taken by the transportation industry (State and private sector) across New Jersey in response to the declaration of HSAS Threat Condition *Red* were seen by IIMG analysts reporting to the IIMG as overly restrictive and potentially adversely affecting the provision of life-sustaining services and the national economy. State-initiated security measures, including such actions as closing all interstate highway traffic and banning most forms of travel; had the potential to increase the negative effects of the terrorist incident well beyond the benefits to the effort to contain the biological event.

An example of the Federal and State governments working at cross purposes was the situation at the Newark International Airport. The Federal government considered the airport open and operational, while its non-Federal staff had been released from work by the acting governor's threat condition *Orange* and *Red* declarations. As a result, Federal authorities anticipated that, in an actual event, the ability to deploy emergency assets could have been limited.

Recommendation: DHS should initiate an interagency effort to re-examine and further refine the coordination of Federal and State plans for development and implementation of protective measures with a specific focus on the Critical Infrastructure/Key Resources sectors, especially in the Transportation sector.

B. National Response Plan Issues

1. Statutory Authority

Issue: The NRP provides a framework designed to integrate and focus the entire nation's capabilities. Concerns exist, however, regarding statutory authorities that predate the statutory authorities that established DHS and the operational constructs of the NRP.

Discussion: Opinions differ regarding whether these pre-NRP requirements have been fully integrated, reconciled, or updated to reflect the role of DHS and the NRP. Many Federal departments and agencies have preexisting mandates, structures, rules, and procedures associated with national disasters and potential terrorist events that predate the DHS and NRP.

Recommendation: Consensus suggests that an interagency-wide comprehensive review and reconciliation may be needed for the various statutes, authorities, directives, policies, and SOPs that relate to the range of incident types described in the NRP.

2. Joint Field Office/Principal Federal Official Decision Making

Issue: Despite the presence of a PFO at both exercise venues, after-action observations suggest coordination of information and operations between Federal and State governments did not meet the needs/expectations of each level.

Discussion: During TOPOFF 3, the PFO in New Jersey experienced a number of instances where key decisions were made by Federal and State officials without the appropriate consultation and, typically, with negative results. The New Jersey PFO TOPOFF 3 AAR cites the following examples:

"The PFO lacked involvement with the Point of Dispensing (POD) negotiations between HHS headquarters and the DHS IIMG. The IIMG sent down a compromised strategy, apparently negotiated with HHS and/or the State which allowed for the implementation of an unworkable and unrealistic Federal plan.

The PFO was unaware until late in the exercise of several conversations between the governor's representative and the SLGCP regarding a number of issues [including coordinating HSAS Threat Conditions] being worked at the JFO."

In Connecticut, the PFO/JFO and State EOC interchanges were affected by the establishment of a "Unified Command Post" (UCP). The UCP was sanctioned under the Oil Spill Contingency Act. Additionally, due to assumed exercise constraints, the UCP was fully established and operational far earlier than it would have been had this been a real attack. As a result, activities/issues that would have stressed the layers of management (local, regional, State, etc.) were managed at the UCP.

Although the role of the PFO is defined in the NRP, the actual process of its integration with the other participants at the State and Federal levels continues. Similarly, although there is still room for improvement in the communications infrastructure within the PFO cell, this problem is not principally the result of telecommunications shortfalls. The root cause of confusion about the PFO is most likely the lack of training and experience with the NRP for personnel staffing the key incident management nodes. Few of the exercise participants have sufficient actual or training experience in incident management under the NRP in response to large-scale terrorist attacks such as that in the FSE scenario.

Recommendation: DHS should develop a Federal Incident Management Training Program to prepare its employees to support the structures and processes of the NRP during an incident. Currently available training programs do not sufficiently prepare the Federal incident management staff to perform their required duties under the NRP. DHS should develop a Federal Incident Management Training Program to train the staff of the HSOC, the IIMG, other DHS operations centers, and the deployable staff of the PFO cell to execute the processes and implement the support structures of the NRP during an incident.

The training program could be considered a potential "certification" function for assignment to selected key roles once the program matures. Aspects of this training should include:

- classroom instruction, as well as supporting interactive, collective training opportunities;
- curriculum linked to actually executing incident management under the NRP;
- training on the information management systems;
- focus on developing the staffs of the HSOC, the IIMG, the DLT, and DLT staff that support incident management, other DHS operations centers, and the deployable staff of the PFO cell; and
- availability to appropriate interagency staffs who serve in DHS fixed or field headquarters cells.

3. Joint Field Office Integration

Issue: The current integration status of the PFO cell and its members within the larger JFO structure justifies an accelerated strategy.

Discussion: TOPOFF 3 provided an opportunity to review the interrelated operations of the JFO, the PFO, and the PFO support cell. In some ways, the JFO operations conducted during TOPOFF 3 were not fully realistic; the two JFOs were operational much earlier than could be expected in an actual event, sites had been preestablished and prepared in advance, and staffs were predesignated and had trained together with knowledge of the exercise's operational scenario. The exercise designers accepted the introduction of these artificialities to achieve a few days of near-steady State operations by these entities within the confines of a four- to five-day exercise.

Many exercise principals indicated the lack of clear distinction of the PFO as a separate entity from the JFO Coordination Group in organization diagrams. Additionally, the inclusion of the PFO in key JFO planning processes seemingly blurred the distinction between the PFO as an overarching strategic coordinator and the JFO Coordination Group as the managers of operational strategy.

Despite the lack of resolution on these issues, the value of the PFO as the DHS Secretary's representative during an incident of national significance was validated by the clearly successful use of the PFO and the PFO support cell as the key DHS communications and coordination link in the field. The PFO successfully resolved potential conflicts with State and local authorities regarding threat condition announcements, risk communications, requests for Federal assistance, and protective measures in both venues. The PFO cell served a critical reporting function providing regular situation reports and answers to ad hoc requests for information. The value of these services was best illustrated when communications or coordination inadvertently bypassed the PFO.

Recommendation: The roles and responsibilities of the PFO and the PFO support cell in regard to their integration with the JOC require further definition. Adjustments are possible within the parameters of documents such as the PFO and JFO SOPs and the deployment of the proposed Federal Incident Management Training Program recommended above.

4. PFO Selection Process

Issue: The selection of a PFO for a particular incident can have a negative effect on the providing agency's ability to perform its incident management responsibilities when that individual's agency happens to play a key role in the response effort.

Discussion: The DHS Secretary designated the USCG First District Commander as the PFO for the WMD event in Connecticut and the FEMA Region II Director as the PFO in New Jersey during the exercise planning process. The selection of these key regional leaders as PFOs effectively removed them from direct operational command of their normal responsibilities at a point in time when intelligence indicated that there were threats to their respective areas and, especially significant regional ports.

Recommendation: Criteria should be developed for the selection of PFOs to optimize the utility of the selected official for the incident and to minimize the operational effects on the providing agency. DHS should consider the development of a decision matrix, including supporting agency input.

5. Incident Reporting Requirements

Issue: The current crisis reporting process is not standardized and, as a result, T3 was unable to establish a creditable operational "battle rhythm." (The incident reporting/communication issue is a repeat topic from previous TOPOFF events.)

Discussion: The collection and sharing of the information required to manage the multiple incidents in the TOPOFF 3 scenario significantly challenged the current information management process. Symptoms of this problem included:

- officials assigned to a strategic planning role in the IIMG spending considerable amounts of time pursuing the answers to individual requests for incident information;
- senior leadership from DHS arriving at key briefings with data that did not closely compare to that of other Federal agencies, despite efforts to coordinate the information; and
- the misalignment of the data being reported in the HSOC with that reported at the State-level or in the simulated national media.

These problems were identified in processes internal to DHS, as well as in cases where the department relied on interagency coordination.

Recommendation: Improvements in this area should begin with efforts by DHS to further refine and define the internal reporting processes, followed by an effort to lead the coordination of interagency reporting. The remediation effort for this issue would build upon existing standard formats and procedures by:

- clearly delineating agency responsibility for specific topic lines of information in the reports;
- creating a suggested template to drive the generation of a more predictable "battle rhythm" to compel data collection requirements; and

- establishing a realistic cyclic schedule for the information dissemination process.

A well-managed process that has the confidence of the leadership would potentially reduce the requirements for the multiple ad hoc requests for information that plagued the incident operations centers during the first days of the exercise.

6. Information Management Systems

Issue: DHS' automation of its information management processes is not fully mature and did not meet participant information technology requirements.

Discussion: Current DHS information management processes do not fully meet the department's requirement to provide a common reporting process and incident management "battle rhythm;" provide a Common Operational Picture (COP); or provide the automated support to fully share capabilities across the incident management environment. DHS can ensure that these four key elements of its information management process are fully developed and implemented in the near term.

The Homeland Security Information Network (HSIN) expected to leverage and integrate the information available on a number of incident management networks, yet the system was identified as ineffective by exercise participants. Some of the issues with HSIN are noted in this excerpt from the draft New London, Connecticut, JFO TOPOFF 3 After-Action Review.

All participants in the JFO understood the need for a coordinated mechanism to pass up-to-the-minute situation status. As per the [draft] JFO SOP, "*The primary [Sensitive But Unclassified] SBU data circuit within JFO is the Homeland Security Information Network (HSIN) JFOnet.*" However, many responders either did not have access or were not properly trained on how to use JFOnet to either upload or access information.

Similar problems were encountered at DHS headquarters. IIMG members preferred to use Microsoft Outlook to exchange information rather than the tools available in HSIN. As in the JFO in New London, this was because participants either had not been offered training or did not see the benefit of learning to navigate the HSIN.

Recommendation: As part of the refinement of the information management processes outlined above, DHS should conduct a review of the operational requirements for incident management automation. The following is a partial list of some of the features that should be considered for an enterprise-wide Operations Management Suite:

- an interactive, simple to use, but powerful web-based solution with an easy to use and straigbtforward user interface;
- a uniform workspace with a robust emergency management application and a contact relationship manager;
- a collaboration application with virtual meetings and secure communication;
- a highly interactive, simple to use Geospatial Information System;
- a robust content management and information database with interfaces to external authoritative references and key information sources;
- tools that automatically connect real-time information and longer term collaboration, and create knowledge and historical records as a by-product;

- automated emergency response plans and decision support guides that prepopulate the incident workspace and management processes;
- templates to promote standardization and consistency for all incident-related reporting and documentation;
- functions that mirror the NIMS and ICS; and
- interoperability with other Federal, State, local, or field emergency management information systems.

The proposed system "should be designed for use by Operations Center desk officers as well as top level management, leaders, and decision makers [and] support all phases and levels of operations management providing a virtual community for DHS team members, partners, and stakeholders."

IV. Environmental Issues

A. Bio Watch Detection Timeline

Issue: The current Bio Watch assessment process is too labor-intensive. Automated detection and/or signaling technology could reduce the time needed for confirmative agent identification by eliminating or reducing reliance on human interface.

Discussion: The scenario for the TOPOFF 3 Senior Officials Exercise 05-02 ("Fierce Squall") included a Bio Watch detection of Yersinia pestis (plague) in New Jersey. In the SOE scenario, the agent was identified within 36–60 hours of its release. Bio Watch detection was included in the TOPOFF 3 scenario as an inject, but its detection capabilities were not actually exercised.

Bio Watch was evaluated by the EPA's Office of Inspector General in March 2005. According to this evaluation, Bio Watch monitors could accelerate confirmative agent identification through improved technology, techniques, and/or procedures.

There are currently various options that are being explored to increase the efficiency and breadth of coverage. Timelines for analysis depend on the specific biological agent, but Bio Watch currently anticipates detection and confirmation of the presence of agents within 36 hours of release. The system may detect a biological attack in time to allow for early diagnosis and treatment of victims' symptoms (detect-to-treat timeline), and shorter detection times would allow for preventive public warnings and enable better containment and treatment of infection. The survival rate from exposure to certain biological agents is higher when antibiotic therapy can be administered before symptoms appear, but after symptoms manifest, the survival rate diminishes significantly.

Recommendation: The CDC, with support from the EPA, should lead a comprehensive evaluation of existing technologies for automated biological agent detection systems that are being developed by public and private sector entities. Sources to evaluate include:

- DOE National Laboratories' Autonomous Pathogen Detection System;
- DOD Chemical and Biological Defense Program technology;
- Oak Ridge National Laboratory's SensorNet program; and
- U.S. Postal Service's BioHazard Detection System.

The CDC and EPA should continuously reassess collection and analysis procedures to implement quicker, more effective techniques. Techniques could include:

- analyzing samples through mobile laboratory units;
- changing the Polymerase Chain Reaction (PCR) testing process to run primary and secondary lab analysis simultaneously;
- exploring the use of alternate sensor technologies such as biological assays and laser fluorescence;
- supplementing Bio Watch monitors with handheld detection devices;
- incorporating less accurate real-time detection technology into monitors; and
- if employing real-time detection technology, implementing an automatic laboratory alert through wireless devices.

B. Bio Watch Monitor Coverage

Issue: Bio Watch coverage of high-risk areas is limited by the number and placement of monitors.

Discussion: Although Bio Watch aims to provide coverage for a high percentage of a city's population, it is unclear whether current procedures for receipt and integration of Bio Watch capabilities (into established medical and laboratory surveillance networks) are effective. Monitors were originally distributed based on criteria specific to air quality monitoring, not biological agent monitoring. Sensors might be located at less than optimal heights, in locations with obstructed air flows, or spaced too far apart.

Recommendations: EPA and CDC should conduct testing of Bio Watch monitors to measure the range at which they can detect each "Category A" biological agent in high-risk areas. EPA, CDC, and State and local agencies should determine the optimal placement of monitors for maximum coverage in a given area, taking into consideration factors such as height, air flow, environmental elements, security and access, pollution, meteorological data, and proximity to high-risk areas and other monitors. EPA and CDC should consider deployment of mobile Bio Watch systems to areas where monitors have been disabled or destroyed, or where credible intelligence indicates a possible biological attack, taking into consideration possible lack of local laboratories and consequence management plans. To test these capabilities, future exercises should be designed to include activities that would stress these systems to focus on their effectiveness.

C. WMD Contamination Management

Issue: The standards that will govern the decontamination and cleanup of public and private property contaminated during a WMD incident have not yet been universally adopted within the Federal interagency community.

Discussion: Uniform national standards do not exist to determine how clean is "clean" in the aftermath of a WMD incident. Common decontamination and cleanup standards that will be applied to public and private property contaminated by terrorist use of a CWA or a TIC-based WMD have not yet been adopted within the Federal interagency community. The decision-making process and authority for determining such standards are inadequately defined and understood at all levels of government.

During TOPOFF 3, the incident site in Connecticut was extensively contaminated by the terrorist use of HD (sulfur mustard), which was dispersed over a wide area near the city pier. Although the duration of the FSE did not include the environmental cleanup of this agent, issues that placed Federal, State, and local authorities at odds did occur especially around the concern of whether it was safe for citizens in or near the affected areas to disregard the order to "shelter in place" initiated locally. Government messages outlining recommendations regarding the level of contamination and its danger to the affected public were contradictory and presented a picture of confusion.

States and local jurisdictions affected by WMD attacks will likely request Federal guidance on reliable standards. The policy challenge of mid- and long-term contamination management has been identified repeatedly in previous exercises, but remains unresolved.

Recommendation: DHS should sponsor an acceleration of effort to develop consensus-based decontamination standards (crisis and long-term exposure) for the anticipated chemicals, biological agents, and radiological materials that are most likely to be used in a WMD incident.

V. International Perspectives

A. International Incident Management Communications

Issue: International incident management communication channels used during the exercise were not fully coordinated with existing day-to-day international communication channels.

Discussion: The international incident management communication channels were not fully integrated with normal condition communication channels during the exercise. The establishment of the dual communication cbannels created uncertainties and prevented development of a COP. The person-to-person communications that are the norm during routine operations were not as well-developed as agency-to-agency communications activated during crisis conditions.

Also, there was uncertainty about when to call upon U.S. embassies to establish or coordinate communications between foreign government agencies and U.S. counterparts. Further, uncertainty existed regarding the role and responsibilities of the Department of State (DOS) during incidents of national significance (INS), as described in the National Response Plan (NRP) and National Incident Management System (NIMS).

Recommendation: Develop a strategy to fully integrate international incident management communications channels with those used for routine communications. Develop a plan to improve users' expertise with international incident management communications channels. Delineate, disseminate, and test the role and responsibilities of the DOS during INS.

B. Alert and Advisory Systems

Issue: Exercise players were uncertain as to the implications of changes in each country's alert/advisory system.

Discussion: Lack of understanding of what actions and policies were executed during the change in the U.S. HSAS led to uncertainty about how Canada and the United Kingdom should react domestically. Similarly, changes in the United Kingdom's alert system were not fully understood hy the United States and Canada.

Recommendation: Create an international working group to clarify how changes in the United States', Canadian, and/or UK's Threat/Alert levels affect each country's security, alert status, and the ramifications of these different/increased levels.

C. International Aviation Issues

Issue: Recognizing that virtually any major domestic incident will have international consequences (i.e., travel, health, law enforcement, citizens traveling abroad), the exercise revealed complex questions specifically regarding aviation-related issues.

Discussion: A recurring topic pertaining to international travel and trade during the exercise was, "*How clean is clean?*" An international consensus of opinion on tbis issue does not exist. Air travel questions remain unanswered concerning the closing of airfields, aircrews refusing to fly into and out of contaminated areas that remain open, decontamination of the aircraft upon arrival

into foreign countries, quarantine of aircraft (which are owned by companies and not governments), and international procedures for handling potentially contaminated items.

Recommendation: Establish a more clearly defined global protocol on aviation issues as they relate to both individual travel and economic trade issues during responses to incidents of WMD terrorism.

VI. Conclusion

TOPOFF 3 FSE was an innovative, challenging, and highly productive exercise designed to stress the system and the agencies responsible for responding to a terrorist attack. The observations, assessments, and recommendations in this summary were garnered from a number of forums and were validated from a practitioner's standpoint.

As the largest and most complex counterterrorism exercise ever attempted, TOPOFF 3 FSE provided a tremendous opportunity for private sector participants and Federal, State, and local governmental organizations to test their procedures and push their agencies to their limits. Many D/As were successful in straining their policies and procedures, and identified potential shortfalls in the process. In addition, the exercise provided many important lessons regarding Federal, State, and local interagency procedures for communications and the integration of support measures.

Because of the extensive data collection process and the effort to make TOPOFF 3 FSE findings both well-documented and traceable through a detailed reconstruction of the exercise events, the more detailed AAR currently in development should provide a baseline upon which subsequent TOPOFF and other counterterrorism exercises can build and be rigorously compared.

This document has been drafted to provide key decision makers with an executive-level assessment of areas and issues that warrant immediate attention and improvement. The lessons derived from this exercise will be valuable to other States and localities as they work to train, exercise, and improve their response capabilities in support of our homeland security.

Annex B: Intelligence Play

I. Summary

The Department of Homeland Security (DHS) made information sharing one of the four key objectives in the Top Officials (TOPOFF) 3 (T3) exercise. To ensure that information sharing was appropriately exercised, an Intelligence Working Group (IWG) was formed. The IWG defined and charted the real-world information sharing channels that presently exist. This enabled T3 planners to create preventable acts that could be put into play through streams of intelligence for analysts to evaluate and intercede if the assessment dictated.

Real-world issues related to intelligence channels, disconnects, and other contentious or undefined areas in the intelligence community (IC) and information sharing arena that significantly impacted the T3 exercise were:

- identification of systems used to contribute to and create a common intelligence picture;
- validation of Interagency processes for information sharing;
- improvement of situational awareness; and
- request for information (RFI) process.

The following annex captures the planning process for the T3 IWG, reviews the intelligence portion of the Full-Scale Exercise (FSE), and identifies lessons learned in information and intelligence sharing. Throughout this annex, recommendations are offered as potential means to improve the handling and flow of operational and potentially time-critical intelligence and analytical products.

II. Introduction

A. Intelligence as an Exercise Objective

To increase the participation of the IC in the TOPOFF exercises, DHS designated intelligence information sharing as one of four key objectives in the T3 exercise. The objective was to test the handling and flow of operational, time-critical information, intelligence, and analytical products.

The integration of intelligence is seldom played at realistic levels in full-scale DHS exercises. Typically, intelligence is a tool used to stimulate play to test operational objectives. Intelligence summaries are produced in the planning process and injected by the control cell at specific times to drive operational decisions.

In conjunction with the objective to test the handling and flow of operational intelligence, the T3 design team created preventable acts with which to confront the intelligence

sector, providing situations that, if assessed correctly, could be intervened or stopped. This intelligence play began 30 days prior to the FSE.

B. Intelligence Working Group

The *T3 Intelligence Working Group Concept Paper* identified the following functions for planning intelligence play:

- Design a functional exercise intelligence architecture that allows for analyst play and the distribution of exercise intelligence through existing real-world intelligence channels. The intelligence architecture must ensure that exercise intelligence does not mix with real-world intelligence.
- Allow participation of top officials; allow the appropriate dissemination of intelligence to State, local, and international exercise participants; and remain linked to the exercise scenario and the Master Scenario Events List (MSEL).
- Develop T3 intelligence play injects and work with the exercise design team to develop realistic intelligence injects.
- Focus on prevention and examine Interagency and international intelligence-sharing processes to ascertain terrorist threats, identify targeted critical infrastructure, and prevent terrorist attacks against the United States and its allies.

The IWG developed an all-inclusive intelligence architecture that resulted in a 70-page document. It became not only a handbook for the exercise, but a handbook for real-world processes in Interagency information sharing that did not previously exist in any government publication. (*Information related to the classification and availability of this document is available through Ms. Sandra Santa Cosgrove, Acting Branch Chief, National Exercise Division, DHS/FEMA, at (202) 786-9594).

III. Backgrouud

A. Intelligence Architecture

Since 9-11, improvements in information sharing have occurred largely due to informal practices such as analyst exchanges and issue-specific distribution lists. Doctrinal changes have also improved information sharing, including the U.S. Patriot Act, the Intelligence Reform and Terrorism Prevention Act, DCID 2/4 and 8/1, multiple executive orders, and memorandums of understanding on information sharing within the IC. Most members of the IC have either augmented an existing counterterrorism (CT) component

or, in some cases, created new ones. The primary counterterrorism centers within the IC are:

- DHS Information Analysis and Infrastructure Protection (IAIP)
- CIA Counterterrorism Center (CTC)
- Federal Bureau of Investigation (FBI) Counterterrorism Division
- Defense Intelligence Agency Joint Intelligence Task Force—Combating Terrorism

Rather than discussing each department or agency in depth, the IWG looked at the intelligence functions to determine how the intelligence members worked together overall. Though terms vary, each department and agency has a process for which information is collected, exploited, analyzed, fused into products, disseminated, and used to support decision making. Decisions based on the best information available result in further requests for information, reprioritization of collection assets to gather more information and reallocation of efforts to meet new demands. Regardless of whether the data collected is satellite imagery or a passenger itinerary printout, it is collected because the data was deemed important. Thus, the cycle begins with planning and guidance that translates into tasks.

This cycle of tasking, collection, analysis, production, and decision making occurs within all government and private organizations. When an issue such as homeland security or counterterrorism cuts across the missions of multiple agencies, the same intelligence process occurring within each organization must be repeated and applied to the Federal government at the aggregate level. In this case, the whole is greater than simply the sum of the parts. The T3 IWG used this cycle to describe the relationship between Interagency intelligence organizations as a way to avoid stove-piped discussions about a particular agency or department.

The IWG agreed that the scope of the objective spanned beyond the statutory members of the IC. The objective required the examination of information sharing between different levels of government (Federal, State, and local); across different mission areas (law enforcement, homeland defense, homeland security); and between different roles and responsibilities (intelligence, operations, and decision making).

B. Defining Exercise Intelligence

The IWG proposed that the Homeland Security Operations Center (HSOC) act as the chief decision making venue, holding weekly briefings derived from the community representatives that reside at the HSOC. Other agencies were encouraged to pulse their internal processes, enabling their own decision makers to weigh in on the intelligence; however, the coordination would ultimately occur at the HSOC.

Based on the above architecture, the IWG implemented the following protocols:

- Normal intelligence channels would be used when:
  - Secret level would be the baseline assumption.
  - Some intelligence might be at higher levels.
  - Tear lines would be encouraged for release to Canada and the United Kingdom (UK).
- Distribution lists would stay true to real-world lists rather than "shot-gunning" all intelligence to all players.
- The Secretary of Homeland Security would be requested to send a letter to the IC departments and agencies (D/As) requesting participation in T3.
- As DHS would be using a fictitious Universal Adversary (UA) (rather than the real-world actors in the FSE scenario), the IWG would provide UA data on various systems for the analysts to research as they would real-world intelligence.
- White noise would be used to obscure the FSE and preventable act intelligence and force analysts to sort through a variety of message traffic.

C. Full-Scale Exercise Intelligence

Once the exercise architecture was established, the IWG identified intelligence indicators that could be created for each event in the scenario, together with associated data that an analyst would require to fully assess the intelligence. For example, the scenario stated that, at D-240, a UA terrorist network sent the precursor material from North Africa to Connecticut. The Department of Defense (DoD) IWG listed potential intelligence indicators such as UA members confirming that a shipment was underway. They also identified potential information gaps to the development group responsible for the generating the scenario—how was it transported, on what vessel, what is the cargo manifest list, crew list, port of entry, and so forth.

Ultimately, the IWG scripted 42 injects providing vague indications and warnings to the events that would occur in the FSE. These injects would take the form of messages originating primarily from the national intelligence agencies and FBI. There was some debate over the assignment of date-time-groups for these injects. According to the scenario, many events occurred as far back as D-400, yet exercise intelligence play was slated to kick off on March 7. The group decided that all injects predating March 7 would be released into real-world systems on Friday, March 4, and all other messages would be released according to their date-time-groups. In retrospect, the initial drop heightened the alert levels in many agencies and allowed analysts to piece together the threat stream more quickly than if the intelligence had flowed over a longer period of time.

D. Preventable Acts

The IWG created five "preventable" acts and sequenced them so that one act could be averted each week during the month of March. A small group consisting of DoD (JS J2 and NORTHCOM), FBI, DHS IAIP, and United States Coast Guard (USCG) met on

October 14 to develop these vignettes—one to meet each agency's objective. Exercise guidelines dictated that the preventable acts could not deviate from the FSE storyline and that the vignettes must not leak too much information about the FSE, thus threatening the exercise startup conditions prescribed for the venues. Finally, all proposed acts would be coordinated with the other members of the IWG and ultimately approved by the DHS exercise planners.

The five original acts included:

- New Jersey (NJ) – arrest of Fatima Barakah (the microbiologist who developed the *Yersinia pestis* weapon for the NJ terrorist cell) as she tries to leave the country
  The objective of this preventable act focused on locating Barakah and arresting her prior to her departure for Miami. The key training audience included the NJ Joint Terrorism Task Force (JTTF), NJ State Police, FBI headquarters, Customs and Border Patrol, Transportation Security Administration (TSA), and IAIP.
- Connecticut – break-up of a support cell in Connecticut and arrest of their logistics coordinator
  The key training audience included the New Haven FBI Field Office, Connecticut JTTF, and the Connecticut State Police.
- NORTHCOM – break-up of a cell in New Jersey that was threatening to attack a military base
  The purpose was to train NORTHCOM Counterintelligence Field Activity–West analysts whose mission was to fuse counterintelligence and law enforcement information to assess threats to DoD facilities.
- USCG – identification and interdiction of a vessel transporting terrorist materials
  The objective was to support the USCG requirement of a field training exercise in which their new Enhanced Maritime Safety and Security Team could conduct a visit, board, search, and seizure operation outside the 12 nautical mile international water line.
- FBI – a credible threat stream used to trigger the FBI to deploy the Domestic Emergency Support Team to Connecticut prior to the start of the FSE

The representatives left the meeting with initial approval from the exercise planners and agreed to meet at the Midterm Planning Conference in November with a draft of each act. They also agreed to hold a scripting conference at the Joint Warfighting Center (JWFC) in Suffolk, Virginia, where the IWG could complete the ground truth documents for each act and begin drafting intelligence injects to support each.

E. Exercise Plan

Having the architecture and preventable acts, DHS exercise planners requested an Exercise Intelligence Annex to the overall exercise plan. IWG members debated over the classification of the annex. One side argued that it should be vague and unclassified because the exercise control cell did not need to know the exact distribution lists and

product details of each agency. Others argued that the document should be written at the classified level simply because no such document currently existed. Such a document would provide enormous value to the community for real-world practices. The IWG decided to provide both products. An unclassified version described the control elements for the intelligence play—RFI processes, MSEL tracking, and so forth (see Annex A). The classified document describing information sharing would become a de facto evaluation guide to how the intelligence play worked in the pre-FSE play. The classified version would contain daily battle rhythms for each organization, expected player products, and details on how the products are disseminated internally and externally for each agency. This product ultimately became the Information Sharing Concept of Operations (CONOPS).

F. Full-Scale Exercise

There were several events that occurred during the FSE that had no intelligence injects to support. These included:

- the fourth vessel en route to Canada;
- Canadian border crossing after the terrorist landed in Maine;
- terrorist activities and plans revolving around Boston and New York;
- FBI operational events occurring during the investigation (e.g., safe house raids, arrests); and
- coordination of Virtual News Network (VNN) unclassified media reports with intelligence.

With the exception of the vessel tracking, these events were not fully synchronized with the IWG. The vessel tracking ground truth changed over 20 times between February and the third week of March. As a result, the data required to generate maritime tracks was late and, during the FSE, conflicting reports confused players.

Regarding VNN, intelligence injects were sent to the VNN scripters to coordinate media reports, but not vice versa. During the FSE, intelligence failed to gain visibility on what media would be reporting that day.

Starting on March 4, the control cell injected 104 intelligence injects into real-world message traffic systems to real-world distribution lists. Most injects were released in classified channels; some were phone calls to operations centers; others were unclassified police reports. During the FSE, the majority of injects came from operations rather than intelligence channels. Over 200 investigative messages were released primarily in law enforcement channels. In all, players produced 140 products, ranging from spot reports to threat warnings to information bulletins. These products appeared in morning situation

briefings, on National Counterterrorism Center (NCTC) Online (NOL), and on seven other exercise websites.[1]

IV. Exercise Design and Artificialities

Without a precedent, the group invented the vignettes, design, requirements, and player expectations right up to the start of the exercise. Mistakes were made, frustrations ensued, but, in the end, most (if not all) of the IWG participants felt that the process presented an extraordinary training and educational experience. The professional relationships formed and cross-agency education exceeded any internal training the planners had previously received. Recommendations to future T3 IWG planners for better facilitation are listed below.

A. Intelligence Objectives, Design, and Expectations

Intelligence objectives, design, and expectations need to be defined at the beginning of the process. Although information sharing was a defined objective—who, what, where, and how to accomplish it—were not defined. As a result, not all agencies were fully prepared to participate in the exercise, and levels of planning and player commitments varied. For example, the White House decision to host twice weekly SVTC meetings in March came two days prior to the intelligence STARTEX and caused participating D/As to drastically adjust their level of play. Furthermore, conflicting guidance on the level of participation was issued. As a result, insufficient time and resources during the planning phase was allocated.

Recommendations:

- Create a memorandum of intent from the DNI providing intent, mission, guidance, and objectives of the exercise and distribute to all IC leaders; formalize effort with a memorandum of understanding regarding planning and vet through all directors of the participating D/As.
- Require early involvement by all agencies deemed vital to the exercise.
- Identify player roles and expectations.
- Establish clear planner/control roles and expectations.

[1] IC websites included NCTC Online, DHS, Joint Staff J2, NORTHCOM J2, NSA, and NGA. SIPRNET websites included NCTC Online, DHS, Joint Staff J2, and NORTHCOM J2. Unclassified portals included LEO.gov.

B. Leadership

The IWG was headed by a civilian contractor and composed of D/A representatives, sometimes contractors, to represent government agency staffs. The chairman performed his function well, but lacked both the position and the authority to make commitments, issue tasks, or make final decisions affecting participating agencies. Also, the group had no senior leadership with the ability to obtain the commitment of organizations crucial to the planning for the exercise, the pre-FSE intelligence phase, and the FSE. The group also relied on a civilian contractor to provide continuity with other planning meetings. There were many lost opportunities to integrate intelligence play with the domestic venues, international activities, media play, and law enforcement operations.

Recommendations: The IWG must be chaired by a senior IC official that is given full tasking and decision-making authority. This individual should:

- Have an understanding of the IC.
- Have a secure position, a position that allows this official to work this as a priority mission, rather than an additional duty (full-time commitment).
- Chair all IWG meetings; issue guidance, direction, and tasks to the members of the IWG; and provide feedback to the IWG.
- Attend venue, Interagency, and media meetings to ensure intelligence activities are integrated with other aspects of the exercise.
- Provide updates to exercise directors of participating D/As.
- Contact D/A directors regarding noncompliance or other issues.
- Have a staff of two to three contractors to assist with administrative work and meeting attendance.

C. Planning Requirements

The planning of the preventable acts was done backwards. Three days before the intelligence phase of the exercise began, a final ground truth document was published. This document endured numerous versions, varied authors, and editing performed without full knowledge of the nuances resident in the document. Unfortunately, not all intelligence controllers started the exercise with the correct version, and, in many cases, were unaware that their versions had been superseded. Two weeks into the exercise, inconsistencies between the ground truth document and proposed injects were noted. Furthermore, several proposed intelligence injects contradicted the content in other injects. Immediate ad-hoc planning sessions were convened to de-conflict these oversights.

Recommendations:

- The overall scenario must be locked prior to the first preventable act planning conference.
- Background material (ground truth documents) must cover all details from "birth-to-death" and from "port to port."
    - The IWG participants can help provide these details.
    - The same working group that develops the exercise scenario should also be responsible for writing the intelligence background material.
- MSEL injects should not be created until these ground truth documents are complete.
- All injects should be scripted and de-conflicted prior to the start of the exercise.
- The only ad-hoc injects that should be allowed are corrective or explanatory injects. New venues or threat streams should not be introduced.

D. International Coordination

International intelligence partners were engaged outside of established, real-world channels. The CIA did not join the planning until January 2005, thus the CIA Chief of Station (COS) in partner nations was not aware of all discussions regarding exercise intelligence play and was not aware of all planned exercise activities. Additionally, the COS was not provided periodic updates so course corrections could be made early in the process.

Recommendation:

- Bring the appropriate DNI and CIA organizations into the planning process as early as possible. Make sure that all U.S. government entities are in agreement on planned activities prior to meeting with international intelligence partners.

E. Control

The Intelligence Control Cell (ICC) needs to be consolidated. When the group worked dispersed during the March 4–31 pre-FSE intelligence play, it was difficult to maintain visibility and control of injects, RFIs, and player status. During this period, the ICC was manned by a skeleton crew. As a result, coordination and collaboration was often chaotic and challenging. However, consolidating the Intelligence Control Group for the FSE was a success.

Recommendations:

- Maintain a consolidated ICC. Ensure representation from all participating D/As (USCG noted as missing in T3 ICC).

- Require additional systems for the ICC that the (Exercise National Military Joint Intelligence Center (the facility where the T3 ICC was located) could not provide:
  - More unclassified computers
  - NSA Net
  - ARCView and ERDAS for NGA
  - IC2PXXX for Maritime Common Operational Picture display
  - Video Teleconference capability
- Consider using USCG Headquarters, Transportation Security Operations Center (TSOC), or JWFC at JFCOM (or similar facility) to provide these capabilities and additional space in future exercises.
- Create a hardcopy library of MSEL items and ground truth documents.

Master Control Cell (MCC) operations during the FSE were completely divorced from intelligence play and the ICC. The classification limitations and lack of secure communications in the MCC prevented intelligence from supporting the FSE operational play. This was illustrated by DHS' and NCTC's reporting of "Nothing Significant To Report" in their morning updates. Many of these issues could have been avoided had intelligence injects to support the FSE been pre-scripted and approved by the MCC. This task was not accomplished because many of the operational events that occurred in the FSE were unknown and/or unavailable to the IWG (see *Leadership* section). Additionally, the MCC had very little situational awareness throughout the FSE due to the lack of secure communications.

Recommendations:

- Integrate intelligence into the FSE and have injects pre-scripted.
- Have established authority to shut down unintended player streams.
- The MCC should be located at a secure facility such as USCG Headquarters, TSOC, or JWFC at JFCOM so that the ICC could be co-located with the MCC. At the very least, the ICC representative at the MCC would have connectivity with the ICC and the players in the intelligence and law enforcement communities.

The RFI process for the exercise was broken. Players received different answers to identical questions, and were completely unaware of what answers were already out there. Despite repeated attempts to control the Interagency RFIs, there was no solution. Most of the issues identified were real-world issues, not exercise issues, therefore the discussion and recommendations regarding this issue are consolidated in the intelligence lessons learned section of this document.

Some agencies disseminated injects to real-world customers, while others limited their distribution list to exercise players. For example, DoD's Defense Attaché Office elements initially did not pass cables to their UK and Canadian counterparts because they were not included on disseminated cables and were later instructed not to participate in the exchange.

F. Universal Adversary

Although using a fictitious terrorist group involves more work upfront for the analysts in terms of studying and preparing analytical documents, there are legal concerns about using a real-world terrorist group or individuals. If the FBI or DHS receives a Freedom of Information Act request for a name of an individual or a group, they are required to turn over all documentation (including exercise inject material) that contains references to the group or individual. Additionally, using a fictitious group avoids the claim that the IC is undermining analytical and operational objectivity regarding the named groups and individuals.

However, the Central Intelligence Agency (CIA) asserts that the use of fictitious individuals and groups undercut their ability to provide robust support to the exercise and severely limits the exercise's utility as a training opportunity for CIA analysts. The CIA routinely provides substantive analytic support to other exercises (e.g., DoD, White House, IC, etc.) where real-world organizations are used. Analysts are able to draw upon years of experience working the particular intelligence problem, thereby enabling them to quickly produce high quality intelligence products in support of exercise play.

Recommendations:

- Resolve discrepancy between FBI/DHS and CIA regarding the use of fictitious versus real-world information for exercise purposes.
- UA should contain additional background data on individuals (i.e., credit and bank histories, publication lists (if appropriate), travel histories, National Crime Information Center hits, watch-listing data).
- UA should contain additional data on terrorist groups (i.e., previously posted disseminated intelligence, open source news articles).
- UA should be available to IC analysts in the form of a database resident on INTELINK and available to State and local LE analysts as a database resident on INTELINK's unclassified Open-source Information System.
- Use photos of Red Team role players in terrorist dossiers where appropriate.

V. Artificialities

Intelligence artificialities included the following:

- The exercise play of the Principals Committee/Deputies Committee/Counterterrorism Security Group process did not reflect real-world processes, making it difficult to draw conclusions about how this process actually works. The fact that many of the participants at these meetings were "role playing" the officials that actually hold these positions caused the behavior of participants to be driven by the artificial exercise environment.

- Few IC agencies dedicated a full team of analysts to exercise participation, so the real-world collaboration that would normally occur did not take place. Analyst play was not uniform across each agency, and those analysts that did participate were not equipped with the Interagency contact lists with which they are accustomed to working.
- CSG and SVTC attendees noted that distribution did not flow in some cases, resulting in a perception of lack of D/A participation. In reality, all agencies had 100 percent participation, resulting in this exercise artificiality.

During the exercise, planners functioned as players in some agencies, and, in others, the players were provided exercise planning information. This resulted in several cases of player "cheating," and severely corrupted the integrity of the analytical component of the exercise.

VI. Exercise Observations

A. Key Issues

Preliminary analysis revealed that not all agencies achieved the same level of situational awareness throughout the exercise. Information flowed, but the speed and degree to which it flowed did not meet exercise planners' expectations. Moreover, the answer to the question of who owns the common intelligence/operating picture remains unsatisfactory, if not unknown. Two major factors quickly emerged as obstacles to an Interagency common intelligence picture (CIP)[2]: systems used to gain situational awareness, and the process by which all agencies gain situational awareness.

B. Systems Used to Contribute to and Create a CIP

1. Dissemination Lists

When controllers released intelligence injects over real-world systems to real-world distribution lists, agencies discovered real-world problems. For example, the TSA Intelligence Service realized that several agencies retained outdated addresses for this organization's predecessor in the Federal Aviation Administration. Also, changes to the DoD Automatic Message Handling System prohibited agencies from sending messages to some directorates within the DoD.

2. Range of Systems/Programs

There is a wide variety of databases and systems that intelligence analysts use to locate information. The Joint Worldwide Intelligence Communications System, Secret Internet Protocol Router Network (SIPRNET), and the unclassified Internet are three separate

[2] A CIP is defined as a picture that facilitates collaborative planning and assists all echelons (extending beyond the primary members of the IC) to achieve situational awareness.

networks. The Homeland Security Information Network, NOL, Law Enforcement Online, and Joint Regional Information Exchange System are portals found on various networks.\Most agencies also host collaborative workspaces on their portals. The "pull" aspect in information sharing is extensive.

Three problem areas emerged under the "too many systems" issue:

- Awareness: Although the IWG "Information Sharing CONOPS" details the products and places available to analysts in the CT community, analysts tended to "pull" from the systems and places they were familiar with.
- Access: Most did not have access to NOL. Few in the IC had access to leo.gov or the jfo.net portal established for the FSE to access law enforcement reporting.
- Accountability: NORTHCOM tended to rely on chat functions (Zircon and Internet Relay Chat, which did not necessarily report actionable intelligence and often resulted in time-consuming tasks to DoD analysts who chased down rumors and faulty information from chats.

NCTC fully supports access and use of NOL and routinely approves access for individuals who meet the security requirements. However, the most significant factor that limited access to NOL, the issuance of an IC Public Key Infrastructure (PKI) certificate by the appropriate D/As, is primarily a problem that resides within those D/As. For non-IC members, NCTC is able to broker the issuance of IC PKI certificates for NOL users in an efficient and effective manner. However, for IC members, the issuance of these certificates is completely controlled by the individual D/A.

As a result of these issues, the situational awareness within each agency varied depending on the reliance of its analysts on different systems.

Recommendations:

1. Scrub IC and Interagency distribution lists.
2. Update lists to include NCTC agencies; promote and facilitate access to NOL.
3. Educate and train chat operators on how to maintain quality control on information disseminated in the collaborative environments and ensure new intelligence is disseminated to support access by the wider IC audience.

C. Interagency Process for Information Sharing

1. Creation of a CIP

Senior players often asked who owned the CIP and wanted visual displays of threat activities, from tactical events at the incident sites to strategic awareness of overseas reporting. Analysts throughout the community were frustrated over the requirement to contact each agency in order to piece together the picture. Often, analysts called the

exercise control cell or simulation cell rather than each other. Conflicting reports emerged in senior-level meetings.

Although there were no straightforward recommendations on where an Interagency CIP exists, there were several observations on how the current system functions. Events during T3 may have highlighted how intelligence agencies can improve situational awareness. A CIP does not attempt to reject outside-the-box analysis, but, rather, to share assessments for utmost situational awareness and development.

Recommendations:

- Make improvements to analysts' awareness of and access to the span of Interagency tools to "pull" intelligence.
    - Retain and maintain an Interagency Handbook for Information Sharing for training purposes. The classified document contains daily battle rhythms for each organization, expected player products, and details on how the products are disseminated internally and externally for each agency; DHS will revise the exercise document for real-world use.
    - Continue to promote access to NOL.
    - Continue analyst-to-analyst exchanges at operations centers.
- Narrow the gap between operational information and disseminated intelligence.
    - Encourage collection and investigation organizations to directly assign reports officers to each collection group involved in the crisis management process and generate intelligence reports for immediate dissemination.
    - Encourage CSG representatives to communicate with their subordinate elements.
    - Review SVTC/CSG notes distribution list.
    - Disseminate DHS Combined Situation Reports to the IC (provides a broad overview of the situation on the ground to analysts and decision makers).

D. RFIs

The RFI process resulted in redundant questions, unanswered questions, and conflicting answers. There was no mechanism to cross-reference responses to RFIs between agencies, as each department or agency has different RFI processes internal to their organization. There are also two types of RFIs: operational RFIs (e.g., analysts' queries for more information based on reporting (What was the license plate on the car?)), and analytical RFIs (questions that require research and analysis and lead to collection tasking (What is the leadership profile of terrorist organization X?)). Our observations and recommendations focus on analytical RFIs.

DoD uses the Community On-Line Intelligence System for End-Users and Managers (COLISEUM), an online database that requires all intelligence agencies within DoD to log their RFI and responses. DHS is moving towards Pantheon, a database built off of COLISEUM, but designed for DHS directorates. The FBI requires external agencies to e-

mail RFIs to the Directorate of Intelligence, Requirements and Collection Unit. NSA has an established process (known as National Signals Intelligence Requirements Process (NSRP)) that few followed due to lack of knowledge from player analysts (especially FBI) about how the process works, or a lack of the NSRP tool at player locations. Many RFIs were submitted to NSA through informal methods (phone calls or e-mails), which made it difficult to keep track of requests and respond in a timely matter.

Internal to each D/A, the RFI process was mostly successful. The problem occurred when the ICC tried to control the answers and found that the real-world system, which the exercise was attempting to simulate, prohibited any control.

Recommendations:

- DDNI/Collection should form an RFI working group to review processes, systems, and provide recommendations for enhancing visibility of RFIs and responses to RFIs between D/As.
  - Consider establishing an RFI fusion center at NCTC.
  - Consider designing an RFI Exercise.
- DoD/DHS should work to ensure that Pantheon and COLISEUM interface. Given that the two databases share architectures and support personnel, the lack of interoperability between the two is a policy issue vice a technological issue.
- Educate new IC members and partners of NSA's NSRP system and encourage them to work with NSA liaisons at their home locations.
- Educate IC analysts about FBI/DHS RFI processes.

E. Flow of Information between Incident Sites and National Intelligence Agencies

In T3, the FBI stood up an intelligence component within the Joint Operations Center (JOC) as part of the Joint Field Office (JFO) (in accordance with the National Response Plan (NRP)) in each venue. During the planning process, DoD and FBI personnel struggled to identify the composition of the intelligence component, as the details are not yet defined in the NRP. Questions such as who sits in the intelligence component and how they integrate with national agencies and the JFO remain unresolved. Because the JFO was a new concept, the objectives were to determine the composition of the intelligence component, the communication requirements and flow, and the integration with the larger JFO. In addition, DoD intelligence players had difficulty identifying how the NRP intelligence component would complement or compete for resources identified in DoD homeland security plans.

When analysts deployed during the FSE to support the NRP, several communication channels failed. Examples of this include:

- USCG did not have secure communications at the JFO.
- The JFO in New Jersey did not have secure communications adequate for Interagency use. The JOC in New Jersey was initially located at the local FBI field office and later moved to Jersey City. The FBI field office maintained secure communications for the duration of the exercise.
- The intelligence component in Connecticut had secure communications, but there was a requirement for PKI certificates that delayed analysts. The intelligence component was eventually managed by DoD due to lack of Interagency participation. Additionally, the JFO intelligence component was shut down early because DoD personnel found that integrating with the JOC was more effective.

Recommendations:

- DHS should develop a detailed plan for the intelligence component and information flow under the NRP.
- FBI, CIA, DoD J2 Intelligence Campaign Plans, and others should work with DHS to define requirements for the intelligence component.
- The Task Force concept should be considered.
- DoD should review the NORTHCOM intelligence planning concepts for support to homeland security operations.
- CONOPS should be developed for the JTF connectivity to JFO intelligence component.

VII. Conclusions

Throughout the After-Action Report (AAR), recommendations are offered as a potential means to improve the handling and flow of operational, time-critical, intelligence and analytical products. These recommendations have been vetted through and discussed by members of the IC as represented by the IWG. Though all observations and recommendations are considered instrumental to improving intelligence and information sharing, a few recommendations stand out as critical.

A. Creation and Maintenance of an Interagency Handbook for Information Sharing

The purpose of this document is to provide analysts with updated information on the structure of the IC, on how intelligence and information flows through the various D/As, and the different RFI processes employed by each member of the IC. It will serve as an instructional guide for analysts to gain familiarity with sister agencies and ideally enhance analyst-to-analyst exchanges. Currently, a draft copy of this handbook has been created and it has been shared with the IC. It will serve as a working document which can

change and adapt as the IC evolves. The DHS (Information Analysis) will serve as the coordination center for changes and updates to this document.

B. Revision of NRP

This revision would include adding a detailed plan for the intelligence component addressed in the current NRP and additional guidance on information flow.

C. Establish Leadership, Participation, and Timeline Criteria

The intelligence piece of the TOPOFF series would benefit from standardizing the planning process. In an effort as monumental as this, the successes of this group must be effectively transferred to the planners of TOPOFF 4.

THIS PAGE INTENTIONALLY LEFT BLANK

Annex C: Private Sector

I. Summary

Private-sector organizations participated in the Top Officials (TOPOFF) 3 (T3) exercise as partners with Federal, State, and local (FSL) government entities to test their combined ability to prepare for and respond to simulated biological and chemical terrorist attacks in Connecticut and New Jersey. The private sector's participation in the exercise was extensive. Over 140 private-sector organizations—representing critical infrastructure sectors, industry associations, public works, faith-based organizations, and multinational non-governmental organizations—played from 450 locations across the United States. The exercise allowed these participants to test the roles defined for private-sector organizations by the National Response Plan (NRP) while also testing new coordination mechanisms, including Private Sector Liaisons and a Private Sector Cell at both the State and Federal levels.

The T3 private-sector participants' involvement in the exercise raised key issues capable of exerting substantial effects on public-private coordination during real-world events. The issues are identified and categorized as follows:

- Prototype Private Sector Coordination Mechanisms
- Public-Private Coordination and Communication
- Testing Internal Emergency Response and Business Continuity Plans
- Cross-Sector Coordination and Communication
- Private Sector Planning
- Volunteer and Donations Management Support

This T3 Private Sector After-Action Report Annex captures the planning process conducted by the Private Sector Working Group, Private Sector Planning Group, and T3 Exercise Planning Team; provides an overview of and analyzes the private sector's participation in the Full-Scale Exercise (FSE); and identifies significant observations and key issues captured by the participants during the conduct of the exercise. The body of this annex concludes with recommendations for improving the integration of the public and private sectors in order to prevent, prepare for, respond to, and recover from weapons of mass destruction (WMD) terrorist attacks.

II. Introduction

T3, the nation's largest, most comprehensive domestic terrorism response and recovery exercise, offered private-sector organizations an unprecedented and unparalleled opportunity to test their current level of integration into the unified and nationwide structure for disaster response and emergency preparedness. The scope and extent alone of private-sector participation was unprecedented—approximately 1,200 individuals representing over 140 private-sector organizations played at 450 locations across the nation during T3. The participating private-sector organizations ranged from small businesses and local transportation providers to Fortune

100 corporations controlling major sub-sectors of the nation's critical infrastructure, from individual public works to multi-million member business associations, from local faith-based organizations to multinational nongovernmental organizations.

T3 also permitted FSL government organizations to exercise their mechanisms and procedures for coordination and communication with the private sector. FSL government organizations assessed the private sector's roles and capabilities in the context of a realistic disaster scenario and gauged the resources that the private sector would need and could provide in order to respond to and recover from a large-scale WMD attack by terrorists.

Private-sector integration is a key component of the emerging unified national structure for disaster response and emergency preparedness. According to one widely cited statistic, eighty-five percent of the Nation's critical is controlled by the private sector. Thus, the National Strategy for Homeland Security states that the Federal government has responsibility for fostering "unprecedented levels of cooperation" between the private sector and all levels of government. Homeland Security Presidential Directive-5 emphasizes "the role that the private and nongovernmental sectors play in preventing, preparing for, responding to, and recovering from terrorist attacks, major disasters, and other emergencies." The Directive further requires the Department of Homeland Security (DHS) to "coordinate with the private and nongovernmental sectors to ensure adequate planning, equipment, training, and exercise activities and to promote partnerships to address incident management capabilities."

TOPOFF 3 tested the plans, policies, and procedures defined in the NRP, and the NRP repeatedly highlights the necessity of private-sector integration. The preface to the NRP states that the implementation of the plan and its supporting protocols "will require extensive cooperation, collaboration, and information-sharing .... between the government and the private sector at all levels."[1]

The NRP includes two support annexes that address private-sector integration in whole or in part. The Private Sector Coordination Support Annex "[o]utlines processes to ensure effective incident management coordination and integration with the private sector, including representatives of the Nation's Critical Infrastructure/Key Resources sectors and other industries."[2] The Volunteer and Donations Management Support Annex "describes the coordinating processes used to ensure the most efficient and effective utilization of unaffiliated volunteers and donated goods during Incidents of National Significance."[3] T3 private-sector integration was designed to test the coordination processes and mechanisms of these two NRP annexes.

[1] NRP, p. i.
[2] NRP, p. xi.
[3] NRP Volunteer and Donations Management Support Annex, p. VOL-1.

A. Purpose of the Private Sector Annex

The Private Sector Annex fulfills the fourth overarching objective for T3: "Evaluation: To identify lessons learned and promote best practices." The description and analysis in this annex are intended to provide a basis for more robust and realistic private-sector play in future TOPOFF exercises. More importantly, the intent is to identify lessons learned that may be used by Federal, State, Local, and Tribal (FSLT) government and private-sector organizations alike to improve their real-world, day-to-day integration into FSLT emergency preparedness and disaster response. The overall goal is to improve the nation's ability to mount an effective, integrated public-private response to and recovery from a WMD terrorist attack.

A second purpose of this annex is to facilitate the Federal government's mandate for a meaningful critique of T3 private-sector integration, a critique that may be appropriately shared with the private sector. The NRP's Private Sector Coordination Support Annex states that the Federal government "conducts after-action critiques of the procedures detailed in this annex with private-sector participants when they are exercised in national-level, DHS-sponsored exercises" and "shares such critiques appropriately with private-sector participants." T3 was such a national-level, DHS-sponsored exercise. This Private Sector After-Action Report Annex is intended to serve as the basis for an appropriate T3 critique that will be shared with the private sector.

B. Scope of Annex

This annex addresses significant issues arising out of the design, planning, execution, and analysis of T3 private-sector integration. This annex does not purport to be a comprehensive review of the entirety of private-sector play in T3. This is not possible, in part because data collectors were not provided for every private-sector organization, nor were they specifically focused on the private sector in the T3 Master Control Cell (MCC). The unprecedented scope and magnitude of private-sector play was deemed in advance to be too great for comprehensive data collection to be effective.

As is true of all T3 evaluations, this annex focuses on high-level issues involving the private sector's emergency preparedness and disaster response coordination. It does not focus on individuals or even on organizations. In the few instances in this annex where organizations are mentioned by name or characterized in a way that may suggest their identity, doing so was necessary to provide adequate context for the issue being addressed or because the organizations are uniquely situated or have unique responsibilities in the nation's integrated structure for disaster response and emergency preparedness.

C. Objectives Guiding Preparation of Annex

In addition to the four primary objectives detailed in the body of the T3 After-Action Report, private-sector integration was designed to fulfill two additional sets of exercise objectives.

The following are the objectives for T3 private-sector integration as determined by the Private Sector Working Group (PSWG):

Intelligence and Information Sharing:

- Exercise communications links with relevant government agencies.
- Improve information sharing processes and capabilities.
- Test the Federal government's Protective Critical Infrastructure Information (PCII) program.

Incident Management:

- Examine private-sector emergency response and business continuity plans.
- Gain and maintain situational awareness of an emerging event.

The second set of objectives designed specifically for T3 private-sector integration was developed jointly by the DHS Office for Domestic Preparedness (ODP), Private Sector Office (PSO), and Infrastructure Coordination Division (ICD). These DHS organizations identified the following as the objectives for T3 private-sector integration from the perspective of FSL government:

Intelligence and Information Sharing:

- Explore options for integrating Federal government/private-sector decision making, incident planning, response, and recovery operations.
- Evaluate information sharing, coordination, and dissemination between private sector and FSL agencies before, during, and after an incident.
- Test the Homeland Security Information Network.
- Test the new DHS/PSO/Federal Emergency Management Agency (FEMA) volunteer and donations website.

Incident Management:

- Test the infrastructure coordination mechanism of the NRP as a single U.S. government point of contact for incident response relative to privately owned critical infrastructure.
- Delineate a course of action for private-sector engagement in the response and recovery mechanisms of FSL departments and agencies.
- Explore the implications and economic impact to the private sector of short-, medium-, and long-term recovery aspects resulting from sustained threat levels and disaster recovery operations.

These objectives guided the data selection, analysis, and reporting reflected in this annex.

III. Background

A. Private Sector Play and Players

Private-sector play during T3 focused on exercising the functional integration of FSL government's coordination mechanisms and processes with the private sector's emergency planning and disaster response and recovery operations. The NRP identifies four summary roles in which private-sector organizations operate during Incidents of National Significance (INS):

- Impacted Organization or Infrastructure
- Response Resource
- Regulated and/or Responsible Party
- State/Local Emergency Organization Member

One or, more often, several private-sector participants functioned in each of these roles during T3. The level of private-sector organizations' participation in the exercise ranged from individuals operating from their organization's offices to a corporate emergency operations center (EOC) and hundreds of employees notionally carrying out their responsibilities under the company's emergency response and business continuity plans.

T3 involved far more private-sector representatives of the nation's critical infrastructure sectors than were initially expected. The PSWG initially hoped to have at least three of the nation's critical infrastructure sectors represented and tested from among the following: transportation (trucking, rail, maritime), chemical/HAZMAT, real estate/commercial, energy (oil and gas), water, and public health. Ultimately, every one of the thirteen critical infrastructure sectors identified in the National Strategy for Homeland Security was represented by more than one player and was exercised during T3. Table 1 lists the industry and critical infrastructure sectors and subsectors and provides the total number of private-sector players that represented each one during T3.

In order to be approved for play, all private-sector participants were required to complete a Player Fact Sheet[4] and submit it for approval to the T3 planning team. Private-sector players were also required to provide a written commitment to communicate exercise-related information according to the protocol defined in the T3 Private Sector Coordinating Instructions and to provide a minimum of one page of feedback after the exercise.

B. Planning and Training Considerations

To ensure that T3 was properly designed and executed to account for the specific and unique characteristics of the private sector, two private-sector groups were formed for the exercise planning process: the PSWG and the Private Sector Planning Group (PSPG). The PSWG was composed of all T3 private-sector participants, as well as the private-sector planners from DHS and the states of Connecticut and New Jersey, as well as the members of the Exercise Planning

[4] The Player Fact Sheet form is an appendix to the T3 Private Sector Integration Concept of Operations.

Team responsible for private-sector integration. Each of the three venues—Connecticut, New Jersey, and National—had its own PSWG. Each venue's PSWG met approximately once a month from September 2004 through February 2005 to disseminate information to the private-sector participants and to generate and capture relevant ideas for the continued planning and execution of T3 private-sector integration.

The PSPG, by contrast, was composed of only those private-sector participants in T3 who were designated by their organizations as T3 planners. Planners were required to attend a one-day training program for T3 field controllers and data collectors that was held in Connecticut, New Jersey, and Washington, D.C., during the weeks leading up to the T3 FSE. The PSPG was far smaller than the PSWG because private-sector organizations playing in the private-sector Tabletop Exercise (TTX) mode[5] were not required to have a planner. About 100 private-sector participants elected to play in TTX mode. The approximately 40 representatives of private-sector organizations who were members of the PSPG were granted access during the T3 planning stage to the draft scenario and Master Scenario Events List (MSEL). They also provided and reviewed proposed events (injects, expected player actions, and requests for information) for the MSEL.

ODP exercised final decision-making authority over all questions and design issues affecting private-sector integration. In addition, the DHS PSO and ICD were heavily involved in the design, planning, and execution of T3 private-sector integration. Among other efforts, the PSO and ICD attended PSWG and PSPG meetings; reviewed the draft exercise scenario; proposed private-sector-specific injects, expected player actions, and requests for information for the MSEL; and facilitated key relationships with and participation by private-sector organizations. The ICD NICC director and his staff planned and provided all of the logistics and other support for the Private Sector Cell co-located at the NICC during the FSE and planned and hosted a T3 private-sector planning meeting in February 2005 and the dry run for the NICC Private Sector Cell.

IV. Exercise Design and Artificialities

This section describes selected private-sector-specific exercise design considerations and artificialities that had a substantial impact on private-sector play in T3. T3 private-sector integration was designed to accommodate characteristics of the private sector that are distinct from most FSL government organizations. Relatively few private-sector organizations and personnel have emergency preparedness and disaster response as their primary responsibility. Before 9/11, relatively few private-sector organizations engaged in disaster response exercises involving substantial interaction with FSL government organizations. Similarly, although many private-sector organizations have well-defined plans for emergency preparedness and business continuity, far fewer have clear, well-defined roles and responsibilities for interacting with FSL government during a disaster response.

[5] The four private-sector-specific modes of play are defined and described more fully below under the heading "Flexible Modes of Private Sector Play."

It thus was determined during the exercise planning stage that private-sector integration should be designed to flexibly accommodate the various levels of time, personnel, and exercise experience each individual private-sector organization could commit to T3. Flexible modes of play and flexible hours of play were two key features designed to accommodate T3 private-sector integration.

An exercise artificiality is a feature of the exercise that could not be played true to reality or freely scripted. Artificialities generally are limitations or constraints on the exercise design. The following artificialities were chosen based on multiple factors. In some cases, the artificiality would not have occurred in a real-world situation; in others, the artificiality was noted because it had a substantial overall impact on exercise play. These artificialities influenced both the exercise design and the conduct of players throughout the exercise. The overall evaluation of the design and execution of T3 private-sector integration should be conducted with an understanding that these artificialities, and others, existed.

A. Flexible Modes of Private Sector Play

Each participating private-sector organization selected and played in one of four modes designed specifically for private-sector integration. The four private-sector play modes are:

- Tabletop Exercise (TTX)
- Command Post Exercise (CPX)
- Closed Loop Exercise (CLX)
- Full Scale Exercise (FSE)

The extent of private-sector organizations' play ranged from notional participation by a few individuals (TTX) to full-scale, on-the-ground involvement (FSE). Each private-sector organization worked closely with the exercise planning team for the venue in which it was playing (Connecticut, New Jersey, or Interagency) to determine which play mode would be the most appropriate for that organization.

The private-sector exercise modes share several fundamental similarities. In all four modes, a private-sector participant's emergency response team, director, or subject matter expert (SME) monitored real-world and simulated channels for information on the unfolding WMD scenario. In all modes, private-sector participants were authorized to disseminate exercise-related information to those personnel at their same location who had relevant responsibilities for responding to the events. All private-sector participants were expected to respond to information about unfolding events according to their pre-established policies, plans, and procedures. For most private-sector participants, this included well-defined emergency response and business continuity plans. Finally, all private-sector participants were free to activate their organizational command posts or EOCs, even though the play mode selected had an effect on the extent of communications these command posts and EOCs could initiate.

Of the four private-sector play modes, FSE mode afforded participants the most robust play. During the exercise, four private-sector organizations playing in FSE mode actually carried out

emergency response operations, including tactical field operations at one or more of the physical locations of the simulated attacks and responses in Connecticut and New Jersey.[6] These FSE-mode players were permitted to coordinate response activities and to initiate communications with any other registered, relevant T3 participant. FSE-mode players were expected to conform their play as closely as possible to the response activities they would actually conduct had the events been real. FSE-mode play was more appropriately suited to non-profit organizations. Few for-profit organizations elected to play full-scale by actually shutting down their operations or deploying participants for tactical field operations.[7]

Approximately 100 private-sector organizations played in private-sector TTX mode. In general, the only external communications TTX-mode players were permitted to initiate were with the NICC Watch or, for those playing in the Connecticut and New Jersey venues, with the Private-Sector Liaison in their respective state's EOC. But TTX-mode players had the option of physically co-locating with a CPX-mode player. In this arrangement, the CPX's T3-trained controller served as the controller for the TTX-mode player as well. Any TTX-mode player that chose this option was permitted an expanded range of communications, including with any other registered and relevant T3 player.

Approximately 36 private-sector organizations played in the private-sector CPX mode. In this mode, the response activities by private-sector organizations extended beyond the internal use of exercise-specific information to (primarily notional) coordination of response activities and communication with other registered T3 participants. Private-sector CPX-mode players that activated an organizational command post or EOC could use it to handle two-way communications with relevant T3 participants from both the private and public sectors. A few TTX-mode and CPX-mode players actually mustered and exercised first responder units, but not at any of the physical locations of the simulated attacks and responses.

Three separate sets of private-sector organizations and associations played in the closed-loop exercise (CLX) mode. Each CLX required a CPX with its T3-trained controller. CLX-mode players were permitted to initiate communications only with their CPX. Members of a CLX could communicate with the other members of their own CLX but only if their CPX controller joined in on the teleconference.

CLX mode was devised during the latter stages of the exercise planning phase, when it was determined that a fourth, new mode of play was needed to accommodate three private-sector organizations and associations. Each of the three represented a large group of players (50+) within a highly specific critical infrastructure or unique sector. The individuals within these organizations and associations needed to share exercise-related information with one another in

[6] As one example, the Salvation Army deployed and operated its canteen operations to feed and care for emergency response workers at the site of the simulated attacks at the City Pier in New London, Connecticut. Such tactical field operations required a Memorandum of Agreement with DHS ODP and the applicable authorities as well as with the venue support team and exercise planning team.

[7] Nevertheless, for-profit private-sector T3 participants from several critical infrastructure/key resources sectors – including transportation, commercial facilities, and telecommunications – have reported that they would prefer, if the exercise design permits, to play in FSE mode during TOPOFF 4.

order to test their respective emergency response and business continuity plans. But a concern arose that the exercise-related information and inquiries any one of these three groups could generate would potentially be too voluminous and multifaceted to be handled efficiently by the rest of the exercise.

Almost all private-sector players participated in T3 in the TTX, CPX, or CLX mode and executed the great majority of their response activities notionally. Few played in FSE mode and carried out their activities "on the ground." The additional artificialities of not playing in FSE mode are likely to have had the most significant effect on private-sector players in critical infrastructure sectors such as the electricity sector and the telecommunications sector. In a real event, they would have had to provide services, maintain equipment, and make critical employees available in the affected areas despite major obstacles such as travel restrictions and limited prophylaxis distribution. Playing in a private-sector mode other than FSE would have had far less effect on the ability of participating private-sector organizations to conduct internal tests of their own emergency response and business continuity plans.

Table 1 shows the number of private-sector organizations that played in each of the four private-sector exercise modes.

Table C-1. Number of Organizations Playing in Each Private Sector Exercise Mode

	TTX	CPX	CLX	FSE
National	59	14	3	0
Connecticut	11	13	0	2
New Jersey	30	9	0	2
Total	**100**	**36**	**3**	**4**

B. Information Exchange in CPX and FSE Modes

Importantly, private-sector organizations playing at the CPX or FSE level were responsible for ensuring that all private-sector organizations with which they exchanged T3 information were authorized to play in T3. A private-sector organization was authorized to play in T3 when the T3 Exercise Director approved the organization's Player Fact Sheet. The exchange of exercise-related materials and information with any individual or organization that was not approved for T3 play was prohibited.

Organizations playing at the CPX or FSE level were required to designate an organizational point of contact to interface with the T3 exercise team. This individual functioned before the exercise as an exercise planner and attended the one-day field controller and data collector training program. During play, this individual functioned as a field controller/data collector and ensured that the organization followed the rules for information exchange and stayed within the prescribed boundaries of the exercise. Rather than identifying an individual to serve as a pre-exercise planner and field controller/data collector, an private-sector participant playing at the

CPX or FSE level could rely on an overarching organization[8] and physically co-locate at the overarching organization's command post or EOC during the exercise. The overarching organization was responsible to ensure that all co-located private-sector participants followed the information exchange rules and did not violate the exercise's boundaries.

C. Flexible Hours of Private Sector Play

In addition to multiple modes of play, T3 private-sector integration offered participants flexible hours of play to accommodate the amount of time and number of personnel each organization could make available for the exercise. The PSWG scheduled official hours for private-sector play, but private-sector planners and players determined the best hours of play for themselves and their organizations.

The official hours of play for private-sector players in the FSE were chosen to permit the players to allocate their time efficiently to correspond with the major private-sector-related events in the exercise scenario. These hours were:

April 4 (Monday)	12:00–20:00	STARTEX (NICC Alert Sent via ENS at 15:08)
April 5 (Tuesday)	08:00–16:00	
April 6 (Wednesday)	07:30–16:00	
April 7 (Thursday)	08:00–14:00	ENDEX for NICC Private Sector Cell, NICC Hotwash 14:30–16:00
April 7 (Thursday)	08:00–11:30	ENDEX for Other Private Sector Participants

All private-sector participants were informed of the official hours of private-sector play. But because most private-sector participants did not play during this entire range of hours, all private-sector controllers in the T3 Master Control Cell and the Connecticut and New Jersey Venue Control Cells were provided a play schedule for all private-sector participants.

Knowing in advance the approximate timing of the initial disclosures of the simulated terrorist attacks, the Exercise Planning Team informed private-sector participants to be ready to play sometime between 12:00 and 15:00 on the first day of the FSE.[9] Pre-exercise documentation and other communications emphasized that, if private-sector participants failed to receive notification, those who wanted to play from the beginning of the private-sector-related events should arrive at their play locations by no later than 15:00.[10]

[8] Examples of overarching organizations that acted in this role in the State venues during T3 include ASIS International and the Fairfield County Business Council in Connecticut and the New Jersey Business Force in New Jersey. The DHS/ICD National Infrastructure Coordinating Center and the FEMA NRCC acted in this role in the National venue.

[9] On the first day of the exercise, April 4, 2005, VNN made its first report of plague (type unspecified) at 11:50. VNN made its first report of the explosion at the New London City pier in Connecticut about an hour and a half later at 13:30.

[10] The actual alert to the private sector of the simulated events was sent by the NICC via the Emergency Notification System at 15:08 on April 4, 2005.

Play ended for all private-sector participants other than those playing at or through (i.e., virtually) the NICC Private Sector Cell at approximately 11:30 on Thursday, April 7. End of play for the NICC Private Sector Cell was the same day at 14:30. An NICC Private Sector Cell Hotwash followed immediately afterwards. Private-sector T3 players attended the Hotwash physically and via teleconference.

D. Prototype Positions for Private Sector Coordination

During the exercise, three new positions were created and played to facilitate private-sector coordination with FSL incident management. A Private Sector Liaison position was created and played in the Connecticut EOC and a Private Sector Liaison Cell in the New Jersey EOC. A Private Sector Cell was established in the NICC.

These positions do not actually exist yet. They were prototyped in part to facilitate the T3 private-sector integration objective of improving public-private information sharing processes and capabilities and with the intention of institutionalizing them after the exercise.

As artificialities, these mechanisms provided private-sector players the opportunity for increased intra-sector coordination, particularly at the national level. As a result of being physically or virtually located at the NICC, private-sector representatives were able to gain a better understanding of the actual operations of the national mechanisms and procedures for coordinating and communicating with the private sector.

Without these prototypes, there would have been less understanding and greater confusion among the private sector about overall situational awareness, including each agency's incident management and emergency response responsibilities. In addition, much of the cross-sectoral coordination and communication during T3 occurred at or through the NICC Private Sector Cell. Without this cross-sectoral coordination and communication, there would have been far less interaction between critical infrastructure representatives and FSL government representatives.

E. Minimal Testing of Unsolicited, Unmanaged Volunteers and Donations

In response to real events of the magnitude of T3, the public has a history of providing large numbers of volunteers and quantities of donations that incident management officials have not solicited, do not have the resources or authority to manage, and often find do not meet the real needs in the field. The 9/11 terrorist attacks are just one real-world example in which the number and magnitude of unsolicited, unmanaged volunteers and donations substantially interfered with critical response and recovery activities.

In T3, such unsolicited and unmanaged volunteers and donations did not appear even notionally, much less actually. The exercise was designed to have private-sector players from faith-based organizations act as role players and place dozens of telephone calls to FEMA/Volunteer Organizations Active in Disasters (VOAD) to offer substantial numbers of unsolicited volunteers and donations. But, in order to avoid overwhelming the resources of FEMA/VOAD that were available for the exercise, the play of these faith-based organizations was terminated on the

exercise's second day. Thus, the FSL incident management teams did not have to face the volunteer and donations management problems that a real-world event would have produced.

F. Multi-State Effects on Private Sector

Multi-state effects on the private sector were largely absent in T3. As a result of real incidents of this magnitude, the effects propagating to states other than Connecticut and New Jersey would have had a profound impact on the private sector.

For example, it is unrealistic to assume that other states or the Federal government would have allowed unrestricted travel by members of the trucking industry and the public who had recently been present in New Jersey. Distribution centers and warehouses would have been likely to refuse shipments that originated in New Jersey. Those that had accepted such shipments before the plague attack was discovered would be in crisis mode attempting to determine whether they were infected or clean, as well as whether they could continue to ship and receive goods. The results would have included cascading delays in supply chains and possibly severe shortages of key resources.

Airline passengers who had recently been in New Jersey also would have been subjected to some type of official procedures to determine whether they posed a threat to the health of others. It is probable that this would have had a significant effect on the operations of the airline industry, and possibly a negative economic effect as well.

Similarly, the arrangements private-sector representatives in the transportation sector made with New Jersey officials to transport key resources and other goods into New Jersey after the travel restrictions were imposed relied on neighboring states, including Pennsylvania and Delaware, for staging. But those states were not playing in T3. All decisions and cooperation by these neighboring states' officials had to be assumed or simulated. Thus, it cannot be concluded that these public-private arrangements forged to adapt to the travel restrictions would have been possible in a real incident.

G. Lack of Real-World Demand for Key Resources

During the exercise, the public did not demand food and other basic necessities when shortages of these key resources occurred or were threatened. The exercise's lack of real-world demand pressure for these key resources is a significant artificiality.

The transportation sector and food sector players in the NICC Private Sector Cell reported that they had a difficult, but manageable, arrangement for transporting food and other key resources into the affected areas in New Jersey before the travel restrictions. After the restrictions were imposed, this arrangement was no longer workable and private-sector players scrambled to fashion an alternative. But the food warehousing, distribution, and retailing systems in a state typically contain just a few days' worth of food under normal demand conditions. Private-sector members of the food sector in New Jersey estimated during T3 that – when purchasing patterns are normal – approximately 1-2 day's of perishable food inventory and 6-8 days' of non-

perishable food inventory is present within the overall system at any given time. Although the "just-in-time" supply system is flexible and responsive to market forces under normal conditions, it is fragile and difficult to restore when shut off or severely disrupted, even for short periods. And public confidence in the ahility of the supply chain to deliver key resources may he one of its most vulnerable links.

It was not possible to simulate the real-world demand for food and other key resources, and the cascading effects of potential shortages could not be fully calculated. However, private-sector representatives of the food sector in New Jersey played the supply chain disruptions and consequences out notionally and concluded that the food shortages would be significant enough to engender civil unrest. The extent of damage from this civil unrest would cause the food industry in New Jersey to still he in the recovery mode at least 30 days after the end of the exercise.

H. Lack of Real-World Stresses on Specific Critical Infrastructure Sectors

Some critical infrastructure sectors were not stressed to the extent and degree they would have been had the T3 attacks been real events. As one example, a private-sector participant representing the electricity sector noted that the sector was tested only lightly and would have undergone far greater stresses had the scenario played out heyond the scheduled four days.

The telecommunications sector in particular was subjected to a noteworthy lack of significant stresses during T3. As one participant at the NICC Private Sector Cell noted, telecommunications facilities across the board were expected to and (notionally) remained fully operational and underutilized for the entire exercise. But even real-world events that are far more localized and result in far fewer casualties than the simulated T3 events cause significant stress and over-utilization of telecommunications facilities.[11] Thus, any overall assessment of the ability of the nation's critical infrastructure to weather a real-world attack similar to the simulated T3 attack must take into account the exercise's designed-in lack of stress on telecommunications systems and facilities.

Similarly, the play of the financial sector was, by design, confined within a CLX. This CLX reported that it successfully tested its critical ringdown system, which ensures that key representatives of the financial sector can contact and share information with each other during an emergency. But little financial information from that closed loop was communicated to or played within the rest of the T3 exercise. Therefore, there is little to be gleaned from T3 regarding the effects of events of this nature on the strength of the financial sector and the national economy.

[11] (See *London rocked by explosions*, CNN.com, July 7, 2005 (available at http://www.cnn.com/2005/WORLD/europe/07/07/london.tube/index.html).)

V. Exercise Observations

This section describes observations of issues that arose that involved the private sector and were not expected before the exercise. The observations were derived from the private-sector secure messages, the venue chat logs, and NICC data collector logs. The three main observations were:

- FEMA/VOAD chose not to exercise the NRP Volunteer and Donations Management Annex;
- surprisingly little official information flowed from FSL government to the private sector; and
- only a few days' worth of reserves exist in the supply chain for key resources such as food and hospital supplies.

On the second day of the FSE, a conference call took place between four faith-based organizations and the American Red Cross (ARC), VOAD, and FEMA. At that time, the faith-based organizations offered both volunteers and donations. The support was turned down. Volunteers and/or donations would be solicited through the partner organizations already in place on the local or statewide level. The faith-based organizations were told to contact their local chapter of the ARC which would draw on its constituency if needed. Due to the refusal of unsolicited volunteers and donations, the coordination mechanisms defined in the Volunteer and Donations Management Annex of the NRP were not able to be exercised.

Throughout the FSE, FSL governments made decisions that affected the private sector, but were not communicated to the private sector. The decision to raise the threat condition to Red in New Jersey and the protective measures to be taken under that condition were areas in which the private sector did not receive official information from the public sector. During the New Jersey government discussions on the lifting of travel restrictions, a decision was made to open one lane on the highway to allow for the movement of supplies. At least one large shipping firm was not told of the access lane until well after the government had opened it. If it had been involved in the decision-making process, the firm could have scheduled and positioned its assets to make efficient use of the limited travel access. Also, the private sector was never informed of recommended protective measures that were developed by DHS.

The scenario in New Jersey and Connecticut demonstrated the scarcity of reserves of food and medical supplies that would be essential in a real-world incident. Not long after the plague began to spread in New Jersey, hospitals experienced critical shortages of supplies such as masks, gloves, and IV fluids. As New Jersey was put under threat condition Red and travel restrictions were put in place, the food sector was severely hampered. Most retail food stores and distribution centers only have a few days worth of supplies on hand and food shipments were stopped at the border. In Connecticut, a shelter-in-place order was given hy the Governor for an area surrounding New London. If the shelter-in-place order had lasted for just two or three days, companies subject to the order who were sheltering their employees would have run out of food.

VI. Key Issues

This section addresses significant issues identified during the planning and execution of T3 private-sector integration. These issues are derived from private-sector participants' observations and feedback contained in comments and documents from Hotwashes and After Action Conferences and in numerous other feedback sources. The issues grouped into six broad categories:

- Prototype Private Sector Coordination Mechanisms
- Public-Private Coordination and Communication
- Testing Internal Emergency Response and Business Continuity Plans
- Cross-Sector Coordination and Communication
- Private Sector Planning
- NRP Volunteer and Donations Management Support Annex

A. Prototype Private Sector Coordinating Mechanisms

The effectiveness of three private-sector coordinating mechanisms prototyped during the exercise —the Connecticut Private Sector Liaison position, the New Jersey Private Sector Liaison Cell, and the NICC Private Sector Cell—led private-sector players to request that they be institutionalized for real-world incidents. The Private Sector Liaison in the Connecticut EOC provided briefings and updates three times a day during the FSE. Electronic bulletins were broadcast to every registered e-mail address, pager, and cellular telephone notifying private-sector participants of an upcoming situational awareness briefing, which was then broadcast to all registered cellular telephones. After the situational awareness briefing, registered private-sector players had the opportunity to engage in a question-and-answer session with representatives of the Connecticut EOC. On average, approximately 20 of the 26 private-sector organizations playing in the Connecticut venue participated in each of these question-and-answer sessions during the exercise.

The Private Sector Liaison Desk at the New Jersey Office of Emergency Management (OEM) handled "hot issues" from companies in New Jersey and passed along questions to the appropriate Infrastructure Advisory Committee chair. The Private Sector Liaison served as a single, centralized point of contact in the State government for representatives of critical infrastructure sectors and industry, making it easier for the private sector to determine who they needed to contact with their problems, requests, and offers of assistance.

The Private Sector Cell at the NICC integrated the DHS specialists with their counterparts representing each critical infrastructure sector. Participants also included private sector players representing other industries and sectors who were playing at the National (as opposed to the State) level. Other than NICC staff, Table 2 lists the number of participants in the NICC Private Sector Cell.

Table C-2. Participants in NICC Private Sector Cell

Personnel Category	Number of Participants
Critical Infrastructure/Key Resource Group	141
DHS Private Sector Office (PSO) Group	47
PCII Group	6
Observers	12
T3 Controllers and Data Collectors	12
T3 Exercise Support Team	6

The Critical Infrastructure/Key Resource Group in the Private-Sector Cell was composed of private-sector representatives of the nation's CI/KR sectors, representatives of the Information Sharing and Analysis Centers (ISACs), and sector specialists from the DHS Infrastructure Coordination and Analysis Office (ICAO). The DHS Private Sector Office (PSO) Group included private-sector participants not directly representing a CI/KR sector as well as members of the DHS PSO.

The NICC provided two briefings each day, including via secure teleconferencing and presentation facilities to those participating in the Private Sector Cell virtually. Private-sector players reported that physical or virtual participation in the Private Sector Cell facilitated effective coordination within and, with some exceptions, between sectors. Participants also reported that they gained a better understanding of the Federal government's actual operations during an INS.

B. Public-Private Coordination and Communication

Issues surrounding coordination and communication between the government and the private sector dominated the comments and feedback from the private-sector players. The issues fall into three categories:

- Lines of Communication
- Method of Communication
- Coordination

C. Lines of Communication

For many private-sector participants, T3 illuminated the official links for coordinating and communicating with FSL government, and highlighted some the weaknesses in those links. Private-sector participants frequently mentioned in their feedback that the exercise enabled them to gain a better, more realistic picture of what information and resources would be available from FSL government during a real-world response to a WMD terrorist attack. They learned what steps the private sector would have to take to coordinate effectively with the government to obtain this information and these resources.

Private-sector participants were surprised by the lack of information coming to them during the execution of the exercise from official channels in FSL government. For the private-sector players in the National venue, this surprise centered on communications from the top down, starting from the White House to the DHS Secretary, the IIMG, and ultimately to the DHS sector specialists and their private-sector counterparts. Notwithstanding the benefits provided by co-locating the Private Sector Cell prototype at the NICC, participants concluded that the information they received back from the IIMG, the NICC, and other Federal organizations was slow and of insufficient quality. For example, at the end of the first day of the FSE, private-sector players were concerned by and had received little information explaining why transportation was not "locked down tight" to contain the plague. Furthermore, the lines of communication and authority between the NICC, the IIMG, and other organizations were unclear to the private sector.

1. Methods of Communication

One of the primary methods by which the private sector and the Federal government communicated during the exercise was through the request for information (RFI) process. But private-sector participants found the process confusing and inefficient. The process for responding to RFIs received by private-sector players via the NICC was not well-defined or well-communicated. Private-sector players in the NICC Private Sector Cell reported that they spent too much time on RFIs as a whole and that the time they spent on each one was not used efficiently because the RFIs they received were not prioritized. They further commented that they should have received feedback to the responses; this would have enabled them to assess the appropriateness of and priority given to the information they provided.

Private-sector participants repeatedly asked that when they send out an RFI, they receive a timely response, even if the response is nothing more than the status of their request. For example, the Real Estate ISAC had to request information on the cancellation of sporting and convention events multiple times on multiple days before the commercial facilities sector received relevant information from the NICC. To permit timely responses, the RFI process needed to he clarified so that the information necessary to the private sector is managed by appropriate Federal personnel who can distribute it to Federal coordination mechanisms to be acted upon and shared with the private sector

A second method through which the public and private sectors communicated was through e-mails. However, many private-sector participants had problems with the e-mail system provided. Many players were not able to keep up with incoming e-mail pertaining to the exercise. Also, most e-mails were not clear as to who the message was supposed to go to, who was supposed to respond to the e-mail, and whether or not it was a question or a statement. In order to remedy that situation, the private-sector participants requested more dedicated phone lines, cell phones, and modes, other than e-mail, for private sector office officials to be reached in emergency situations.

Participating private sector organizations emphasized that they have the ability, capacity, and redundant systems necessary to pass information quickly and efficiently to their sectors,

industries, nationwide locations, and workforces. In the absence of timely information from public officials, the private sector turns to other sources, sometimes resulting in decisions that do not match the actual situation. For example, at the time when representatives of the transportation/rail sector responded to an RFI, they had not received the information that New Jersey was raising its threat advisory level to Red. If the railroad sector had known about the raise in threat level, their response to the RFI may have been different. If the private sector does not receive credible and reliable information from official sources, businesses and industries go ahead and adjust the supply chain according to their own continuity plans or in response to perceived threats based upon unofficial, back-door communication links.

2. Public-Private Coordination

Critical decision making by the government in the midst of a crisis can have significant unintended consequences if not fully coordinated with the private sector in advance. Throughout the exercise, there was a widespread lack of knowledge of the protocols involved and the appropriate private-sector responses to a decision hy a State government or hy DHS to raise the threat advisory to the Red level. For many private-sector participants, the greatest challenges faced during the exercise were a result of the State of New Jersey declaring Red and imposing travel restrictions, both with little or no advance coordination with the private sector. Emergency travel restrictions seriously limited the movement of critical employees and supplies within the private-sector workforce. When the discussions regarding the lifting of such restrictions take place, the private sector should be involved. The private sector requested clarification of and involvement in the decision-making process for raising and lowering threat advisory levels.

The private sector would also like to improve the coordination during response and recovery efforts of private-sector assets. The private sector has an array of assets at its disposal: facilities, materials, supplies, vehicles, and even aircraft. When governmental response resources are stretched or stressed, the private sector could provide assistance. DHS, as well as State OEMs, must know in advance who within the private sector owns or controls which assets. Pre-coordinating these assets would enhance preparedness and facilitate a more effective response within each state.

The DHS PCII Program was developed to enhance public-private coordination and information sharing. This program enables members of the private sector to voluntarily submit to the Federal government sensitive information regarding the nation's critical infrastructure with assurances and safeguards protecting the information from public disclosure. Testing the PCII Program was one of DHS's express objectives for T3 private-sector integration. The NICC established a PCII Coordination Cell for the exercise to handle and expedite PCII protections for critical infrastructure information submitted by the private-sector participants.

The data show that some testing of the PCII Program took place during the exercise, including PCII approval of information submitted by the chemical sector and subsequent use of that information by the Transportation Security Administration (TSA). It was also noted that the TSA sought to share this information with a State EOC until a PCII representative explained that the PCII Program has not yet approved states to receive such information. But the data on the whole

suggest that the PCII Program was tested only lightly and are insufficient to support any conclusions about the program's effectiveness or efficiency during disaster response operations.

D. Testing Internal Emergency Response and Business Continuity Plans

T3 raised the level of awareness of many private-sector organizations' employees regarding the critical roles that their business functions and emergency response plans play during an event. The exercise illustrated to private and public sector players that cascading effects of absenteeism, especially of critical employees, can shut down organizations and sub-sectors. Private-sector organizations must be able to get critical employees to work to maintain continuity of operations. A large percentage of the huge (notional) financial losses in the New Jersey chemical sector (estimated at $557 million during the first week of the FSE alone) was caused by absentee-related plant closures or slowdowns. Even an automated operation requires critical employees to enter areas affected by events when vital systems go down. But during the FSE, a lurking, unresolved question arose about the definition of a critical employee and whether the criteria applied by law enforcement will match the private sector's definition. It is unclear whether the necessary training and coordination has been undertaken to enable law enforcement personnel to recognize specially marked company vehicles.

T3 also provided a useful, realistic opportunity for private-sector organizations to test their emergency response and business continuity plans. With some exceptions, a large majority of responding private-sector organizations reported that the realism and richness of the FSE scenario and events permitted them to gain a better understanding of the strengths and weaknesses of their plans. The commercial facilities sector reported that large disparities continue to exist in the sector's response capabilities and emergency plans, which range from excellent to non-existent. Some facilities' management plans to automatically self-evacuate during an event, and there is no industry standard response to a shelter-in-place instruction by a State. For this purpose, the private-sector participants sought improved information and coordination on appropriate private-sector protocols and responses to heightened Federal and State threat alert levels.

Several companies said that they would consider volunteering their facilities to be Points of Dispensing (PODs) under the Strategic National Stockpile program. Many private-sector participants felt that hosting a POD would be part of their business continuity planning. Community Emergency Response Team training for company volunteers would be necessary to enable private-sector organizations to fulfill this commitment.

E. Cross-Sectoral Coordination and Communication

T3 provided many examples demonstrating that coordination and communication between various sub-sectors of the private sector are both indispensable and often insufficient to respond effectively and efficiently to an event of this magnitude. Private-sector organizations themselves gained a greater awareness of the extent of critical infrastructure interdependencies, and the NICC Private Sector Cell provided many opportunities for and examples of positive, effective cross-sector communication and coordination. The food and agriculture sectors and the

transportation sectors engaged each other and many other sectors in decision making and information gathering, which had important effects on the movements of key resources during the FSE. Representatives of the private-sector players in the NICC Private Sector Cell repeatedly organized and coordinated cross-sectoral lines of communication.

In many cases, participating private-sector groups did not know what decisions were being made in other sectors and by whom they were being made. They reported that their knowledge, or their lack of knowledge, of those decisions would have significant impacts across sectors in a real-world event. It was noted that in real time, a useful display of critical information could be presented at the NICC Coordination Center Cell, which would include a summary of the current situation, a timeline of events, and the time and substance of major governmental decisions that have been made. Several private-sector participants expressed support for the creation of a private sector analog to the IIMG, which would, in their view, improve cross-sector integration for planning and evaluation.

F. Private Sector Integration Planning and Training

A large majority of the private-sector organizations that provided feedback stated that the exercise was thoroughly and professionally planned in a manner that allowed them to participate effectively and realistically in the event scenario and response and recovery efforts. A few commented that the involvement of private-sector participants in the planning process was insufficient and did not enable them to exert sufficient influence on the design of the exercise to ensure meaningful, realistic play for their organizations. Some private-sector participants also felt that they would have benefited from additional or more in-depth training. A key observation was that those who represent the private sector in exercises must be SMEs who are well-versed in each subject matter and sector for which they are responsible. In addition, those representing the private sector during actual events must have substantial exercise and/or real-world disaster response and recovery experience.

Private-sector participants commented on the need for greater private-sector input into the National Infrastructure Protection Plan and the NRP. The private-sector integration in these plans needs to be more robust, and this requires substantial private-sector assistance.

G. Volunteer and Donation Management Support Annex

Little actual testing of the NRP Volunteer and Donations Management Support Annex was conducted during T3. Faith-based organizations who had been trained to execute injects by simulating members of the public telephoning VOAD to offer unsolicited volunteers and donations were requested by agency-affiliated players to stop participating on Day 2 of the FSE. Protocols were apparently not in place for handling VOAD-type donations and volunteers. The decision was made to suspend this play because the telephone call injects would have flooded the local VOAD centers. It was stressed that the volunteer and donations management function was unprepared to handle the influx of calls and donations that could potentially come in during a real-world crisis. The lesson learned was that VOAD is not yet prepared for massive offers of voluntary assistance and donations at the local or national levels. Additional testing and

emergency response operations development is necessary for the volunteer and donations management system to be prepared to handle a 9/11-style outpouring of volunteers and donations in a future exercise or real-world event.

Faith-based organizations' participation in T3, particularly in the planning stages, did provide them experience in coordinating with the Federal government for disaster response efforts. A leader of one of the faith-based emergency management organizations stated immediately after faith-based play was shut down that their involvement in T3 led his local VOAD director to offer to meet with him after the exercise to share lessons learned, as well as how faith-based organizations can be a part of that VOAD district's working emergency response plan.

VII. Conclusions

Exercise play in T3 provided an unprecedented range and number of private-sector organizations an opportunity to exercise their coordination and communication with FSL government in response to a domestic WMD terrorism attack. The scope and magnitude of private-sector participation in T3 were far greater than in T2. A significant majority of the private-sector participants who provided feedback agreed that the planning and execution of T3 private-sector integration was effective and facilitated robust play by their organizations. They further reported that T3 enabled them to test their emergency response and business continuity plans in an effective, realistic manner. Numerous organizations are improving these internal plans as a result of the exercise.

Private-sector participants also reported good coordination and communication within their own sectors and with their sector's DHS sector specialists. Much of this was facilitated by the prototype Private Sector Liaison mechanisms in Connecticut and New Jersey and the prototype Private Sector Cell in the NICC. There is a broad consensus among private-sector participants that these mechanisms should be institutionalized for operation during real-world events.

But T3 also demonstrated that real-world integration of the private sector into FSL government disaster response and recovery efforts is still in or near its infancy. Official government sources provided private-sector participants little of the information they needed to make sound, informed decisions. Private-sector participants perceived themselves to have been omitted from the decision-making processes on critical issues affecting their interests, as well as their ability to respond to the attacks. Private-sector participants deemed the lack of communication and coordination with official government sources to be particularly inadequate regarding travel restrictions, threat advisory level changes, and the availability and priority of necessary prophylaxis measures. Little or no advance private-sector coordination was provided before these decisions were announced. Once made, these decisions' specific objectives and recommended responses were not effectively communicated to the private sector. As a result, private-sector participants were left to rely on their own sources of information[12] and their own criteria for

[12] Often that meant only Virtual News Network (VNN), a simulated cable news network that broadcasted information about exercise-related events to T3 players via secure satellite downlink, and VNN.com, a simulated Internet-based news service available to T3 players via a secure Web site.

deciding how to protect their employees, keep critical employees on the job, and continue to provide services and resources essential to effective public-private response operations. Also, despite private-sector representatives' efforts to provide effective responses to governmental RFIs, FSL government entities reported that the roles, responsibilities, and resources that private-sector organizations offer in a disaster response operation remain unclear.

Some cross-sectoral coordination occurred during the exercise, particularly through the operation of the prototype private-sector coordination mechanisms in Connecticut and New Jersey and at the NICC. But, most private-sector participants reported that cross-sector coordination and communication was inadequate to mount an optimal response to attacks of the magnitude simulated in T3.

Two key testing objectives for private-sector integration were not realized in T3: testing the NRP's Volunteer and Donations Management Support Annex and testing the PCII Program. Little attempt was made to respond to the telephone calls that were planned as exercise injects from role players from faith-based organizations who offered unsolicited volunteers and donations. The only reported result is that the faith-based players have a greater understanding of how to interact with the Federal government for disaster response and recovery. Similarly, given the lack of exercise data involving the PCII Program, no conclusions regarding its efficacy can be drawn from T3.

Annex D: Cyber Exercise in Connecticut

I. Summary

While the principal focus of the Top Officals (TOPOFF) exercises continues to be incident management, there is another element of our country's critical infrastructure that experts consider highly vulnerable to a terrorist-related attack: the national information infrastructure. TOPOFF 3 (T3) is the second Top Officials exercise to include a limited cyber component.

The Connecticut T3 Cyber Exercise was conducted on a not-to-interfere basis with the T3 Full-Scale Exercise. It took place March 22–23, 2005, at the Connecticut Department of Information Technology headquarters in East Hartford, Connecticut. There were approximately 80 participants including top officials and network operation centers (NOCs) from the Connecticut State Department of Information Technology, the Connecticut Department of Transportation, the Connecticut State Police, the Connecticut Education Network, and the city of New Haven.

The major objectives of the exercise were to:

- develop state and organizational information technology (IT) cyber security policies and procedures;
- determine policy effectiveness related to large-scale cyber attacks;
- develop strategies and planning frameworks to coordinate inter-governmental response and consequence management to cyber attacks;
- maintain continuity of operations during a cyber attack;
- develop recommendations for senior decision makers responding to potential cyber crisis events; and
- to explore the government and private sector role in maintaining public confidence during and after a large-scale cyber attack.

The exercise encompassed three cyber attack scenarios, each associated with different aspects of the cyber security problem. The intensity of the cyber attacks increased with each scenario, culminating in a final attack targeting specific networked entities within crisis or consequence management roles.

The NOCs used a simulated network developed by the Institute for Security Technology Studies (ISTS) as the primary source of exercise-related stimuli. The network replicated elements of regional, wide-area networks and an inter-governmental network.

After the exercise, participants highlighted the following key issues for consideration:

- a need for documentation of new technologies plans, policies, and procedures;
- development of plans and procedures associated with Homeland Security Advisory System (HSAS) levels;
- a need to identify network organizations and their functions;
- the importance of radio communications and non-voice over Internet protocol (VoIP);

- uniform government wide-area networks (WANs) policies; and
- remote access network control applications.

Participating top officials and NOCs felt that the Connecticut T3 Cyber Exercise was an excellent training tool and guide for current and future development of various information systems.

II. Introduction

The media frequently reports government officials' concerns over terrorist plans to conduct internet-based cyber attacks. These news stories often recycle theoretical scenarios attributed to foreign government information warfare capabilities. But, terrorist organizations, such as the TOPOFF 3 universal adversary, may also use cyber attacks to disrupt emergency services as a means to reinforce and multiply the effect of a physical attack. The Connecticut T3 Cyber Exercise examined the integration of inter- and intra-governmental actions related to a large-scale cyber attack on a major urban area of the United States. The attack was synchronized with a terrorist weapons of mass destruction (WMD) attack.

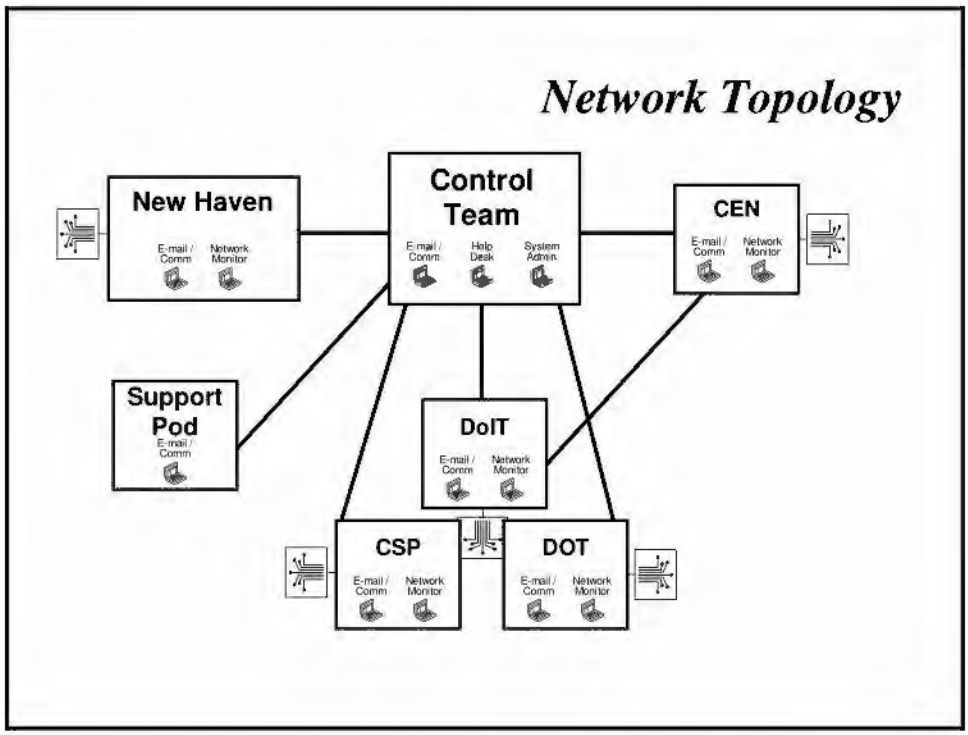
III. Background

The impact of cyber terrorism, both as an attack medium and as a means to disrupt crisis or consequence management, was highlighted as a shortfall of TOPOFF 2000. Accordingly, in T2, a cyber excursion was conducted to introduce the synergies associated with a blended terrorist attack. In planning T3, it was understood that incident management exercise including WMD and cyber attack elements might be counterproductive to the T3 objectives. Thus, the New Jersey and Connecticut state venues each held an isolated cyber exercise preceding the full-scale exercise.

IV. Exercise Design and Artificialities

During the exercise, players were divided into five NOCs and one support group (see Figure 1). Over a period of two days, players worked through three cyber attack scenarios. To support the development of these scenarios, the exercise design team used an outline of the attacker's (a generic "Red") aims, means, and methodologies.

Figure D-1. Network Topology



A simulated network, developed by ISTS, was utilized during the exercise. It served as the primary source for stimulating events and actions in the exercise. Regional, wide-area networks (e.g., the public access to governmental organizations) and an inter-governmental network (i.e., a private intranet used within the state) were replicated for use in the simulated network. Network status display console operators were briefed on how to use the simulated network before interactive play began.

During each scenario, the teams (groups) responded to the data provided on the exercise simulated network, or through other means. They addressed plans, policies, and procedures, as well as many management or technical issues. Although incident management and cyber security plans provided a foundation for the participants' actions and decisions, they were not constrained by these plans or other current, real-world plans and management concepts. The exercise was self-assessed and evaluation criteria were determined by each of the participating organizations.

Scenario 1, *Disjointed Attacks*, featured an "above normal" level of network disruptions. Players were asked to revalidate assumptions, upon which their incident response plans were founded, and to identify other suppositions. They also reviewed both the internal and external communication flows of their NOCs and discussed relevant cyber security issues. Players then identified and prioritized the implications of prolonged periods of "above normal" network disruptions. Finally, they examined the impacts on planned processes, courses of action, and resource requirements detailed in their response or disaster recovery plans.

Scenario 2, *Coordinated Attack*, was a low-level, coordinated cyber attack against stakeholder organizations. Players addressed response issues related to this particular attack. In addition,

players acknowledged the actions necessary to respond to these attacks in a combined manner and resume network operations.

Scenario 3, *WMD Force Multiplier*, was an overwhelming, coordinated cyber attack acting as a "force multiplier" for a combined terrorist WMD attack. NOCs addressed the necessary actions to re-establish or maintain network operations to permit crisis and consequence management.

V. Exercise Observations

Using their incident response plans, policies, and/or procedures, players reacted to the stimuli generated during these scenarios. Players then analyzed their reactions and evaluated the stimuli that were used in the scenario. The Control Team observed a general lack of communication within and between organizations. There often was a lack of written policies and procedures that could be used as guidance to their responses. A heavy focus on the reaction of the players was recorded. It was also noted that participants had limited communication with the Federal government.

One of the many challenges facing most IT security programs is the relative newness of their supporting technologies and programs. As a result, many existing plans, policies, and procedures have not been documented. This exercise revealed the need to examine and record "who does what when" during both normal operations and accidental or malicious disruptions.

The exercise also highlighted a need for the exploration of appropriate plans and procedures to respond to changes in the HSAS threat conditions. The exercise begged the question: What proactive steps should be taken when the threat condition escalates from Yellow to Orange and then to Red?

During the cyber exercise, players learned that critical public health and safety functions exist on a network that some senior officials consider of secondary importance and may have a low restoration priority if network resources become limited. An important question to relate is: What organizations reside on a network and what functions do these organizations perform?

An over-reliance on digital information technologies may cause the loss of important functionalities should significant network disruptions occur. The exercise re-enforced the need to retain radio communications and VoIP telephone capabilities, particularly in organizations involved in public health and safety.

In complex, government WANs, especially if sub-networks spur from the WAN, uniform, consistent, and enforced polices are necessary to ensure network security and reliability. This exercise demonstrated that, without these policies, there is a potential for ineffective communication and coordination of WAN-wide problem resolution.

Nearly all governmental networked information systems require "on-location" personnel for their overall operation and upkeep. Should government workers or contractors not be able to access their systems for whatever reason (such as chemical or biological contamination), these networks may degrade gracefully or crash. The exercise confirmed that business continuity, continuity of

operations, and disaster recovery plans should include remote access to network control applications.

VI. Conclusions

The Connecticut T3 Cyber Exercise focused on the player's ability to respond to a large-scale cyber attack within the framework of a WMD event. It was an opportunity for participants to validate plans, policies, and procedures and refine their organization's roles and responsibilities. In addition, participating organizations uncovered potential weaknesses and areas for improvement. The players gained valuable experience working in a controlled environment with a diverse group of skill sets. Collectively, they recognized the need for improved external coordination and communication with other organizations in solving the key issues identified during this exercise. Players expressed the desire to formalize existing exercise and training outreach programs to build upon the lessons learned through this experience and share them with others in the cyber security field.

THIS PAGE INTENTIONALLY LEFT BLANK

Annex E: Cyber Exercise in New Jersey

I. Summary

The New Jersey Top Officials (TOPOFF) 3 (T3) Cyber Exercise, a one-day interactive tabletop exercise was conducted on March 30, 2005, at the Office of the Attorney General complex in Trenton, New Jersey. This exercise examined, in an operational context, the integration of inter- and intra-governmental actions related to a large-scale cyber attack, synchronized with a terrorist weapons of mass destruction (WMD) attack. The exercise was designed to examine disruptions to networks, responses, the consequences to those disruptions, and the implications for protective measures.

II. Introduction

State agencies and municipalities encounter increased challenges when trying to respond to a physical WMD event, while also responding to disruptions of government-related information networks. The cyber exercise was designed to address this mutifaceted challenge. Accordingly, within the context of a WMD event, consideration was given to the following:

- the effectiveness of the various cyber security policies, procedures, and practices of various departments and levels of government;
- the ability of participating network operations centers to integrate and effectively conduct or manage a sustained response to a cyber attack;
- the planned flow of communications and information in an operational response context; and
- the decision and coordination processes considering a range of potential consequences.

III. Backgrouud

The specific T3 New Jersey Cyber Exercise objectives are as follows:

- Examine information technology (IT) practices—including incident prevention, reporting, response, communications, containment, investigation, etc.—to effectively respond to the effects of a cyber attack.
- Gain an understanding of implications for policies, procedures, and practices resulting from a cyber attack, including issues related to:
    - internal coordination (State, local, and private sector);
    - Federal notification and response; and
    - other organizations.
- Refine a planning framework to:
    - enhance processes, policies/procedures, and training sufficiency;
    - maintain continuity of operations within participating organizations;

- develop alternatives and recommendations for senior decision makers responding to potential cyber crisis events; and
- sustain confidence in government information networks during an attack.

IV. Exercise Design and Artificialities

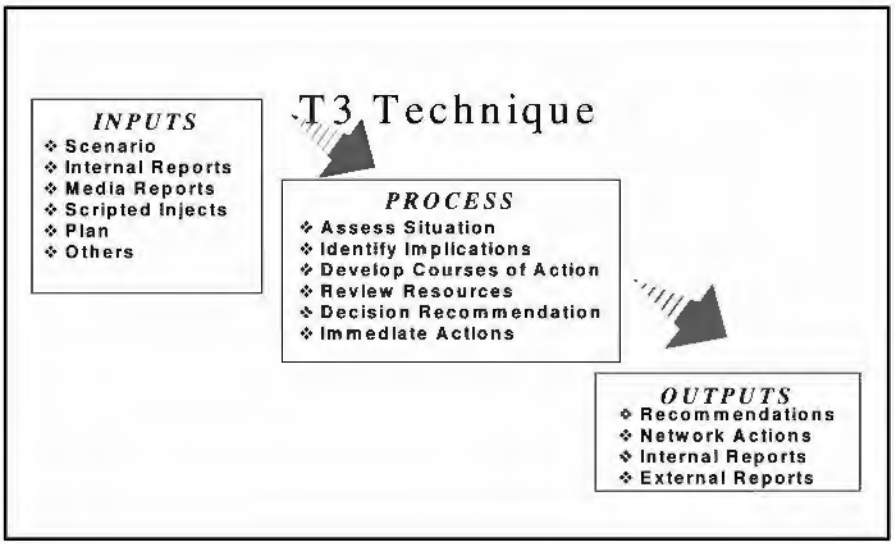
A. Scenario

The scenario included a simulated, coordinated Internet cyber attack from a terrorist cell or other associated groups. The T3 Cyber Exercise scenarios were considered in context of a range of threats from "script-kiddy" to state-sponsored, coordinated and uncoordinated attacks. At the beginning of the exercise, it was unclear to participants if the attacks were coordinated events or merely random intrusions. The purpose of the attack was not to take down the Internet, but to use the Internet to erode public confidence in the government, while, at the same time, disrupting the Federal, State, and local government's ability to provide for the health and safety of the public.

The overall technique employed within each interactive session was based upon the following paradigm: input ⇒ action ⇒ output. Using information provided by a scenario or scripted injects, participants responded to issues related to the specific theme of an exercise session and developed the products/actions required at the end of the sessions.

Figure 1 shows the general flow of this interactive technique.

Figure 1. T3 Exercise Technique



V. Concept of Exercise Activity

The exercise was an opportunity for participating organizations and individuals to:

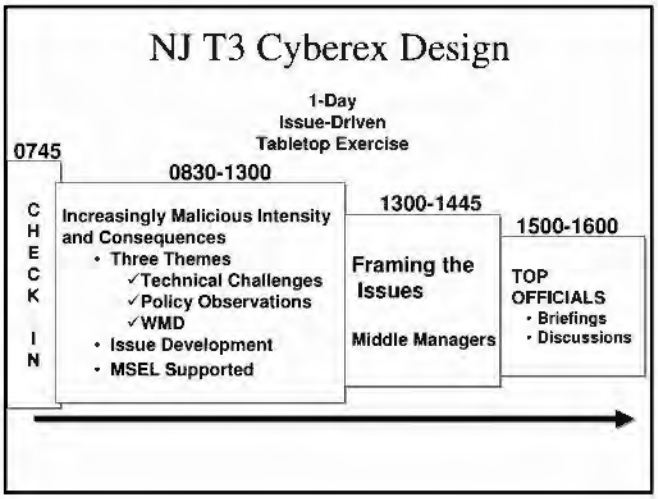
- examine policies, procedures, and practices;
- improve coordination and confidence;
- augment skills;
- refine roles and responsibilities;
- reveal weaknesses and resource gaps; and
- build teamwork.

As this exercise was self-assessed, evaluation criteria were determined by each of the participating organizations.

Although the incident management and cyber security plans in use by participating organizations provided a foundation for participants' actions, their decisions were not constrained by these plans and other current real-world plans and management concepts.

Figure 2 shows the broad design concept.

Figure 2. T3 Cyber Exercise Design

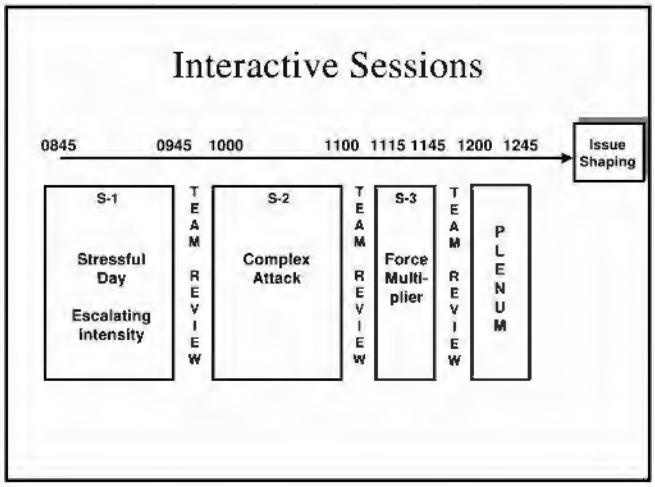


Multiple injects were used in three sessions of interactive play, each associated with different aspects of a cyber security problem (see Figure 3). These included:

- Session One: This session exercised a variety of communications paths and explored some complex policy questions. New Jersey and Hudson County incident response capabilities and practices were examined. Law enforcement issues were included in the prepared scenarios.

- Session Two: This session exercised the players' ability to correlate information to determine complex attack vectors. Participants examined their capability to identify remediation actions and potential unauthorized information exposure. Communications, law enforcement, and policy issues were included.
- Session Three: This session explored force multiplier effects and assessed their consequences. It included a major WMD event for state agencies and a power failure to key county facilities and networks.

Figure 3. Interactive Sessions



An executive-level seminar (see Figure 2) was conducted to examine policy issues and issues of common interest related to events that occurred during the three interactive sessions. Issues were framed and provided to an audience of "top officials."

VI. Participants

T3 players were primarily those Federal, State, and county representatives who have active roles in the daily operations, management, and security of information networks, systems, or infrastructure within their organizations. These participants played key roles in responding to and managing the consequences of the significant cyber disruption events presented in the scenario. The primary players in the exercise were the IT organizations of:

- New Jersey Department of Law and Public Safety, Office of the Attorney General
- Office of Information Technology
- New Jersey Department of Law and Public Safety, New Jersey State Police
- New Jersey State Department of Health and Senior Services
- New Jersey Department of Law and Public Safety, Office of Counterterrorism
- Hudson County

Supporting these players were representatives knowledgeable in the following disciplines:

- Commercial telecommunications providers, hardware and software vendors, and an Internet service provider (ISP)
- Federal computer incident response agencies
- Federal law enforcement agencies
- Information sharing and analysis centers

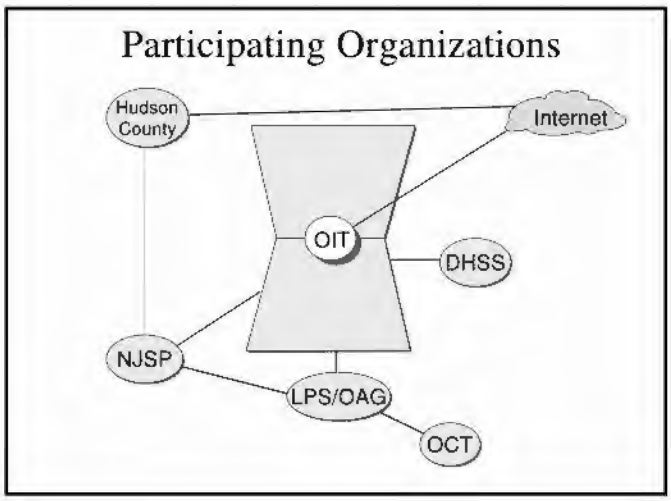
A. Top Officials

A group of top officials from Federal, State, and county government organizations participated in the New Jersey T3 Cyber Exercise. The top officials were composed of executives at the commissioner level in positions to consider appropriate options for policy resolution. These individuals acted as an executive body to address and resolve cyber security issues challenging the State and county participants.

VII. Exercise Organization/High-Level Network Topology

Figure 4 depicts the overall organizational topology for the New Jersey T3 Cyber Exercise. During the interactive sessions, participants were divided into different teams and tasked to address cyber security policies, procedures, and practices, and other management or technical issues. Six organizations (five State and Hudson County) participated as principal players in these interactive sessions.

Figure 4. Participating Agencies/Organizations



Each exercise entity was composed of individuals familiar with their agency or department's use of the cyber infrastructure. These entities responded to and managed the consequences embedded in each inject. Due to limited time, some elements were not addressed. Unresolved issues were brought forward in the final plenary session. The general responsibilities of each group included:

- assessing the situation and defining the problems presented;
- identifying the consequences of the problems and the impact of these consequences;
- describing the actions necessary to respond/mitigate these challenges; and
- determining the issues associated with these actions.

A. Control Team

A Control Team monitored all exercise activities and adjusted the process, as necessary, to support exercise objectives. The Control Team was responsibile for directing the exercise process, administration, and plenary sessions. Control Team members included co-facilitators, New Jersey exercise leads, recorders, and other selected individuals.

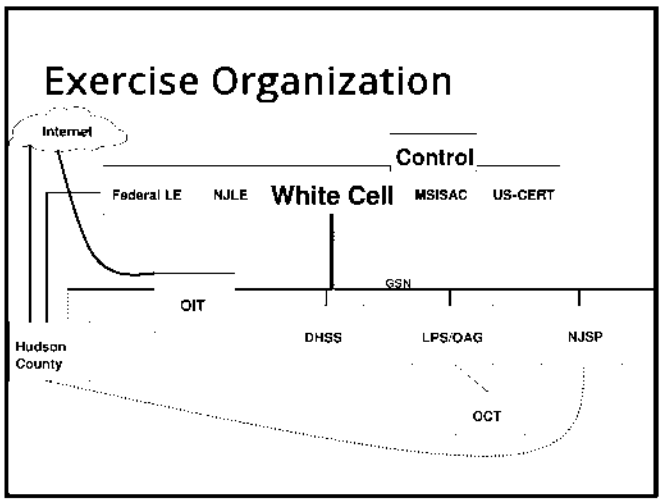
B. White Cell

A White Cell resided within the Control Team. White Cell members included Federal law enforcement, the Multistate-Information Sharing and Analysis Center, U.S. Computer Emergency Readiness Team, New Jersey State Prosecutors, New Jersey State Police (NJSP), NJSP Cyber Unit, NJSP Division of Criminal Justice, Regional Forensics Laboratory, and other entities that were integral to the conduct of exercise play. Participating organizations coordinated with other participating organizations or agencies as required by existing policies, procedures, and practices.

Communication was accomplished through a closed network e-mail system or face-to-face meetings. Teams documented each communications exchange between teams.

Figure 5 provides a notional layout of the exercise organization.

Figure 5. Exercise Organization



VIII. Artificialities

A. Network Operations

The cyber security element of T3 was conducted on a not-to-interfere basis with the principal full-scale exercise; therefore, no real-life networks were employed. Each team worked from a representation of their own network approximating actual network functionality and connectivity. This graphic depiction was provided to each team at the beginning of interactive play. Injects presented to players were tailored to their organizational network. Players interpreted the situation in relation to their respective network and responded accordingly.

B. White Cell

Coordination among organizations or agencies not directly represented was accomplished through interaction with the Control/White Cell.

IX. Exercise Observations

A. Key Issues

Overarching issues fell principally into the categories of "Policies, Procedures, and Practices," communications, and risk management.

The following issues were highlighted:

- A leadership mechanism should be developed to provide oversight of New Jersey State cyber security and continuity of operations.
- Policies and procedures should be distributed in writing to improve security and standardization of practices across the state (or country).
- A service agreement should be in place to define obligations and expectations of both the provider and users, even though the ISP resides within the broader state organization.
- A risk assessment should be conducted statewide on all IT-related capabilities.
- Federal organizations must mature their capability offerings to better meet user needs.
- ISPs, anti-virus vendors, and hardware manufacturers (servers and routers) offer potential to assist in developing responsive operational solutions to IT challenges.
- Best practice documentation in areas such as configuration management, acceptable use, and incident response should be created and distributed.
- A need exists for a recovery plan addressing the process, priorities, and any exceptions that may be required in the takedown of the entire state network.
- Situation awareness requirements should be clearly established in policies and procedures, and the thresholds for reporting must be defined.

- A statewide list serve and non-Internet-based notification system need to be established to inform state agencies and local government organizations of critical issues, incident response needs, critical alerts, etc.
- A clearly defined threshold for reporting criminal intent or behavior to law enforcement should be established and documented.

X. Conclusions

The New Jersey T3 Cyber Exercise focused on the player's ability to respond to a large-scale cyber attack within the framework of a WMD event. The players gained valuable experience by working in a controlled environment with a diverse group of skill sets. The players recognized the need for improved external coordination and communication and working with other organizations to solve the key issues identified during this exercise. Lessons learned emphasized a strong need for standardization, the lack of which allows weakness in areas that require strength and confindence in the event of a real-world incident.

Annex F: Acronym List

A

AAC	After-Action Conference
AAR	After-Action Report
ACF	Alternate Care Facility
ADLE	Advanced Distance Learning Exercise
AF	Air Force
AMEMB	American Embassy
AMHS	Automatic Message Handling System
AMOC	Air and Marine Operations Center
ARC	American Red Cross
ARF	Action Request Form
ASPHEP	Assistant Secretary for Public Health & Emergency Preparedness
ATV	All-Terrain Vehicle
AVOPS	Aviation Operations

B

BW	Biological Warfare

C

CBP	Custom and Border Patrol
CC	Control Cell
CDC	Centers for Disease Control and Prevention
CDO	Command Duty Officer
CDRS	Communicable Disease Reporting System
CDS	Communicable Disease Service
CERCLA	Comprehensive Environmental Response, Compensation, and Liability Act
CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity
CIP	Common Intelligence Picture
CIS	Catastrophic Incident Supplement
CLX	Closed Loop Exercise
CoC	Chief of Control

COCOM	Combatant Command
COE	Center of Excellence
COLISEUM	Community On-Line Intelligence System for End-Users and Managers
COMDIR	Communications Directory
COMMPLAN	Communications Plan
CONOPS	Concept of Operations
COO	Chief Operating Officer
COP	Common Operating Picture
COS	Chief of Station
COSIN	Control Staff Instructions
COTP	Captain of the Port
CPU	Computer Processing Unit
CPX	Command Post Exercise
CRI	City Readiness Initiative
CSG	Counter-Terrorism Security Group
CST	Civil Support Team
CT	Connecticut
CT	Counterterrorism
CTC	CIA Counterterrorism Center
CTD	FBI Counterterrorism Division
CW	Chemical Warfare
CWA	Chemical Warfare Agents

D

D/A	Department/Agency
DACC	Department and Agency Control Center
DAO	Defense Attaché Office
DCID	Director of Central Intelligence Directive
DCO	Defense Coordinating Officer
DDNI	Deputy Directors of National Intelligence
DNI	Director of National Intelligence
DEA	Drug Enforcement Agency
DEP	Department of Environmental Protection
DEST	Domestic Emergency Support Team

DHS	Department of Homeland Security
DHSS	Department of Health and Senior Services
DIA	Defense Intelligence Agency
DMAT	Disaster Medical Assistance Team
DMORT	Disaster Mortuary Operational Response Team
DPH	Department of Public Health
DPH ECC	Department of Public Health Emergency Coordination Center
DOC	Department of Corrections
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DTRA	Defense Threat Reduction Agency

E

EAS	Emergency Alert System
ECC	Emergency Control Cell
ECG	Exercise Control Group
EEI	Essential Elements of Information
EMS	Emergency Medical Services
EMSST	Enhanced Maritime Safety and Security Team
ENDEX	End of Exercise
EOC	Emergency Operations Center
EPA	Environmental Protection Agency
EPIC	El Paso Intelligence Center
EPR	Emergency Preparedness & Response
ERT	Emergency Response Team
ERT-A	Emergency Response Team – Advance Element
ESF	Emergency Support Function
ESP	Extranet Secure Portal
EVALPLAN	Evaluation Plan
EXCON	Exercise Control Cell
EXNMJIC	Exercise National Military Joint Intelligence Center
EXPLAN	Exercise Plan

F

FAA	Federal Aviation Administration
FAC	Family Assistance Center
FAMS	Federal Air Marshals Service
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information System
FCC	Federal Coordinating Center
FCO	Federal Coordinating Officer
FD	Fire Department
FDA	Federal Drug Administration
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
FOSC	Federal On-Scene Coordinator
~~FOUO~~	~~For Official Use Only~~
FRC	Federal Resource Coordinator
FSE	Full-Scale Exercise
FSL	Federal, State, and local
FSLT	Federal, State, Local, and Tribal
FSLTE	Fronte Salafiste Liberation de Terre Entrangere
FTO	Foreign Terrorist Organization

G

GAO	General Accounting Office

H

HAN	Health Alert Network
HAZMAT	Hazardous Materials
HCC	Health Command Center
HHS	Health and Human Services
HOTS	Health Operations Tracking System
HQ	Headquarters
HRSA	Health Resources & Services Administration
HSAS	Homeland Security Advisory System
HSC	Homeland Security Council

HSEEP	Homeland Security Exercise & Evaluation Program
HSIN	Homeland Security Information Network
HSOC	Homeland Security Operations Center
HSPD	Homeland Security Presidential Directive

I

IA	Interagency
IAIP	Information Analysis and Infrastructure Protection
IAP	Incident Action Plan
IC	Incident Command
IC	Intelligence Community
ICC	International Control Cell
ICD	Infrastructure Coordination Division
ICE	Immigration and Customs Enforcement
ICEPP	Incident Communications Emergency Policy & Procedures
ICER	Incident Communications Emergency Reference
ICG	International Control Group
ICON	Information Control System
ICP	Incident Command Post
ICP	Intelligence Campaign Plan
ICPACC	Incident Management Public Affairs Coordination Committee
ICS	Incident Command System
IED	Improvised Explosive Device
IIMG	Interagency Incident Management Group
IMAAC	Interagency Modeling and Atmospheric Analysis Center
IND	Investigational New Drug
INR	Intelligence and Research Office
INS	Incident of National Significance
INT-C	International Controller
INTELINK	Intelligence Link
IPR	Illustrative Planning Scenario
IRC	Internet Relay Chat
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Provider
ISTS	Institute for Security Technology

IT	Information Technology
IWG	Intelligence Working Group

J

JFCOM	Joint Forces Command
JFO	Joint Field Office
JIC	Joint Information Center
JIS	Joint Information System
JITF-CT	Joint Intelligence Task Force – Combating Terrorism
JOC	Joint Operations Center
JRIES	Joint Regional Informational Exchange System
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communications System
JWFC	Joint Warfighting Center

K

L

LE	Law Enforcement
LEO	Law Enforcement Online
LINCS	Local Information Network & Communications System
LNO	Liaison Officer
LSG	Large Scale Game

M

M&L	Maritime and Land Security
MA	Mission Assignment
MARSEC	Maritime Security
MCC	Master Control Cell
MCoC	Master Chief of Control
MI	Managed Inventory
MOA	Memorandum of Agreement
MOC	Mission Operations Center
MRC	Medical Reserve Corps

MSEL	Master Scenario Events List
MST	Management Support Team

N

NARAC	National Atmospheric Release Advisory Center
NCC	National Control Cell
NCIC	National Crime Information Center
NCP	National Oil and Hazardous Materials Pollution Contingency Plan
NCS	National Communications System
NCSD	National Cyber Security Division
NCRCC	National Capital Region Coordination Center
NCTC	National Counterterrorism Center
NDMS	National Disaster Medical System
NEADS	Northeast Air Defense Sector
NEP	National Exercise Program
NGA	National Geospatial Intelligence Agency
NGO	Nongovernmental Organization
NICC	National Infrastructure Coordinating Center
NICCL	"Nickel Line" National Incident Communications Conference Line
NIMS	National Incident Management System
NJ	New Jersey
NJ LINCS	New Jersey Local Information Network and Communications System
NL	New London
NLIA	Newark Liberty International Airport
NMCC	National Military Command Center
NOAA	National Oceanic & Atmospheric Administration
NOC	Network Operation Center
NOL	NCTC Online
NORTHCOM	US Northern Command
NPS	National Pharmaceutical Stockpile
NRCC	National Response Coordination Center
NRO	National Reconnaissance Office
NRP	National Response Plan
NSA	National Security Agency

NSRP	National Signals Intelligence Requirements Process
NSRT	"Nothing Significant to Report"
NSSE	National Security Significant Event
NTC	National Targeting Center

O

ODP	Office for Domestic Preparedness
OEM	Office of Emergency Management
ONRA	Office of National Risk Assessment
OPA	DHS Office of Public Affairs
OSHA	Occupational Safety & Health Administration
OSIS	Open-Source Information System
OSLGCP	Office of State and Local Government Coordination and Preparedness

P

PAO	Public Affairs Officer
PCII	Protective Critical Infrastructure Information
PCR	Polymerase Chain Reaction
PD	Police Department
PDA	Preliminary Damage Assessment
PFO	Principal Federal Official
PIO	Public Information Officer
PKI	Public Key Infrastructure
POC	Point of Contact
POD	Point of Dispensing
PPE	Personal Protective Equipment
PROFLOW	Procedural Flow Synopsis
PSO	Private Sector Office
PSPG	Private Sector Planning Group
PSWG	Private Sector Working Group

Q

QRF	Quick Reaction Force

R

RDD	Radiological Dispersion Device
RFI	Request for Information
RRCC	Regional Response Coordination Center
RRT	Regional Response Team
RSS	Receipt, Storage, and Staging

S

SA	Situational Awareness
SAC	Special Agent-in-Charge
SARA	Superfund Amendments and Reauthorization Act
SARS	Severe Acute Respiratory Syndrome
SCO	State Coordination Officer
SEOC	State Emergency Operations Center
SERT	Secretary's Emergency Response Team
SFO	Senior Federal Official
SIOC	Strategic Intelligence Operations Center
SIGINT	Signals Intelligence
S/L	State/Local
SIMCELL	Simulation Cell
SIPRNET	Secret Internet Protocol Router Network
SITREP	Situational Report
SME	Subject Matter Expert
SNS	Strategic National Stockpile
SOE	Senior Official Exercise
SOP	Standard Operating Procedures
SOW	Statement of Work
STARTEX	Start of Exercise
SUV	Sport Utility Vehicle
SVTC	Secure Video Teleconference

T

T2	TOPOFF 2
T3	TOPOFF 3

T4	TOPOFF 4
TARU	Technical Advisory Response Unit
TECS	Treasury Enforcement Communications System
TFR	Temporary Flight Restriction
TOPOFF	Top Officials
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSIS	Transportation Security Intelligence Service
TSIS-OC	TSIS-Operations Center
TSOC	Transportation Security Operations Center
TSOC-CDO	TSOC-Command Duty Officer
TTIC	Terrorist Threat Integration Center
TTX	Table Top Exercise

U

UA	Universal Adversary
UC	Unified Command
UCP	Unified Command Post
UK	United Kingdom
U.S.	United States
USAR	Urban Searcb & Rescue
USCG	U.S. Coast Guard
USPHS	U.S. Public Health Service
USPS	U.S. Postal Service
US&R	Urban Search and Rescue
USSS	U.S. Secret Service

V

VA	Veterans Administration
VBIED	Vehicle-Borne Improvised Explosive Device
VBSS	Visit, Board, Search, and Seizure
VCC	Venue Control Cell
VCoC	Venue Chief of Control
VIP	Very Important Person
VMAT	Veterinary Medical Assistance Team

VMI	Vendor Managed Inventory
VNN	Virtual News Network
VOAD	Volunteer Organizations Active in Disasters
VoIP	Non-Voice-over Internet Protocol
VTC	Video Teleconference

W

WAN	Wide-Area Network
WMD	Weapon of Mass Destruction

X

Y

Y. pestis	Yersinia Pestis

Z

THIS PAGE INTENTIONALLY LEFT BLANK

T4 Command Post Exercise After-Action Report

June 19-22, 2006

Homeland Security

ADMINISTRATIVE HANDLING INSTRUCTIONS

1. The title of this document is *T4 Command Post Exercise After-Action Report.*

2. WARNING: This document is ~~for Official Use Only (FOUO).~~ It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to he controlled, stored, handled, transmitted, distrihuted, and disposed of in accordance with DHS policy relating to ~~FOUO~~ information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

3. Reproduction of this document, in whole or part, without prior approval of the T4 National Exercise Program (NEP) Chief is prohibited.

EXECUTIVE SUMMARY

Top Officials (TOPOFF) 4 (T4) is the fourth in the series of congressionally mandated, biennial, national homeland security preparedness exercise activities designed to train and test national decision makers and to use resources of multiple departments and agencies (D/As). Beginning with the T4 Command Post Exercise (CPX), T4 involves a series of activities dealing with terrorism prevention, incident management, intelligence-handling and investigation, public information, and evaluation. The T4 CPX serves to address the national counterterrorism strategy; exercise the national ability to prevent, respond to, and recover from a weapon of mass destruction (WMD) incident; and engage senior Federal officials.

Sponsored by the Department of Homeland Security (DHS) Office of Grants and Training (G&T), the 2006 T4 CPX was held on June 19–22, in conjunction with the Federal Emergency Management Agency (FEMA)-sponsored Forward Challenge 2006 (FC 06) and Federal Bureau of Investigation (FBI)-sponsored Marble Challenge 2006-02 (MC 06-02) exercises. Over 60 D/As participated in the exercise, along with private sector organizations and State and local officials from Virginia, Maryland, and Washington, DC. Officials from Portland, Oregon, and Guam participated in the exercise simulation cell (SIMCELL).

The evaluation of the exercise focused on three general areas: WMD response, situational awareness and information sharing, and public information. Within each of these areas, several key issues emerged and are addressed in this after-action report (AAR).

Focus Areas and Key Issues

WMD response
• Some predetonation decisions/actions may have compromised operational security. • Protective actions/recommendations were not coordinated with State and local governments. • The May 25 National Response Plan (NRP) notice of change was not fully implemented. • The deployment of Federal and volunteer personnel was limited by WMD contamination.
Situational awareness and information sharing
• Federal D/As and the NCR did not share situational awareness. • Intelligence was not consistently shared across Federal D/As and the National Capital Region (NCR).
Public information
• Conflicting guidance was provided to Federal government employees and the public before the WMD blast.

We summarize each issue below and follow with a list of suggested corrective actions. It is important to note that exercise artificialities and implementation issues affected the exercise and the key issues discussed in this report. Although the White House and Homeland Security Council were engaged in the planning process, they did not participate in the exercise, which affected the decision-making process. Other artificialities, such as differing levels of play by participants, limited coordination among the Federal interagency and between the Federal interagency and the NCR.

Some predetonation decisions/actions may have compromised operational security.

During the T4 CPX, several predetonation decisions and actions could have compromised operational security, notably, implementing the continuity of government condition (COGCON) Level 1, raising the HSAS level, and implementing the Catastrophic Incident Annex (CIA) of the NRP. Federal law enforcement and intelligence personnel assume that terrorists would alter their plans if they thought they were compromised. For example, terrorists might advance their timetable for detonation, alter their plan to strike at secondary targets, destroy evidence of their activities, flee in an attempt to escape without completing their mission, or discard or hide the device for later retrieval. The COGCON level elevations were scripted both in this exercise and in a previous DHS tabletop exercise for senior officials, *Vulcan Warrior*[1], that examined the issue of operational security in a WMD scenario. Participants in *Vulcan Warrior* did not support the scripted COGCON Level 1 decision because they felt the activities associated with COGCON Level 1 could not be carried out without alerting the terrorists.

DHS should collaborate with the intelligence community and State and local governments to examine these decisions and actions and identify potential alternatives to COGCON Level 1 in this type of scenario. In addition, operational security issues should be addressed in NRP supporting policies and procedures.

Protective actions/recommendations were not coordinated with State and local governments.

During the T4 CPX, several key protective actions/recommendations were not coordinated with NCR jurisdictions, most notably increasing the COGCON level to 1, raising the HSAS to Red, and evacuating Prince George's County, Maryland. Thus, the NCR was unable to participate in the development of protective actions and examine how they would be implemented in coordination with the Federal government. It is likely that the lack of participating senior leadership; different levels of commitment among Federal, State, and local (FSL) D/As to the CPX; and misunderstandings about exercise design all contributed to the artificial decision-making process. Future exercises should focus on the coordination of protective actions with State and local officials.

The May 25 NRP notice of change was not fully implemented.

The National Operations Center (NOC), Incident Advisory Council (IAC), and the NOC planning element are new entities replacing the Homeland Security Operations Center (HSOC) and Interagency Incident Management Group (IIMG). The supporting policies and procedures for these entities have not yet been developed. Because the membership for the IAC has not been established, members of the IIMG played as the IAC Transition Team. The NOC participated fully, but has not increased in size beyond the HSOC. The NOC planning element was not yet established.

Because these changes came only weeks before the exercise[2], personnel had little information about what their new roles were and how they should interact within the larger response

[1] Senior Official Exercise (SOE) 05-4, held in May 2004.
[2] They were established in the May 25, 2006, notice of change to the NRP.

structure. Planning efforts are underway to develop the supporting doctrine. In addition, DHS should educate the emergency response community about the role of these new structures and how they are implemented.

The deployment of Federal and volunteer personnel was limited by WMD contamination.

It was unclear who was responsible for determining what areas were considered safe when Federal D/As were making plans to deploy personnel and other resources into the affected area. For example, the American Red Cross (ARC) was concerned about deploying volunteer personnel to staff shelters and other sites, and some D/As disagreed about where mobilization centers should be located. The simulation of Federal field response teams likely contributed to this problem.

A coordinated strategy for staging and deploying responders, and ensuring they were not exposed to unsafe levels of contamination was not evident during the exercise. This responsibility should be clarified to ensure consistent protective actions are employed across the response effort.

Federal D/As and the NCR did not share situational awareness.

Despite efforts to improve communications and information sharing across Federal D/As, they all lacked a shared situational awareness of key information during the T4 CPX. According to the NRP, the NOC is responsible for providing a general domestic situational awareness and a common operational picture. According to the HSOC SOP, the HSOC (now called the NOC) provides information to D/As through a variety of communications links including the Homeland Security Information System (HSIN).

The NOC Common Operating Picture (COP), a new component of HSIN, was not available for this exercise. Furthermore, other methods of communicating this information did not appear to be used in its place. Thus, Federal D/As and NCR organizations gathered information from many different sources, resulting in varied understandings about key information during the exercise. The decisions made in Secure Video Teleconference (SVTC) meetings were not formally documented and disseminated, which contributed to the problem.

The COP has the potential to improve information sharing and situational awareness across FSL D/As. DHS should ensure that D/As are able to access and use the system, that there are redundant methods for sharing information, and that D/As are able to assimilate this information into a shared situational awareness.

Intelligence was not consistently shared across Federal D/As and the NCR.

There were differences in the intelligence information available at Federal D/As and within the NCR during the exercise. Whereas some D/As received detailed information about the threat in the NCR and Landport, others received little or no information. The location of personnel in secure and nonsecure sites contributed to these problems because classified information can only be transferred through secure phones or computer systems. Even when personnel in nonsecure

sites had clearance to receive the information, they often did not have access to secure phones or computer systems. The ability of some Federal D/As and the NCR to take protective actions and prepare their response to a nuclear/radiological incident was affected by this lack of information. DHS should coordinate with the intelligence community to further assess and address this issue.

Conflicting guidance was provided to Federal government employees and the public before the WMD blast.

One of the most important requirements during emergencies is to provide the public with protective action guidance. During the T4 CPX, conflicting protective action guidance was provided to Federal government employees and the public in the NCR and in Landport before the WMD blast. The likely outcome would be public confusion in the NCR and in Landport before the WMD blast and frustration with the Federal D/As.

Although there is a balance between protecting operational security and providing information to the public, information passed to nonessential government personnel, at a minimum, must also be relayed to the public. Nonessential government workers will likely call their families and friends once an announcement is made, thus assuring that the larger public will know something unusual is occurring. Therefore, DHS should work with OPM to develop a standardized emergency leave policy for nonessential government personnel with an elevation to COGCON Level 1 so that it is consistent among all D/As and is also consistent with expected guidance to the public.

Federal D/As were able to "speak with one voice" after the WMD detonation in Landport. However, it is important to recognize that in a real WMD emergency the public will look to their State and local governments first for protective action guidance. Therefore, Federal D/A guidance must he consistent with that provided by the State and local public affairs agencies. This has proved to be a significant challenge in previous TOPOFF exercises and was not examined during the T4 CPX. This issue should be readdressed during the full-scale exercise.

Corrective Actions

The following corrective actions were developed in coordination with a small group of interagency T4 CPX planners. They are intended to be further refined by DHS and the larger interagency into a corrective action plan and are described in more detail in Appendix B.

WMD response
• Conduct pre-exercise training and education for senior leadership. • Write exercise concept of operation plans (CONPLANs) for senior leadership. • Expand pre-exercise participant training. • Develop alternatives to COGCON Level 1 in the COOP architecture. • Create additional measures in COOP plans to minimize impact on local communities. • Develop an interagency playbook for NRP. • Write operational plans for catastrophic scenarios. • Collaborate with the NCR to address protective action coordination. • Establish SOPs for the IAC and NOC.

• Establish procedures for publicizing changes to the NRP. • Develop a training and education program for the NRP. • Clarify the responsible entity for providing guidelines for deployment into potentially contaminated areas.
Situational awareness and information sharing
• Finish development and deployment of the COP. • Develop parameters and standards for the COP, to include spot reports and SITREPS. • Establish video teleconference protocols for incidents of national significance. • Develop D/A-specific policies and procedures for HSIN. • Conduct a feasibility study of integrating HSIN with web-EOC. • Review intelligence sharing procedures. • Develop reachback alternatives for senior leadership. • Ensure that all COOP facilities have SCIFs and can share information at the same level of classification. • Develop a process for linking the National Infrastructure Coordination Center (NICC) with public messaging during an emergency.
Public information
• Analyze options for a dynamic public messaging system and integrate with Integrated Public Alert and Warning Systems (IPAWS) work. • Standardize leave policy for nonessential government personnel in an emergency. • Develop D/A-specific HSAS playbooks.

TABLE OF CONTENTS

1.0 EXERCISE OVERVIEW

1.1 Background

Top Officials (TOPOFF) 4 (T4) is the fourth in the series of congressionally mandated biennial national homeland security preparedness-related exercise activities designed to train and test national decision makers and to use resources of multiple departments and agencies (D/As). Beginning with the T4 Command Post Exercise (CPX), T4 involves a series of activities dealing with terrorism prevention, incident management, intelligence-handling and investigation, public information, and evaluation. The T4 CPX serves to address the national counterterrorism strategy; exercise the national ability to prevent, respond to, and recover from a weapon of mass destruction (WMD) incident; and engage senior Federal officials.

Sponsored by the Department of Homeland Security (DHS) Office of Grants and Training (G&T), the 2006 T4 CPX was held on June 19–22, in conjunction with the Federal Emergency Management Agency (FEMA)-sponsored Forward Challenge 2006 (FC 06) and Federal Bureau of Investigation (FBI)-sponsored Marble Challenge 2006-02 (MC 06-02) exercises. Over 60 D/As participated in the exercise, along with private sector organizations and State and local officials from Virginia, Maryland, and Washington, DC. Officials from Portland, Oregon, and Guam participated in the exercise simulation cell (SIMCELL). Figure 1 lists all T4 CPX participants.

Figure 1. T4 CPX Participating Organizations

American Red Cross **Central Intelligence Agency** **Defense Information Systems Agency** **Department of Agriculture** **Department of Commerce** **Department of Defense** - Office of the Secretary of Defense **Department of Education** **Department of Energy** **Department of Health and Human Services** **Department of Homeland Security** - FEMA - Civil Rights and Civil Liberties - Domestic Nuclear Detection Office - Immigration and Customs Enforcement - Preparedness Directorate - National Communications System - Office of Operations Coordination - Office of Science and Technology - Transportation Security Administration - U.S. Citizenship & Immigration Services - U.S. Coast Guard - U.S. Customs & Border Protection - U.S. Secret Service	**Department of Housing and Urban Development** **Department of Interior** **Department of Justice** - FBI - Criminal Division Counter Terrorism Section - Alcohol, Tobacco, Firearms, and Explosives - U.S. Marshals Service **Department of Labor** **Department of State** **Department of the Treasury** **Department of Transportation** - Federal Aviation Administration **Department of Veterans Affairs** **Environmental Protection Agency** **Executive Office of the President** - Office of Science & Technology Policy **Export – Import Bank of the U.S.** **Federal Communications Commission** **Federal Reserve System** **General Services Administration** **Guam** **Internal Revenue Service** **National Archives and Records Administration**	**National Capital Region** - DC EMA - Virginia DEM - MEMA - Supporting Jurisdictions and Agencies **National Labor Relations Board** **National Science Foundation** **National Transportation Safety Board** **Nuclear Regulatory Commission** **Office of Personnel Management** **Office of the Director of National Intelligence** **Office of the U.S. Courts** **Peace Corps** **Pension Benefit Guaranty Corporation** **Portland, Oregon** **Securities and Exchange Commission** **Small Business Administration** **Social Security Administration** **U.S. Agency for International Development** **U.S. Army Corps of Engineers** **U.S. House of Representatives** **U.S. Postal Service** **U.S. Senate Office of the Sergeant at Arms**

1.2 Scenario

The T4 CPX scenario was derived from National Planning Scenario (NPS) 1—Weapons of Mass Destruction (WMD) Detonation—and its associated Universal Adversary (UA) threat models. Comprising 15 scenarios of plausible terrorist attacks and natural disasters, the NPS series serves to yield core prevention and response requirements to help direct comprehensive preparedness planning efforts. The UA is a fictitious adversary for general exercise use.
Designed to achieve the objectives of all three exercises (T4 CPX, FC 06, and MC 06-02), the scenario involved the acquisition of two WMD from the former Soviet Union arsenal by UA terrorists associated with radical Sunni groups. The terrorists smuggled the weapons into the United States in separate shipments. One WMD was trucked across the southern border and intended for detonation in the National Capital Region (NCR). Intelligence regarding this weapon drove the U.S. government to initiate Continuity of Operations (COOP) procedures. The other WMD arrived in the fictitious coastal city of Landport, Central Pacifica (CP) via charter vessel and was detonated in port upon detection.

1.3 Exercise Concept

A prevention and response-focused exercise, the T4 CPX was driven by events and intelligence from a Master Scenario Events List (MSEL) simulating domestic terrorist incidents in the NCR and the notional city of Landport, CP. The principle training audience included D/A senior officials and staff, multicoordination centers (e.g., Incident Advisory Council [IAC][3] Transition Team), and the DHS National Operations Center (NOC)[4] personnel. Designed to capitalize on lessons learned from prior TOPOFF and Senior Officials Exercises (SOEs), the T4 CPX tested and evaluated policies and procedures outlined in the National Response Plan (NRP) and National Incident Management System (NIMS).

1.4 Evaluation Methodology

The evaluation approach for the T4 CPX is based on the methodology outlined in HSEEP Volume II and the methodology used in previous TOPOFF exercises. It uses observation/data collection, reconstruction, and analysis to determine what happened in the exercise and to develop findings and recommendations.

The analysis focuses on interagency issues and coordination as put forth in the NRP, NIMS, and supporting protocols. This analysis and after-action report (AAR) does not look at D/A specific tasks, procedures, or performance. D/As are encouraged to conduct their own evaluation and analysis of their exercise performance for internal use and dissemination.

The methodology uses the following three-step process:

1. *Observation/data collection* collects the data necessary to reconstruct exercise events.
2. R*econstruction* compiles and synchronizes the data to determine what happened and when.

[3] The Incident Advisory Council replaced the Interagency Incident Management Group (IIMG).
[4] The National Operations Center replaced the Homeland Security Operations Center (HSOC).

3. *Analysis* uses the reconstruction to provide findings and recommendations related to the exercise objectives.

See the Evaluation Plan (Annex G of the Exercise Plan [EXPLAN]) for a detailed description of this methodology. In addition to examining the overarching objectives, we selected several focus areas of analysis for the T4 CPX, shown in Table 1. These areas are derived from specific exercise objectives and were chosen because they meet one or more of the following criteria:

- Identified as an unresolved issues in past TOPOFF exercises
- Identified as an issue during the response to Hurricane Katrina
- Relevant to the T4 CPX scenario

Table 1. Focns Areas of Analysis

Focus Area	T4 CPX Objectives	Mission
WMD response	Test existing procedures for domestic incident management of a terrorist WMD event and top officials' capabilities to respond in partnership in accordance with the NRP and NIMS. Exercise the authorities, responsibilities, and capabilities of the Federal assets necessary to respond to a terrorist WMD incident.	Execution of Federal authorities, responsibilities, and decision making during a WMD incident
Situational awareness and information sharing	Test the ability of command/operations/intelligence centers to share intelligence and information and maintain a common operational picture (COP).	Multiagency coordination
Public information	Exercise the coordination of a domestic and international media and public communications strategy and public messaging in the context of a terrorist WMD incident.	Coordination of public communications strategy and public messaging

A quick-look report was prepared within 72 hours of the exercise and was based on immediate feedhack from the exercise hotwash. As part of the data collection process, DHS requested that participants submit their lessons learned and comments on the quick-look report by July 15. Appendix C includes a list of participants who submitted responses, along with a compilation of lessons learned.

Following the analysis of each issue, suggested corrective actions are presented. These actions were developed in coordination with a small group of interagency T4 CPX planners. They are intended to be further refined by DHS and the larger interagency into a corrective action plan.

1.5 Exercise Artificialities

The following artificialities and constraints were used to accomplish the exercise objectives:

- Weather and atmospheric conditions for notional locations in the exercise were based on historical weather patterns to create a specific dispersal pattern of the agents involved in the exercise event. This was necessary to drive exercise play to meet the agreed upon overarching and agency-specific exercise objectives determined during the T4 CPX planning process.
- There were varying levels of play among senior officials, and surrogates played in place of some key decision makers. The Homeland Security Council (HSC) Counterterrorism Support Group (CSG) did not participate in the exercise as planned. Senior leader Secure Video Teleconference (SVTC) meetings were held in place of the CSG meetings to simulate the decision making that would have occurred during these meetings. The level of play among D/As varied as well and is described in the EXPLAN.
- D/As and organizations not participating in the T4 CPX were simulated through the Simulation Cell (SIMCELL). These included much of the Department of Defense (DoD), FEMA Region X, and State and local officials of Landport and Central Pacifica. The SIMCELL representation of nonparticipating agencies was determined by the agencies' published policies, procedures, doctrine, and requests for information (RFIs) developed during the planning process.

In addition to the artificialities the following exercise implementation issues impacted play:

- During the T4 CPX, the Intelligence Control Cell (ICC) was not collocated with the Master Control Cell (MCC) and did not operate around the clock.
- Some participants were not aware who was participating and who was not or how to interact with the SIMCELL.
- Some field entities such as the HHS Regional Emergency Coordinators (RECs) were not simulated.
- Some D/As were not participating in all exercises (e.g., participating only in FC 06) or gave one of the exercises priority by limiting play in the others.

Along with the artificialities, these issues had the following impact on play:

- Key decision-making activities were simulated or carried out at a lower level of authority, and there was no final adjudicator present. Decisions were also not coordinated with the NCR players.
- There was limited Federal interagency and Federal-NCR coordination in exercise play. For example, Emergency Support Function (ESF) #12 (Energy) and ESF #13 (Public Safety and Security) did not send representatives to the NRCC. This limited the NRCC's ability to respond to ESF #12 and ESF #13 issues and to coordinate with the Department of Energy (DOE), which was the coordinating agency under the NRP nuclear/radiological incident annex in this scenario.
- Players had difficulty communicating and coordinating with simulated organizations. For example, participants in the NRCC were not initially aware that Region X was being

simulated. Later, they did learn how to contact the SIMCELL and were able to interact with a simulated Region X.

- There was limited involvement from Federal D/As and the NCR in public information play, and no one actually acted as the State and local counterpart for Landport. In addition, the National Joint Information Center (NJIC) never received any guidance from White House Communications or from the HSC.

As described in Table 2, DHS has developed corrective actions to ensure better senior leader participation in future TOPOFF exercises.

Table 2. Exercise Participation: Suggested Corrective Actions

Corrective Action	Description	Responsible Agencies	Timeline
Conduct pre-exercise training and education for senior leadership.	Conduct training and education for senior leaders prior to the next Full Scale Exercise (FSE) to ensure they are engaged and have full awareness of their anticipated role.	DHS—Preparedness Directorate	6 Months
Write exercise CONPLANs for senior leadership.	Write a concept of operations (CONPLAN) for the next FSE. Senior leadership would be the target audience, and the intent would be to provide them with a description of their roles and responsibilities during the exercise.	DHS—Preparedness Directorate	6 Months
Expand pre-exercise participant training.	Expand the training and information materials provided to players and field controllers to ensure they are aware of the expectations for coordination and interaction with participating and simulated organizations.	DHS—Preparedness Directorate	12 Months

2.0 EXERCISE GOALS AND OBJECTIVES

2.1 Goals

T4 was designed to train and test national decision makers and to use resources of multiple D/As in homeland security preparedness. The overarching goals of T4 are as follows:

1. **Prevention**: To test the handling and flow of operational and time-critical intelligence between agencies to prevent a terrorist incident.
2. **Incident management**: To test the full range of existing procedures for domestic incident management of a terrorist WMD event and to improve top officials' (Federal/State/local) capabilities to respond in partnership in accordance with the NRP and NIMS.
3. **Intelligence/investigation**: To test the handling and flow of operational and time-critical intelligence between agencies prior to and in response to a linked terrorist incident.
4. **Public information**: To practice the strategic coordination of media relations and public information issues in the context of a terrorist WMD incident or Incident of National Significance.
5. **Evaluation**: To identify lessons learned and promote best practices.

2.2 Objectives

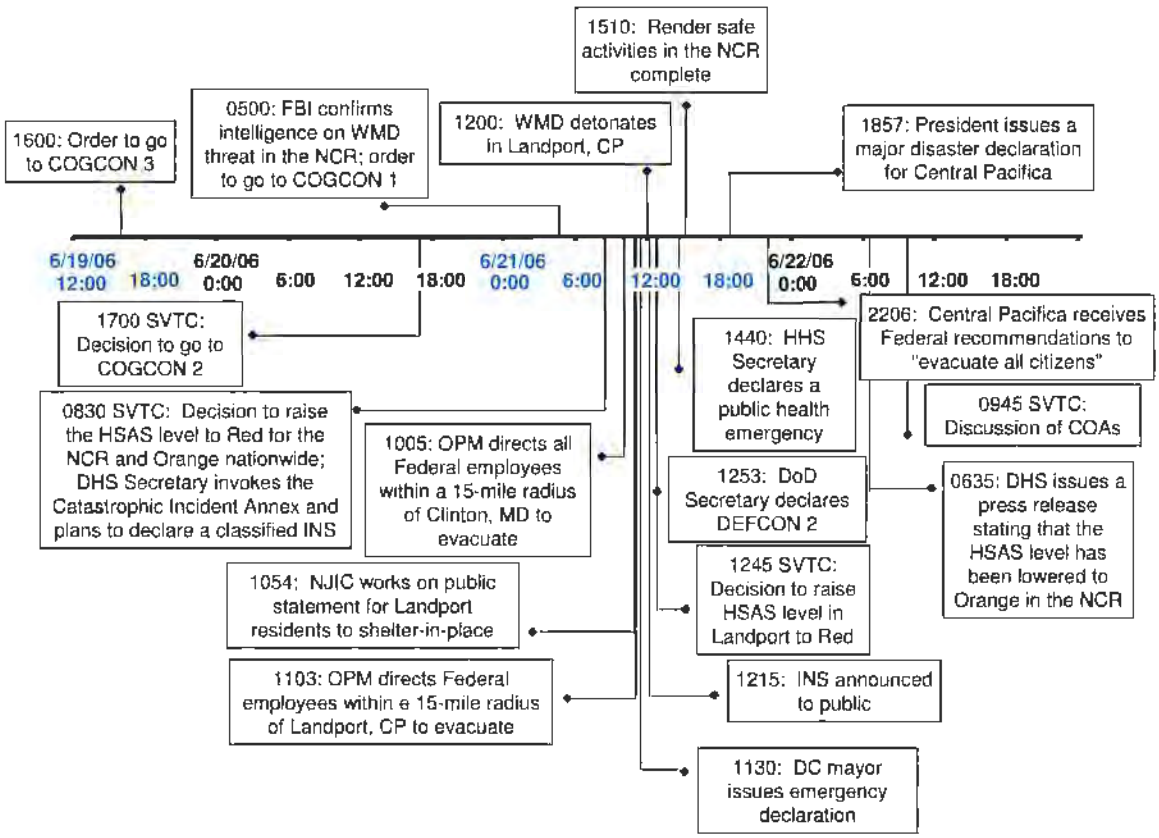
The T4 CPX objectives were as follows:

1. Examine the effects of implementing continuity programs in the context of a credible terrorist WMD threat.
2. Exercise and validate D/As' Continuity of Operations (COOP) plans, procedures, and policies.
3. Exercise the coordination of a domestic and international media and public communications strategy and public messaging in the context of a terrorist WMD incident.
4. Test existing procedures for domestic incident management of a terrorist WMD event and top officials' capabilities to respond in partnership in accordance with the NRP and NIMS.
5. Exercise WMD render safe operations.
6. Exercise the authorities, responsibilities, and capabilities of the Federal assets necessary to respond to a terrorist WMD incident.
7. Examine the handling of mental health and special needs issues that may arise during and after a terrorist WMD event.
8. Examine emergency operations planning and citizen protection capabilities in response to a terrorist WMD incident.
9. Examine public health, medical support, mass decontamination, and mass care requirements during a terrorist WMD incident.
10. Test the ability of command/operations/intelligence centers to share intelligence and information and maintain a COP.

3.0 EXERCISE EVENTS SYNOPSIS

The T4 CPX scenario involved two WMDs; one was located and rendered safe in the NCR, and the other detonated in Landport, CP. The following is a reconstruction of injects, decisions, and actions from June 19 through June 22, 2006. It is based on the logs and supporting data collected by data collectors stationed at key locations during the exercise. It is a factual recount of the decisions and actions as they unfolded during the exercise. Some of these events deviated from what was expected by the exercise planners. An overview of the key events is shown in Figure 2.

Figure 2: T4 CPX Key Events



3.1 June 19, 2006

The White House ordered the move to COGCON 3 at 4:00 p.m. D/As were required to assume COOP activities for COGCON 3 by 8:00 a.m. on June 20.

At a 6:00 p.m. meeting, the NCR Senior Policy Group discussed the possibility of a threat to the region and decided to implement normal 4th of July protective measures. It convened an incident action planning meeting the next morning.

Following an attempt to photograph port security measures and on-duty customs agents in Landport, CP, Pakistani-American student and radical Muslim Karim Mohammed Butt was confronted by building security, and arrested by the Landport Police Department at 7:00 p.m..

The FBI Joint Terrorism Task Force was notified, and they began interrogating Butt. He revealed that he knew Jaffar bin-Husseini, a Pakistani-American and fellow Islamic radical charged with executing operations in Landport, but he did not provide any information about the terrorist plot.

3.2 June 20, 2006

Local authorities and the FBI confirmed Butt's identify. Butt hinted that the device had a radioactive component. At 5:00 p.m., law enforcement officers located several empty containers with traces of heroin, one lead-lined container, and a USB device in a warehouse in New Dayton, Maryland.

DHS hosted a SVTC at 5:00 p.m. to discuss possible threats in the NCR. The participants, who included the DHS Secretary, discussed releasing the WMD intelligence to the mayors of five potentially targeted cities. They also proposed a snow-day type response to limit persons in the cities and prevent morning commutes. The Department of State reported that it had approached Russia for information on any missing weapons, and the FBI reported that it would begin searching for a possible WMD in the NCR. Participants decided to increase the readiness levels of response assets and to go to COGCON 2[5]; the order was given at 7:16 p.m.

The FBI and DOE began searching the NCR at 7:00 p.m.

3.3 June 21, 2006

3.3.1. 5:00 a.m.–12:00 pm.

At 5:00 a.m., the FBI confirmed the intelligence on a WMD threat in the NCR, resulting in the DHS order to go to COGCON 1 by 9:00 a.m. The FBI located the device in New Dayton, MD[6], and deployed assets to the site by 9:00 a.m.

By 7:47 a.m., a domestic threat conference call was convened. Participants learned that a WMD had been located in the NCR.

At 8:00 a.m., State and local NCR emergency management offices began activating and tracking the incident and response activities.

During an 8:30 a.m. SVTC that ended about an hour later, participants decided to raise the HSAS level to Red for the NCR and Orange nationwide, and evacuate Prince George's County. This prompted a discussion of who has the authority to call for such an evacuation. In addition, the DHS Secretary decided to invoke the Catastrophic Incident Annex of the NRP and stated that he planned to declare a classified Incident of National Significance.

At about 9:14 a.m., the IAC discussed the intelligence it had on the two WMDs, which said one was in the NCR and a second was potentially in Landport. At 10:05 a.m., DNDO participants

[5] Increasing the COGCON level to 1 was also discussed, but the increase to COGCON 2 was chosen in part because it was prescripted.

[6] This was a notional location for Clinton, MD. The Marble Challenge field exercise was carried out at another location.

also discussed intelligence suggesting Landport as a second target. The NOC had just received WMD threat modeling for the NCR and continued working on an analysis for other potentially targeted areas.

At 9:00 a.m., VNN reported that an exodus of Federal employees from Washington, DC, was causing traffic delays, and that there were rumors of Federal government relocation. VNN confirmed these rumors at 9:53 a.m., reporting that the Federal government was indeed undergoing COOP activities.

There had been growing speculation all morning among participants regarding whether the Office of Personnel Management (OPM) would release Federal employees; there had still been no decision at 8:45 a.m. At 10:05 a.m., the OPM directed all Federal employees within a 15-mile radius of Clinton, MD, to evacuate.[7]

At 9:54 a.m., personnel working in the NJIC were told a "snow day" order was in effect for Landport and began working on press releases that explained what was happening in both Landport and the NCR.

When ESF#1 (Transportation) personnel working in the National Response Coordination Center (NRCC) learned that an evacuation of Prince George's County was underway at about 10:30 a.m., they inquired whether Federal assistance was required. Later they were told that the evacuation was being handled locally and that no Federal assistance was needed. The NRCC also reported at 10:30 a.m. that the Domestic Emergency Support Team had (notionally) deployed to the NCR.

VNN reported at 10:45 a.m. that there was a threat to the Washington, DC region. At 10:55 a.m., it reported that the HSAS level for Washington DC had increased to Red, and the nation to Orange.

During the National Incident Communications Conference Line (NICCL) call at 9:54 a.m., snow day declaration and shelter-in-place orders were reported to be in effect for Landport. At 11:03 a.m., the OPM director directed Federal employees within a 15-mile radius of Landport, CP, to evacuate and seek shelter north of the area.

Back in the NCR, DHS issued a press release at 11:11 a.m. on the evacuation of Prince George's County, MD and the elevation of HSAS levels. At 11:30 a.m., the DC mayor issued an emergency declaration, and FEMA reported that FIRST, ERT-N, NDMS, and US&R teams had been activated and deployed to East and West Coast mobilization centers.

With the WMD aboard, Husseini attempted to dock in Landport at 11:00 a.m. The number of law enforcement in the area and continuous news reports on television made Husseini increasingly nervous. He decided to arm the weapon and called Butt repeatedly, but to no avail.

[7] OPM may have been acting on knowledge of the scenario rather than the current intelligence information that was in play.

Husseini's attempt to dock his yacht at this location arose suspicion among CBP officers, who began boarding and searching the vessel. When their radiation identifier registered multiple neutron readings, the officers contacted the Laboratory Scientific Services and attempted to transmit the data. At the point of detection, Husseini detonated the device using his cell phone, causing a low yield detonation.

3.3.2. 12:00 p.m.–12:00 a.m.

Within minutes of the detonation, VNN reported an unidentified explosion in Landport and confirmed within the hour that it was a nuclear detonation. It did not report that the detonation was a terrorist attack until 2:35 p.m.

At 12:15 p.m., the DHS Secretary publicly declared the Landport attack an Incident of National Significance.

After much consideration, HHS decided to give administrative leave to all NCR employees at 12:20 p.m. Options for both unscheduled and administrative leave were discussed.

DHS issued a press release at 12:23 p.m. stating that an investigation of a credible threat to Landport was underway. By 12:30 p.m., 14 NDMS teams, four US&R teams, and an ERT-N had deployed to Philadelphia, PA, and additional teams were (notionally) on alert. FEMA Regions III, IV, and X also (notionally) activated. At this time, DHS also confirmed that the Landport blast was nuclear.

At 12:30 and 12:45 p.m., DHS hosted an SVTC, during which participants decided to raise the HSAS level in Landport to red. At 1235 HHS operations called DoD about patient movement. The DoD Secretary declared DEFCON 2 at 12:53 p.m.

Back in the NCR, the HSAS level remained at red, and FBI render safe activities were ongoing. At 12:33 p.m., the DC mayor declared a public emergency in response to the threat. There was speculation that an evacuation of DC was imminent.

At 1:15 p.m., ESF #8 reported that FMS and RDF teams had been activated and staged (notionally) and that FEMA had (notionally) deployed essential commodities to the affected area. In the meantime, the president issued a statement on the Landport attack.

At 1:17 p.m., DOE completed initial NARAC/IMAAC plots for Landport in response to a request for the models at 12:18 p.m. Despite inquiries to the HSOC, HHS did not receive the plume model; by 1:50 p.m., its own subject matter experts (SME) had drawn graphs to estimate casualties and how long responders can safety stay in the bot zone. After additional inquiries to DHS, HHS finally received the plume models at 2:05 p.m. Similarly, the Landport SIMCELL did not receive the plume models either. After inquiring of the IMAAC, it received them about five hours after the detonation.

By 2:10 p.m., several ERTs and one FIRST were (notionally) on their way to Landport and Region X, while NDMS, Disaster Mortuary Operations Response Teams (DMORT), and US&R teams were (notionally) mobilized. In addition FEMA began coordinating response activities

with the American Red Cross. At 2:20 p.m., DHS issued a press release on Landport response activities as well as a statement from the DHS Secretary. Twenty minutes later, the HHS Secretary declared a public health emergency. SNS pushpacks and TARU teams were identified for deployment to Landport.

DHS distributed the Incident of National Significance statement at 2:44 p.m. By 3:00 p.m., it released estimates that approximately three to three and a half square miles were completely or mostly destroyed in the Landport attack. There were no casualty estimates at this time.

At 3:10 p.m., the FBI completed render safe activities in the NCR and began preparing the device for shipment by 5:55 p.m. By this time 15 to 20 percent of Prince George's County had been evacuated.

During a 3:30 p.m. NICCL conference call, the JICC learned that that radioactivity in Landport was moving southeast and that first responders were (notionally) having difficulty getting to the area. The CDC reported that it had contacted public health directors and other health officials and that the SNS was ready for deployment.

By 3:38 p.m., USTRANSCOM had implemented its patient movement capability to support NDMS and other pending missions. Shortly thereafter, the DoD Secretary ordered a surging of DoD asserts in the northwest region to accommodate mass casualties.

At 3:55 p.m., Landport informed HHS that it needed ten Disaster Medical Assistance Teams (DMAT) and five DMORT, and recommended using Landport airport as a staging area. Its hospital system had been locked down to avoid further contamination. In the meantime there was ongoing discussion at DHS on the status of render safe operations, whether the HSAS level in the NCR should he lowered to Orange, and whether evacuation from the NCR should cease.

According to a 4:30 p.m. VNN report, the Landport detonation resulted in 1,000 confirmed fatalities, 15,000–30,000 estimated fatalities, and 30,000–100,000 recipients of fatal doses of radiation. At 4:54 p.m., HHS issued press releases on its ongoing Landport response activities and safety and decontamination recommendations, and DHS issued a press release naming principal Federal officials. HHS issued another press release an hour later on the public health emergency declaration for Central Pacifica.

At 5:04 p.m., the JTF-NCR issued a press release on the Andrews Air Force Base evacuation that took place earlier that day. The FBI moved the device out of the NCR at 6:19 p.m.

At 6:57 p.m., the president issued a major disaster declaration for Central Pacifica.

FEMA issued a press release at 9:21 p.m. on the disaster declaration, and another at 9:30 p.m. on response activities in Landport.

At 9:30 p.m., the HSAS level was reduced to Orange in the NCR and the Prince George's County evacuation order was rescinded. DHS reported 1,000 known fatalities, 15,000–30,000 estimated

fatalities, and 30,000–100,000 estimated recipients of fatal doses of radiation in the Landport detonation.

3.4 June 22, 2006

DHS issued a press release at 6:35 a.m. stating that the HSAS level had been lowered to Orange in the NCR. At 9:45 a.m., it hosted a SVTC to discuss courses of action for sheltering in place, mass decontamination, mass care, and response assets in Landport.

At 10:30 a.m., the DHS Secretary gave an update on ongoing response activities, followed by a statement to DHS employees at 11:08 a.m.

The T4 CPX concluded at 12:00 p.m.

4.0 ANALYSIS OF MISSION OUTCOMES AND CRITICAL TASK PERFORMANCE

This section analyzes exercise play and the key issues that arose in the three focus areas of analysis selected in the Evaluation Plan. Table 3 shows those focus areas and their key discussion issues.

Table 3. Focus Areas of Analysis

Focus Area	Issues
WMD response	• Some predetonation decisions/actions may have compromised operational security. • Protective actions/recommendations were not coordinated with State and local governments. • The May 25 NRP notice of change was not fully implemented. • The deployment of Federal and volunteer personnel was limited by WMD contamination.
Situational awareness and information sharing	• Federal D/As and the NCR did not share situational awareness. • Intelligence was not consistently shared across Federal D/As and the NCR.
Public information	• Conflicting guidance was provided to Federal government employees and the public before the WMD blast.

4.1 WMD Response

Homeland Security Presidential Directive 5 (HSPD-5) designates that the Secretary of Homeland Security is responsible for coordinating Federal resources within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. The NRP and NIMS are the overarching doctrine for carrying out this responsibility. In this section, we discuss several issues that arose in the coordination of the response to the T4 CPX WMD scenario.

4.1.1. Some predetonation decisions/actions may have compromised operational security.

The NRP contains the following information regarding operational security:

- Operational security considerations may dictate that activation of NRP elements be kept to a minimum, particularly in the context of certain terrorism prevention activities.
- In the preincident mode, notification of an Incident of National Significance may be conducted discreetly, on a need-to-know basis, so as to preserve the operational security and confidentiality of certain law enforcement and investigative operations.
- The NRCC begins interagency operations by coordinating initial activation, the deployment of special teams, etc., as dictated by operational security considerations.
- PFO designations may be made on a discreet need-to-know basis to preserve operational security.

The HSOC, NRCC, and IIMG SOPs[8] provide no additional details on operational security considerations other than what is already described in the NRP.

Summary of Issue
During the T4 CPX, several predetonation decisions and actions could have compromised operational security: notably implementing COGCON Level 1, raising the HSAS level, and implementing the Catastrophic Incident Annex (CIA) of the NRP.

Consequence
It is assumed by Federal law enforcement and intelligence personnel that terrorists would alter their plans if they knew they were compromised. Alterations could include advancing their timetable for detonation, altering their plan to strike at secondary targets, destroying evidence of their activities, fleeing in an attempt to escape without completing their mission, and discarding or hiding the device for later retrieval.

Analysis
Some of the decisions and actions taken in the T4 CPX contrasted with those made during a previous tabletop exercise with a similar scenario. *Vulcan Warrior,* the fourth in a series of Homeland Security tabletop exercises for senior officials in FY-05, addressed policy and operational issues that could arise if the president ordered the Federal government to implement a COGCON for COOP Level 1 plan in response to the threat of an imminent improvised nuclear device (IND) attack. The discussion centered around what information would be shared, and with whom. Many of the same decisions and actions that occurred during Vulcan Warrior were also considered during the T4 CPX. Therefore, we compare some of these decisions with the discussions recorded during *Vulcan Warrior.*

COGCON Level 1
As in *Vulcan Warrior*, the elevation to COGCON Level 1 was prescripted for the purposes of the T4 CPX. However, participants in *Vulcan Warrior* did not support the scripted COGCON for COOP Level 1 decision, given the scenario course of discussion. Participants felt it would be impossible to inform all Federal agencies that they would need to prepare for imminent relocation of their leadership to their Level 1 alternate facilities without risking an immediate compromise of operational security. They felt that such a decision would almost certainly be detected by the terrorists and could trigger early detonation of the IND. In addition, they predicted that such a decision would almost surely trigger a massive, spontaneous evacuation from the Washington, DC, metropolitan area, resulting in massive gridlock and putting more people at risk for the effects of the IND, if detonated.

HSAS Elevations
A consensus emerged among participants in *Vulcan Warrior* that the intelligence and information related to a potentially imminent, but non-geographically specific, WMD threat would be tightly controlled and shared only among those with a need to know. Based on this insight/decision, officials determined that there would he no benefit to changing the HSAS. Participants in *Vulcan Warrior* did not discuss changes to the HSAS level once they had

[8] The HSOC and IIMG SOPs have not yet been updated to reflect the transition to the NOC and IAC.

geographic specificity of the threat. However, they did acknowledge that operational security would still be the prime concern with this additional information.

The T4 CPX threw a twist into the *Vulcan Warrior* scenario with two WMD threats, one known to be in the NCR and a second, less specific threat to several geographic areas. Several decisions were made in response to the known threat to the NCR, namely changing to COGCON Level 1 and raising the HSAS level. It is possible that these decisions could have compromised operational security for the operations against the second threat. In fact in the scenario the Landport terrorist Husseini detonated the second WMD early because he was concerned about the continuous news reports and felt threatened by the CBP officers who boarded and searched his yacht.

Declaring an INS and Implementing the CIA
Just after the SVTC on the morning of June 21, many D/As were told an INS was in effect and that the CIA had been activated. Although some of the initial reports that the Secretary had declared an Incident of National Significance used the terms "secret" or "classified," this information was fairly well known prior to the blast and there was no direction on how this information should be treated.[9] Thus, operational security was not widely considered when taking actions prior to the blast that could have been noticed by the public or the terrorists. For example, FEMA began preparing to prestage personnel and supplies in both the NCR and Landport according to the CIA. Such actions were not discussed in *Vulcan Warrior*.

Recommendation
Because the move to COGCON Level 1 was prescripted, the exercise provided only a limited opportunity to examine alternatives to this action. DHS should collaborate with the intelligence community and State and local governments to examine these decisions and actions and identify potential alternatives to COGCON Level 1 in this type of scenario. In addition, operational security issues should be addressed in NRP supporting policies and procedures. Suggested corrective actions are listed in Table 4.

Table 4. Operational Security: Suggested Corrective Actions

Corrective Action	Description	Responsible Agencies	Timeline
Develop alternatives to COGCON Level 1 in the COOP architecture.	Consider alternatives to COGCON Level 1, such as creating operational depth by ensuring that geographically dispersed individuals are trained to carry out COOP roles and responsibilities or using devolution in place of moving all essential personnel.	DHS—FEMA	12 Months
Create additional measures in COOP plans to minimize impact on local	Additional measures should be added to COOP plans to account for a deployment's impact on the local economy and infrastructure and for the logistical challenges associated with deployment. Memorandums of Understanding (MOUs) should	DHS—FEMA	6 Months

[9] It was not released to the public in an official statement until 2:20 p.m. on June 21.

Corrective Action	Description	Responsible Agencies	Timeline
communities.	be signed with the host communities.		
Develop an interagency playbook for the NRP.	Develop an interagency playbook for the NRP. This would be a companion piece to the NRP that would be prescripted with operational security considerations, user checklists, have a common set of questions, and would also be developed for the 15 National Planning Scenarios.	DHS—Preparedness Directorate	9 Months
Write operational plans for catastrophic scenarios.	Write specific operational plans that would complement the operational framework contained in the Catastrophic Incident Annex of the NRP and address operational security in specific scenarios.	DHS—NOC Planning Element	1 Year

4.1.2. Protective actions/recommendations were not coordinated with State and local governments.

Summary of Issue

During the T4 CPX, several key protective actions/recommendations made by DHS were not coordinated with the NCR, most notably increasing the COGCON level to 1, raising the HSAS level to Red, and evacuating Prince George's County, Maryland.

Consequence

The NCR was unable to participate in the development of protective actions and examine how they would be implemented in coordination with the Federal government. It is likely that the lack of participating senior leadership, different levels of commitment among FSL D/As to the CPX, and misunderstandings about exercise design all contributed to the artificial decision-making process.

Analysis

During the 8:30 a.m. SVTC on June 21, participants decided to raise the HSAS level to Red for the NCR and to evacuate Prince George's County. The previous day, a SVTC was held to discuss intelligence and changes in COGCON levels. No officials from the NCR were consulted about these decisions.[10] On many occasions during the exercise, NCR officials requested information through the Office of National Capital Region Coordination (ONCRC), which was repeatedly unable to obtain information from the NOC for release. For example, NCR players were notified that the COGON Level was raised to Level 2 at about 8:00 p.m. on June 20, by the ONCRC. Officials from DC immediately responded by asking why and whether a change in HSAS level was being considered. The ONCRC forwarded this request to the NOC but received no information to pass on to the NCR participants.

[10] The COGCON level changes were prescripted for the CPX.

It is possible some information was withheld from NCR officials for operational security concerns. If so, this is counter to the criteria established during *Vulcan Warrior*, in which participants said that operational security is more important than sharing information only when the geographic location of the WMD threat is unknown. At that time in the T4 CPX, one WMD threat was known to be in the NCR. Because information about that threat was not shared with NCR officials, they were not involved in decision making regarding protective action recommendations. As discussed later in the Public Information section, the Federal government took protective actions in the NCR in response to the threat.

There was little discussion recorded about the implications of decisions made in the 8:30 a.m. SVTC. For example, with the HSAS level being raised to Red in the NCR and Orange for the nation, what were the particular actions that FSL D/As were supposed to implement in response to this elevation? What did this mean for jurisdictions near but outside of the NCR? Although not widely recorded during this exercise, this issue has received considerable discussion during past TOPOFF exercises and it is unclear whether it has been clarified. Also not discussed was what the public should be doing in response to the HSAS elevation. The information given in the 11:11 a.m. press release on June 21 was to follow the guidance of State and local officials and review family preparedness plans. Because this decision and press release were not coordinated with State and local officials, they did not have the opportunity to develop recommendations.

Many players thought that the DHS Secretary had ordered the evacuation of Prince George's County.[11] The Federal authority to order an evacuation is defined in the NRP. The NRP assumes that evacuation plans are initiated on the State and local level and that Federal officials will work in conjunction with State authorities when executing the plan. Federal assistance is provided when the emergency or disaster overwhelms the State or local entity, and once involved, Federal officials take the lead on coordination and technical assistance. For example, the Department of Transportation (DOT) would aid in coordinating critical facility closures and movement restrictions to allow for traffic flow during an evacuation.

Clearly, the evacuation of Prince George's County was an action that would have required a tremendous amount of coordination with State and local officials in the NCR. Questions that would need consideration include the following:

- Where were county citizens supposed to evacuate considering the HSAS level was Red for the entire NCR and that traffic congestion that was being reported?
- Where were shelters to be set up and who was to operate them? How were people to get there?
- How were those with special needs being assisted?

When the ESF#1 (transportation) Liaison in the NRCC heard that Prince George's County was being evacuated at about 10:30 a.m. on June 21, he inquired whether there was a need for

[11] It is likely that the outcome from the SVTC was the recommendation to evacuate Prince George's County. The Evaluation Team was not privy to the SVTC, nor were any notes released from the SVTC. Regardless of what was stated in the SVTC, the D/As proceeded as if the evacuation had been ordered.

Federal assistance. The NRCC followed up on this and was told that no Federal assistance was required and the evacuation was being handled locally.

Recommendations
The coordination of protective actions in collaboration with state and local governments was not fully exercised in the T4 CPX. The Federal government should include State and local NCR governments in future COOP and HSAS-related preparedness activities to improve coordination of protective actions during a crisis. Suggested corrective actions are listed in Table 5.

Table 5. Coordinating Protective Actions: Suggested Corrective Actions

Corrective Action	Description	Responsible Agencies	Timeline
Collaborate with the NCR to address protective action coordination.	Conduct exercises, workshops, and/or plan reviews in coordination with the NCR to ensure that Federal government plans for evacuation and other protective actions are fully synchronized with NCR plans.	DHS—Preparedness	6 Months

4.1.3. The May 25 NRP notice of change was not fully implemented.

A few weeks before the exercise on May 25, 2006, DHS issued a notice of change detailing several revisions to the NRP. One change established the NOC as the successor to the HSOC, and reformulated the former IIMG as a senior advisory council and adjudication body for the Secretary of Homeland Security in his role as the Federal incident manager.

Summary of Issue
The NOC, IAC, and the NOC planning element are new entities replacing the HSOC and IIMG. The supporting policies and procedures for these entities have not yet been developed. Because the membership for the IAC has not been established, members of the IIMG played as the IAC Transition Team. The NOC participated fully, but has not increased in size beyond the HSOC. The NOC planning element was not yet established. Furthermore, the NRP is a high-level policy document and many of the supporting plans and procedures that are necessary to carry out the roles and responsibilities it describes are still under development.

Consequences
Personnel had little information about what the new roles of the NOC and IAC were and how they should be interacting within the larger response structure.

Analysis
The definition of the IAC as recorded in the May 25 notice of change is as follows:

> "The IAC is a tailored group of senior Federal interagency representatives that adjudicates matters that cannot be resolved by the NOC-NRCC and provides strategic advice to the Secretary of Homeland Security during an actual or potential incident requiring Federal coordination."

Previously, the IIMG was described as a "Federal headquarters-level multiagency coordination entity that facilitates strategic Federal domestic incident management for Incidents of National Significance." During the exercise, the IAC Transition Team prepared courses of action (COAs) briefings for the Secretary and developed planning priorities. This role was similar to what the IIMG had done in past exercises and emergencies.

The COA groups within the IAC included domestic counterterrorism and law enforcement; border, maritime, and transportation security; critical infrastructure protection; public health and medical; emergency response and recovery; WMD detection and preparedness, and incident communications. On June 21 and 22, these groups met to develop courses of action and recommendations for the Secretary. However, the IAC Transition Team was not well integrated into the larger Federal response structure. As a result, it had difficulty receiving information and fulfilling a strategic role during the exercise.

At 9:00 a.m. on June 21, the IAC Transition Team was reported to be in a holding pattern because it had received no direct taskings. By 9:22 a.m., it developed its own planning priorities, which included NCR consequence management, incident communications, HSAS status, radiological detection, and mass evacuations.

At about 10:00 a.m., following the SVTC, the IAC was tasked to provide recommendations on resource allocation. Members discussed whether this was an appropriate tasking. They thought their role was to adjudicate resource decisions for the ESFs. However, they did not know if the NRCC was stood up at that time with all the ESFs. In fact, the NRCC was operational and was already addressing resource allocation.

By 2:02 p.m., the IAC Transition Team was focusing on what resources and capabilities that each IAC Transition Team member agency could bring to the table in preparation for the next SVTC. The IAC Transition Team representatives responded by developing lists of teams, assets, and capabilities. As discussed, the NRCC had already begun tracking and deploying assets. For example, it had already notionally activated NDMS and USAR teams and begun preparing to prestage essential commodities as described in the CIA.

Several times during the day, the IAC Transition Team participants noted problems receiving information because they were not participating in the SVTC with the Secretary and DHS leadership. Thus, they received information secondhand and much later than they expected. The ONCRC representative reported receiving more intelligence through NCR personnel working in the field than was received from the NOC. As discussed in the next section on information sharing, many participants experienced this problem. The IAC Transition Team also reported problems sharing information with their D/As because they were in a secure location where information was treated as classified and could only be shared through secure channels with cleared personnel.

Recommendations

Additional work is needed to ensure the recent updates to the NRP are transformed into an operational capability. This requires developing supporting policies and procedures and

educating the emergency response community about the role of these new structures and how they are implemented. Corrective actions are listed in Table 6.

Table 6. NRP Changes: Suggested Corrective Actions

Corrective Action	Description	Responsible Agencies	Timeline
Establish SOPs for the IAC and NOC.	Establish SOPs for the IAC, the NOC planning element, and the NOC itself, making sure to integrate those plans with any changes to COOP plans and the functionality of the COP.	DHS—Office of Operations Coordination	3 Months
Establish procedures for publicizing changes to the NRP.	Develop and establish procedures, to include associated training and education, for publicizing and institutionalizing changes to the NRP so that Federal, State, and local (FSL) officials and responders are aware of changes to the response architecture.	DHS—Preparedness Directorate & FEMA	3 Months
Develop a training and education program for the NRP.	Develop a comprehensive, continuing training and education program for the NRP that is aimed at FSL levels—both for authorities and responders.	DHS—Preparedness Directorate & FEMA	6 Months

4.1.4. The deployment of Federal and volunteer personnel was limited by WMD contamination.

According to the nuclear/radiological incident annex of the NRP, the Advisory Team for Environment, Food, and Health is responsible for providing protective action recommendations, including:

- health and safety advice or information for the public and for workers; and
- recommendations for relocation, reentry, and other radiation protective measures prior to recovery.

In this scenario, DHS and DOE, as the coordinating agency, would oversee this effort. Because the field activities in the Landport area were simulated, the Advisory Team was not fully exercised during the T4 CPX.

Summary of Issue

It was unclear who was responsible for determining what areas were considered safe when Federal D/As were making plans to deploy personnel and other resources into the affected area.

Consequences

A coordinated strategy for staging and deploying responders and ensuring they were not exposed to unsafe levels of radiological contamination was not evident during the exercise. The simulation of Federal field response teams likely contributed.

Analysis

The IMAAC distributed hazard assessment reports that modeled predictions of health effects. These analyses were intended to inform protective action recommendations and support policy making. However, no entity appeared to step in and fill this policy role. Thus, D/As were left to independently interpret this information.

For example, the American Red Cross (ARC) was concerned about the safety of volunteer personnel. ARC received several requests for assistance that included:

- sheltering attendants and family members of patients to be evacuated to 15 hospitals in the Landport area under ESF#8;
- distributing clothing to those going through decontamination sites; and
- providing support to the cities/States sheltering evacuees from the Landport area.

In the 2:00 a.m. NRCC SITREP on June 22, ARC noted that mass care assistance was limited to decontaminated individuals in areas outside of the impacted area. ARC participants also noted that life safety issues were the main operational concern of ARC Disaster Operations Center (DOC) activity leads.

Similarly, FEMA raised concerns about the NDMS and USAR teams deployed to the Landport area, many of which were notionally deployed prior to the detonation. These personnel were being staged at two mobilization centers: Ft. Lewis in Tacoma, WA, and the National Guard Base in Salem, OR. Ft. Lewis is about 130 miles from the notional city of Landport and Salem is about 50 miles away. At a 3:00 p.m. meeting on June 21, FEMA personnel discussed the safety of their responders and the need to ensure that they were not exposed to unsafe levels of radiation. At about the same time, HHS discussed the staging of NDMS teams at the Landport airport. The Landport SIMCELL told HHS that the area was safe, hut FEMA did not agree. At 7:20 p.m. that evening, FEMA told HHS that it would not support missions close to blast site and directed all assets to Ft. Lewis for staging.

Information sharing problems and exercise artificialities likely contributed to FEMA's concerns regarding personnel safety. On a 10:30 a.m. conference call with the NOC on June 21, the NRCC asked the NOC to provide a briefing on the potential impacts of a nuclear device. However, it never received a response to its request. When the NRCC had scientific questions about the detonation and the radiological contamination, there was no one present to provide an answer. These questions would have been raised to the ESF#12 liaison from DOE. However, this position was not staffed for the exercise.

Recommendations

A single point of contact should be designated as the responsible entity for providing a strategy for the deployment and staging of personnel and supplies into a potentially contaminated environment. This will ensure consistent protective actions are employed across the response effort. Suggested corrective actions are listed in Table 7.

Table 7. Response Personnel Safety: Suggested Corrective Actions

Corrective Action	Description	Lead Agency	Timeline
Clarify the responsible entity for providing guidelines for deployment into potentially contaminated areas.	Determine the responsible entity and roles of DHS/DOE and the Advisory Team for providing guidelines for deployment into potentially contaminated areas.	DHS/DOE	1 Month

4.2 Information Sharing and Maintenance of a COP

One objective of the T4 CPX was to test the ability of command/operations/intelligence centers to share intelligence and information and maintain a COP. These activities are important for maintaining a shared situational awareness among D/As and ensuring a coordinated multiagency response. The sharing of response and intelligence information is examined in this section.

4.2.1. Federal D/As and the NCR did not share situational awareness.

According to the NRP, the NOC is responsible for providing a general domestic situational awareness and a common operational picture. According to the HSOC (NOC) SOP, the NOC provides information to D/As through the following avenues:

- Existing real-time communications links
- HSIN
- Distributing warnings and bulletins
- DHS alerts (INS and HSAS level changes are listed as examples).

Summary of the Issue
Despite efforts to improve communications and information sharing across Federal D/As and with NCR organizations, they all lacked a shared situational awareness of key information during the T4 CPX. DHS is currently developing the COP, a component of HSIN, which provides a series of information screens that are designed to be displayed on a computer or projected on a display wall. The COP was not available at the time of the exercise. In addition, other methods of communicating key information did not appear to be used in place of the COP.

Consequence
Federal D/As and NCR organizations gathered information from many different sources, resulting in varied understandings about key information during the exercise.

Analysis
The Evaluation Team tracked the situational awareness of the following key pieces of information among Federal D/As:

- HSAS level changes
- Declaration of an Incident of National Significance
- Activation of the Catastrophic Incident Annex
- Presidential Disaster Declaration (PDD)

It is important to note that the first three were decisions made in SVTC meetings[12] during the exercise. Many participants in these meetings noted that formal meeting control procedures, such as preparing and distributing an agenda, preparing meeting summaries, and tracking taskings, were not used. Equipment problems also limited access for some participants, such as HHS, which did not have SVTC capability at its COOP site. The results of these meetings were not formally published and disseminated either. This resulted in participants coming out of the meetings with different understandings of what transpired and passing along different information to their D/As.

HSAS Level Change

In response to the intelligence injects, the Secretary of DHS decided to raise the HSAS level during an 8:30 a.m. SVTC that ended at approximately 9:40 a.m. Figure 3 compares the time to the first documented change in HSAS level across key Federal D/A operations centers. The figure labels show the source of the information at each location. The earliest notifications occurred at the NJIC and DoD SIMCELL. Both received phone calls from SVTC participants immediately following the meeting. The change was discussed or announced at most other locations about 45 minutes to an hour later. Some learned about it through senior leadership who had participated in the SVTC. Other D/As learned of the change through alternate sources, like the NICCL or VNN. In fact, the NJIC and NICCL calls became a good source of information for some D/As in the exercise because the NJIC conducted fact-checking exercises where it tracked and validated pieces of information. NCR participants were not notified of the HSAS level change, hut later heard about it through the press release.

All Federal D/As heard that the HSAS level was raised to Red in the NCR and Orange for the nation. As shown in Table 8, Federal D/As had inconsistent understandings of the HSAS level for Landport. The NRCC and DNDO were notified that the level was raised to Red for Landport following the SVTC, while most others assumed it to be Orange like the rest of the nation. Many of the D/As shown in the table were not notified of the Landport HSAS level being raised to Red or finally heard about it later that evening or the next day. Some D/As still did not assimilate the information even after Secretary Chertoff reported it in a statement released at 2:20 p.m. on June 21.

[12] As discussed earlier under artificialities, senior level SVTC meetings were held in place of the HSC CSG meetings because the HSC did not participate.

Figure 3. Time of First Notification of an HSAS Level Change[13]
Decision made during the 8:30 a.m. SVTC, which ended at approximately 9:40 a.m.

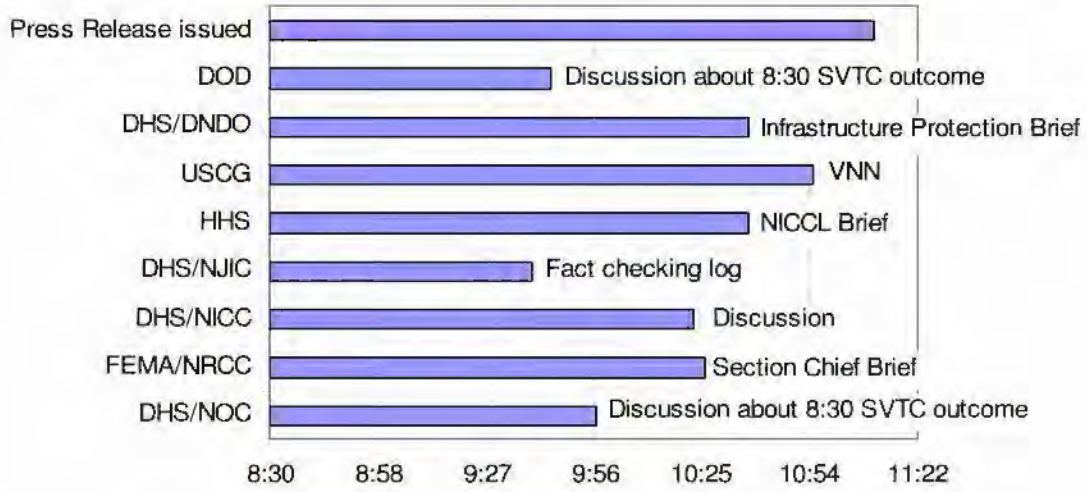


Table 8. Situational Awareness of the HSAS Level for Landport[14]

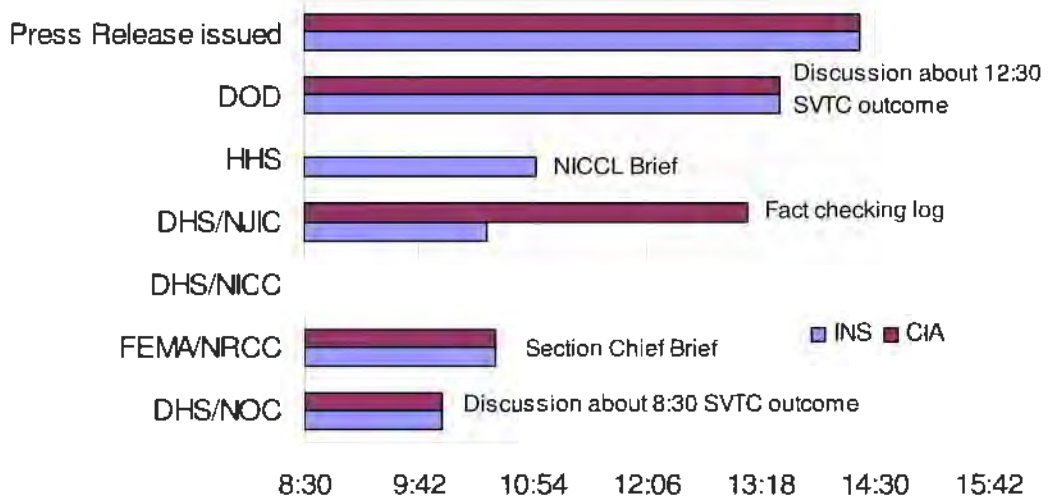
	June 21			June 22
	11:00 a.m.	3:00 p.m.	7:00 p.m.	7:00 a.m.
NOC	Orange		Red	Red
NRCC	Red	Red	Red	Red
NICC	Orange	Orange	Orange	Orange
NJIC	Orange	Red	Red	Red
HHS	Orange	Orange	Orange	
USCG	Orange			
DNDO	Red	Red	No data	No data
DoD	Orange	Orange	Orange	Orange
Public (VNN)	Yellow	Orange	Red	Red

INS and CIA
Also at the 8:30 a.m. SVTC, the Secretary of DHS decided to declare an Incident of National Significance and activate the Catastrophic Incident Annex. As shown in Figure 4, some Federal D/As experienced delays in learning about these two decisions and some never learned of it at all. More D/As knew that an Incident of National Significance was declared than knew the Catastrophic Incident Annex had been implemented. This may be because the Incident of National Significance was included on HSOC[15] and FEMA spot reports, the earliest of which was recorded at 11:30 a.m. on June 21.

[13] See Appendix A for a list of acronyms.
[14] See Appendix A for a list of acronyms. Blank spaces indicate that it is unclear what the HSAS was thought to be at that time in that location because it was not recorded in the data. "No data" indicates a time when data were not available for that location.
[15] The title on the spot reports had not yet been changed to the NOC.

Figure 4. Time of First Notification of an Incident of National Significance and Catastrophic Incident Annex[16]

Decision made during the 8:30 a.m. SVTC, which ended at approximately 9:40 a.m.

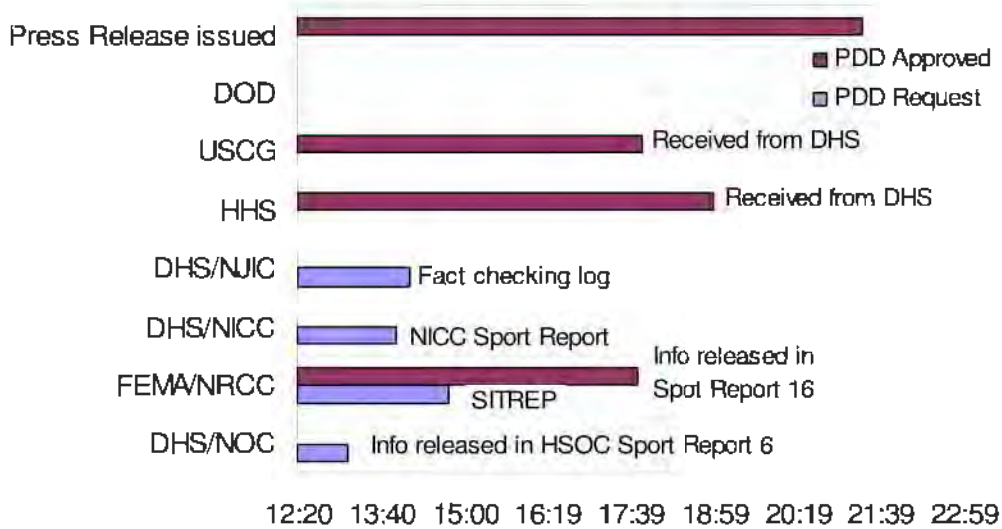


PDD

As shown in Figure 5, several Federal D/As did not hear about the PDD even though it was documented in NRCC Spot Report 16. This indicates that either the spot report was not disseminated widely or it was not read and assimilated by all of the receiving D/As. There was a significant time lag between the simulated request by the governor and tbe PDD. During this time, we recorded numerous conversations where personnel were wondering if the president had declared it a disaster. The delay is likely due to exercise control staff, as the final decision by the White House had to be simulated.

Figure 5. Time of First Notification of PDD Request and PDD[17]

PPD requested at 12:20 and approved at 17:00



[16] See Appendix A for an acronym list.
[17] See Appendix A for an acronym list.

Recommendations

The COP has the potential to improve information sharing and situational awareness across FSL D/As. DHS should ensure that D/As are able to access and use the system, that there are redundant methods for sharing information, and that D/As are able to assimilate this information into a shared situational awareness. Suggested corrective actions are listed in Table 9.

Table 9. Situational Awareness: Suggested Corrective Actions

Corrective Action	Description	Responsible Agencies	Timeline
Finish development and deployment of the COP.	Finish development and deployment of the COP system for use in the NOC.	DHS—Office of Operations Coordination	Ongoing
Develop parameters and standards for the COP, to include Spot Reports and SITREPS.	Develop parameters and standards so that D/As have established guidelines for accessing and contributing to the COP; development of these standards should be integrated with work on D/A-specific policies and procedures for HSIN.	DHS—NOC & Interagency	Ongoing
Establish Video Teleconference protocols for Incidents of National Significance.	Establish protocols for the use of SVTC during Incidents of National Significance to ensure that the necessary officials are included in the conferences and agendas, and to ensure that summaries of conclusions are distributed to all attendees.	DHS—Executive Secretary & Office of Operations Coordination	3 Months
Develop D/A-specific policies and procedures for HSIN.	Individual D/As should develop their own policies and procedures for the use of HSIN during a crisis and use those procedures during subsequent exercises.	DHS—NOC & Interagency	1 Year
Conduct a feasibility study of integrating HSIN with web-EOC.	Conduct a study of the integration of the two information-sharing systems—HSIN and web-EOC—so that FSL governments have access to the same information.	DHS—Preparedness Directorate & SLGC	1 Year

4.2.2. Intelligence was not consistently shared across Federal D/As and the NCR.

Summary of the Issue

There were differences in the intelligence information available at Federal D/As and within the NCR during the exercise. Whereas some received detailed information about the threat in the NCR and Landport, others received little or no information. The location of personnel in secure and nonsecure sites contributed to these problems because classified information can only be transferred through secure phones or computer systems. Even when personnel in nonsecure sites had clearance to receive the information, they often did not have access to secure phones or computer systems.

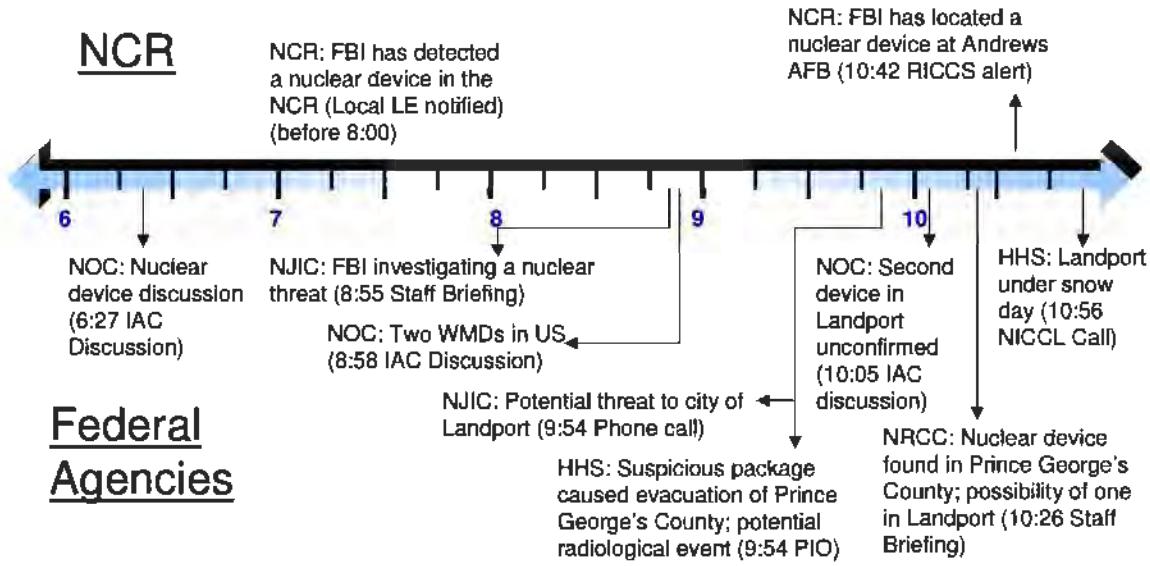
Consequence

The ability of some Federal D/As and the NCR to take protective actions and prepare to respond to a nuclear/radiological incident was impacted by the lack of information.

Analysis

Figure 6 shows excerpts of discussions and communications recorded at several locations during the exercise. The NOC was a secure site and personnel working there knew they had relocated because of a nuclear threat to the NCR. The other Federal sites were not equipped to handle classified information and personnel working there were not immediately aware of the nature of the threat and why they had relocated. By midmorning, however, all had heard that they were dealing with a nuclear/radiological threat. This information came from many different sources and was not formally disseminated. Some of it could be the result of leaks in the exercise scenario.

Figure 6. Information Known about the Threat



The FBI told NCR law enforcement officials very early on June 21 that a nuclear device had been located in the NCR. They passed this information to their senior officials, who attempted to get official notification from the NOC through the ONCRC and G&T. According to existing procedures for intelligence dissemination, the intelligence community members disseminate their information to the NOC. The NOC is then responsible for packaging the information at the various classification levels necessary for use by State/local customers, as well as other Federal agencies.[18] Although a request for information was made to the NOC, it is unclear why no information was released to the NCR.[19]

[18] Memorandum from Russell Schweikhard, Central Intelligence Agency, July 13, 2006.
[19] Our evaluation plan did not include the collection of data on classified processes and procedures.

Many participants said that the lack of intelligence hindered their ability to take protective measures and to respond appropriately. For example, HHS personnel had no information on the threat at the time their COOP site was activated and only learned through their PIO that there was a potential radiological event. In an 11:00 a.m. conference call with the DHS chief medical officer, HHS said that it was not informed of any intelligence information and was now 14 hours behind curve in terms of preparing to respond. NCR officials raised similar concerns and noted that the lack of intelligence limited their planning activities and ability to take protective measures. As discussed earlier, operational security concerns are one reason that intelligence sharing might be limited. The protection of sources is another.

Also contributing to information sharing problems was that personnel were located in a variety of secure and nonsecure sites. For example, personnel with the IAC operated from a secure site where all the information they received was treated as classified. Thus, they could only pass information to their D/As through secure channels such as secure telephones or computer systems. Personnel receiving this information also needed proper clearance. However, even when personnel with the clearances were available, they often did not have the equipment necessary to receive classified information.

Many participants noted that much of the information available in secure sites or on secure systems was unclassified, but personnel could not easily have this information downgraded to pass on. For example, the NICC said that information that was unclassified or classified at a low level was carried on systems with higher classifications that required arduous processes to move the information to systems where information sharing and visibility would be higher. It was unclear even with unclassified products whether they were cleared or not for release to the general public or private sector critical infrastructure and key resource partners (i.e., trusted industry community).

Related to this issue, the NICC received numerous requests for information from the private sector. Because much of the information it was receiving came over classified systems, it could not easily downgrade this information for dissemination to private sector organizations. The NICC does not typically coordinate with the NJIC, so it did not have ready access to fact sheets and talking points to distribute to its private sector partners.[20] It is important to note that the NJIC typically coordinates with the DHS Private Sector Office, which then provides information such as fact sheets and talking points to the private sector. However, during the CPX, the DHS Private Sector Office did not participate at the NJIC, which may have exacerbated this prohlem.

Recommendations

Coordinate with the intelligence community to further assess and address intelligence sharing. Improve coordination between the NICC and NJIC during emergencies to ensure information is disseminated to private sector organizations. Suggested corrective actions are listed in Table 10.

[20] The NICC and the NJIC have identified this as a potential problem and are identifying solutions.

Table 10. Intelligence Sharing: Suggested Corrective Actions

Corrective Action	Description	Responsible Agencies	Timeline
Review intelligence sharing procedures.	Review intelligence sharing procedures and the role of the NOC to ensure that potential blockages in information flow are addressed.	DHS—NOC OI&A	6 Months
Develop reachback alternatives for senior leadership.	Investigate alternative approaches to providing leadership officials in COOP facilities access to reachback and additional support capabilities and resources.	DHS—Preparedness Directorate & NOC	3 Months
Ensure that COOP facilities have SCIFs and can share information at the same level of classification.	For information-sharing purposes, ensure that COOP facilities, that have mission essential tasks that require TS/SCI information, have SCIFs with SIPRNET and DSN access.	DHS—Preparedness Directorate & NOC	12 Months
Develop a process for linking the NICC with public messaging during an emergency.	Develop protocols that describe NJIC and NICC communication and coordination in public messaging to ensure necessary information reaches the private sector.	DHS—Preparedness Directorate, AS Public Affairs & NOC	6 Months

4.3 Public Information

The term "emergency public information" reflects an understanding that public information during an emergency might differ from normal, day-to-day, public information provided to citizens by the government. In the event of a major disaster or emergency, this often means the coordination, development, and delivery of time-critical, lifesaving information to all potentially affected people. For this reason, public officials and government spokespersons often find that this aspect of their jobs is different in an emergency environment, and more important. In a climate of heightened uncertainty and concern, the timing and content of official statements can save lives, the media and general public are likely to scrutinize statements more, and some statements could incur heightened political liabilities.

During the T4 CPX, the NRP was employed and ESF #15 was activated. Federal D/As set up a NJIC and activated the NICCL for communication and coordination of public information. Table 11 shows the D/As that staffed the NJIC and those that issued press releases. In parentheses are the total numbers of press releases issued during the CPX. It is important to note that there was limited participation from the NCR and no real or simulated participation from State and local public affairs communities representing Landport or Central Pacifica.

CPX media play consisted of VNN broadcasts, the VNN.com website, and a media SIMCELL. As they have done in past TOPOFF exercises, VNN maintained an exercise website with articles and video clips about the exercise world. It also posted Federal D/As press releases on the website. The media SIMCELL represented a news wire service. The media SIMCELL made phone calls to Federal D/As, including the NJIC, and conducted mock interviews. They logged those calls and responses to their questions, and provided an hourly update to the MCC. Especially newsworthy information was provided as learned to VNN through the VNN controller, but the SIMCELL operated independently from VNN.

Table 11. D/A Public Affairs Participation during the T4 CPX

D/A	Represented at the NJIC	Issued Press Release
DHS	X	X (11)
HHS	X	X (2)
FEMA	X	X (2)
USDA	X	
OPM	X	
DOJ	X	X (1)
FBI	X	X (1)
BLM		X (3)
DOE		X (1)
FCC		X (4)
DOD (JTF-NCR)		X (2)
NRC		X (3)
NTSB		X (1)
NCR	X (participated in NICCL calls)	
Landport/CP		

4.3.1. Conflicting guidance was provided to Federal government employees and the public before the WMD blast.

Summary of Issue

One of the most important requirements during emergencies is to provide the public with protective action guidance. During the T4 CPX, conflicting protective action guidance was provided to Federal government employees and the public in the NCR and in Landport before the WMD blast. However, that after the WMD blast in Landport, Federal D/As provided consistent information and guidance to the public.

Consequence

Given the conflicting information provided to the public and government employees in the NCR, the likely outcome would be additional confusion in the NCR and in Landport before the WMD blast and frustration with the Federal D/As.

Although it is significant that Federal D/As were able to "speak with one voice" to the public after the WMD blast in Landport, it is important to recognize that in a real WMD emergency, the

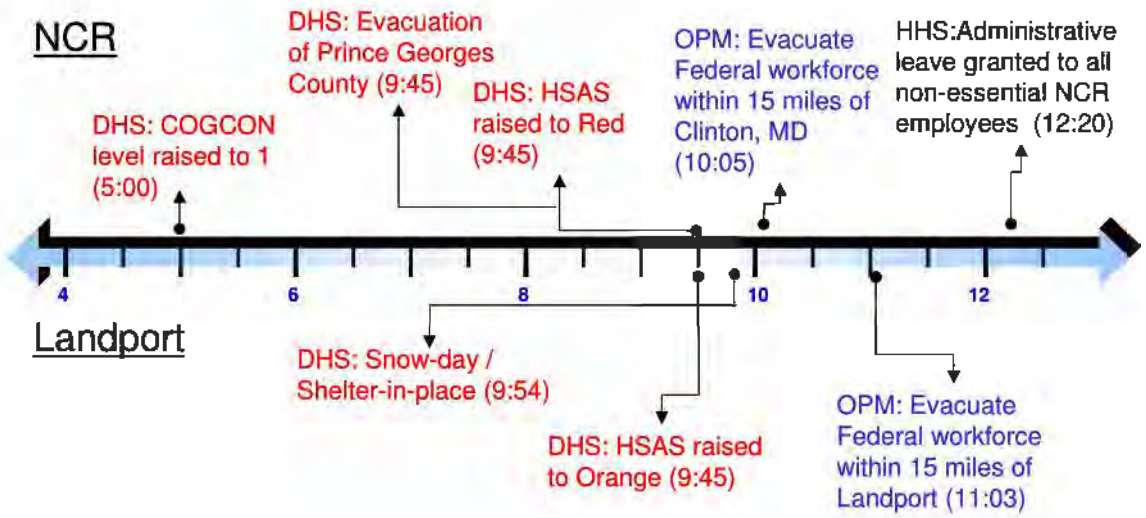
public will look to their State and local governments first for protective action guidance. Therefore, Federal D/A guidance must also be consistent with that provided by the State and local public affairs agencies. This has proved to be a significant challenge in previous TOPOFF exercises and was not examined during the T4 CPX.

Analysis

During the T4 CPX, conflicting protective action guidance was provided to Federal government employees and the public in the NCR and in Landport before the WMD blast. This is shown in Figure 7.

The COGCON level was raised to 1 at 5:00 a.m. on June 21. OPM did not release nonessential government employees at this time. Instead, the decision was left to the individual D/As. This caused concern among officials at several D/As. For example, FEMA officials discussed what to do with their nonessential personnel but took no further action; DOT officials discussed whether this was a Federal or OPM decision, as there were no requests for Federal assistance. As far as the evaluation team could determine, the only D/A to take official action was HHS, which decided to grant administrative leave to their employees in the NCR at 12:20 p.m. Clear guidance or direction from OPM when the COGCON level was raised to 1 could have alleviated this concern.

Figure 7. Protective Action Guidelines

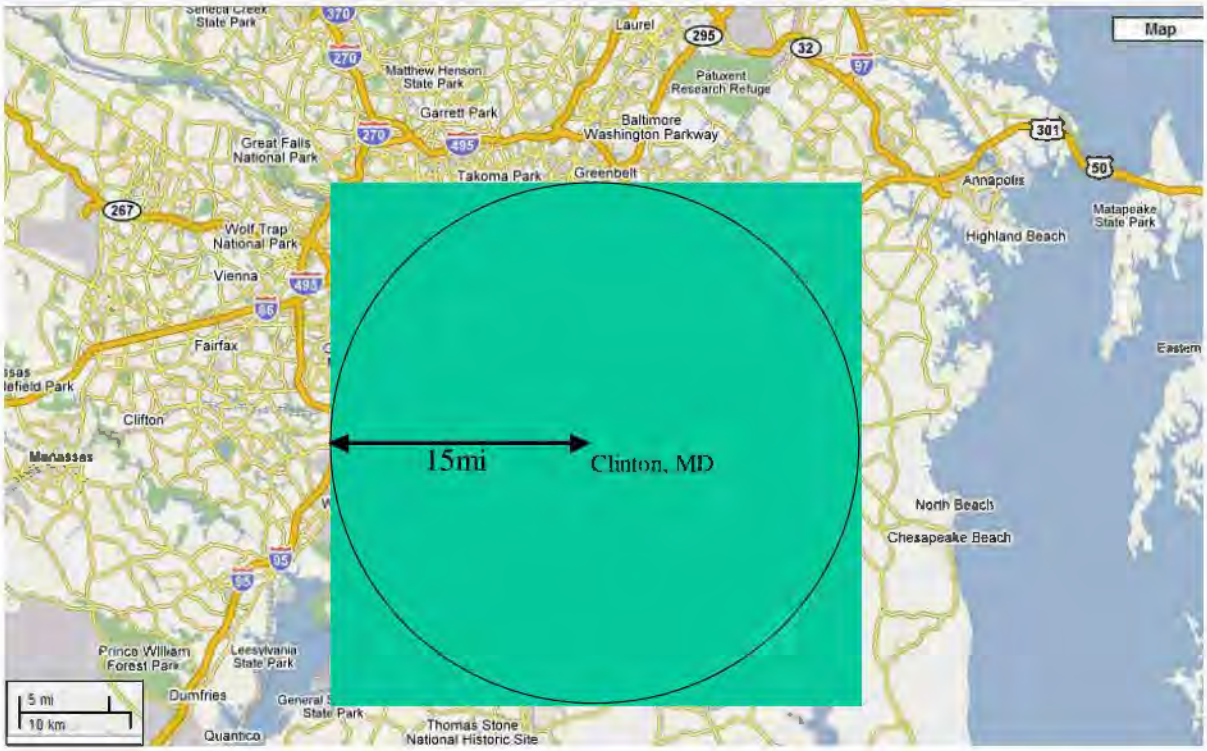


At 9:45 a.m., the HSAS level was raised to Red in the NCR, and the Federal government recommended that Prince George's County be evacuated. At 10:05 a.m., OPM directed the Federal workforce to evacuate only within a portion of the county—15 miles around Clinton, MD. Notably, an evacuation area of this size includes several additional counties, including portions of Fairfax and Arlington Counties in Virginia, and portions of Washington, DC, including the White House (see Figure 8). In a real emergency, these inconsistencies would have

likely been observed and reported upon by the media, subsequently causing concern and confusion among the public.

Shortly after the HSAS level was raised to orange at 9:45 a.m., the NJIC began working on a public statement for Landport residents to shelter-in-place. At 11:03 a.m., OPM directed all Federal employees within 15 miles of Landport to evacuate.[21] The evaluation team has no data to show that the same recommendation was passed along to the public. This certainly is a cause for concern because, in a real emergency, Federal employees evacuating a city would not escape the notice of the media or the public. An emergency alert system (EAS) message was sent out after the blast.

Figure 8. Evacuation Area around Clinton, MD



Although there is a balance between protecting operational security and providing information to the public, information passed to nonessential government personnel, at a minimum, must also be relayed to the public. In practical terms, the government workers are going to call their families, inevitably alerting the public that something unusual is occurring.

The protective action guidance issued by the Federal D/As after the detonation in Landport was consistent. For example, in a press release just after the WMD blast, DHS referred directly to the CDC protective action recommendation. In addition, in a statement by the DHS Secretary at 10:30 a.m. on June 22, he described assets that had deployed to Landport and activities undertaken and repeated the recommended protective action guidelines. The information in this statement was consistent with press releases by each individual D/As made the day prior.

[21] Participants could have been acting on information leaked from the exercise scenario when making this decision.

Although it is significant that Federal D/As were able to maintain a consistent message to the public, in a real WMD emergency, the State and local protective action guidelines would also have to be consistent. This significant challenge was not addressed in the CPX.

Recommendations

Federal D/A guidance must be consistent with that provided by the State and local public affairs agencies. This has proved to a significant challenge in previous TOPOFF exercises and was not examined during the T4 CPX. This issue should be readdressed during the full-scale exercise. Suggested corrective actions are listed in Table 12.

Table 12. Public Information: Suggested Corrective Actions

Corrective Action	Description	Responsible Agencies	Timeline
Analyze options for a dynamic public messaging system and integrate with IPAWS work.	During a WMD event, different protective actions may need to be taken by the public, depending on where they are located. For instance, those in the fallout plume need to evacuate, while most others should shelter-in-place. Undertake an analysis of alternative means of delivering prescripted risk messages to different geographic segments of a population in order to communicate tailored recommendations for protective measures. This work should be integrated with the ongoing IPAWS initiative.	DHS—FEMA & DOC—NOAA	Ongoing
Standardize leave policy for nonessential government personnel in an emergency.	OPM should standardize emergency leave policy for nonessential government personnel with an elevation to COGCON Level 1 so that it is consistent among all D/As and is also consistent with expected guidance to the public.	OPM	3 Months
Develop D/A-specific HSAS playbooks.	Each D/A develop criteria/playbooks that outline what happens internally to their organizations when the HSAS threat level is raised.	DHS & Interagency	6 Months

5.0 CONCLUSIONS

The evaluation of the exercise focused on three general areas: WMD response, situational awareness and information sharing, and public information. Within each of these areas, several key issues emerged and are addressed in this AAR.

Focus Areas and Key Issues

WMD response
• Some predetonation decisions/actions may have compromised operational security. • Protective actions/recommendations were not coordinated with State and local governments. • The May 25 NRP notice of change was not fully implemented. • The deployment of Federal and volunteer personnel was limited by WMD contamination.
Situational awareness and information sharing
• Federal D/As and the NCR did not share situational awareness. • Intelligence was not consistently shared across Federal D/As and the NCR.
Public information
• Conflicting guidance was provided to Federal government employees and the public before the WMD blast.

Exercise artificialities and implementation issues affected the exercise and the key issues discussed in this report. Most notably, there was limited participation by the White House and HSC in the exercise itself, which affected decision-making and coordination. In addition, other artificialities limited Federal interagency and Federal-NCR coordination.

Many of these issues were raised in past TOPOFF exercise and/or were noted during the response to Hurricane Katrina. Appendix B of this report includes a Corrective Action Plan focused on addressing these issues.

APPENDIX A: ACRONYM LIST

ACRONYM	DESCRIPTION
AAR	AFTER-ACTION REPORT
ARC	AMERICAN RED CROSS
CBP	CUSTOMS AND BORDER PATROL
CDC	CENTERS FOR DISEASE CONTROL
CIA	CATASTROPHIC INCIDENT ANNEX
COA	COURSE OF ACTION
COGCON	CONTINUITY OF GOVERNMENT CONDITION
CONPLAN	CONCEPT OF OPERATIONS PLAN
COOP	CONTINUITY OF OPERATIONS
COP	COMMON OPERATING PICTURE
CP	CENTRAL PACIFICA
CPX	COMMAND POST EXERCISE
CSG	COUNTERTERRORISM SUPPORT GROUP
D/AS	DEPARTMENTS AND AGENCIES
DHS	DEPARTMENT OF HOMELAND SECURITY
DMAT	DISASTER MEDICAL ASSISTANCE TEAM
DMORT	DISASTER MORTUARY OPERATIONS RESPONSE TEAM
DNDO	DOMESTIC NUCLEAR DETECTION OFFICE
DOC	DISASTER OPERATIONS CENTER
DOD	DEPARTMENT OF DEFENSE
DOE	DEPARTMENT OF ENERGY
DOJ	DEPARTMENT OF JUSTICE
DOT	DEPARTMENT OF TRANSPORTATION
EOC	EMERGENCY OPERATIONS CENTER
ERT-N	EMERGENCY RESPONSE TEAM- NATIONAL
ESF	EMERGENCY SUPPORT FUNCTION
EXPLAN	EXERCISE PLAN
FBI	FEDERAL BUREAU OF INVESTIGATION
FC 06	FORWARD CHALLENGE 2006
FCC	FEDERAL COMMUNICATIONS COMMISSION
FEMA	FEDERAL EMERGENCY MANAGEMENT AGENCY
FIRST	FEDERAL INCIDENT RESPONSE SUPPORT TEAM
FSL	FEDERAL, STATE, AND LOCAL
HHS	DEPARTMENT OF HEALTH AND HUMAN SERVICES
HSAS	HOMELAND SECURITY ADVISORY SYSTEM
HSC	HOMELAND SECURITY COUNCIL
HSEEP	HOMELAND SECURITY EXERCISE AND EVALUATION PROGRAM
HSIN	HOMELAND SECURITY INFORMATION SYSTEM
HSOC	HOMELAND SECURITY OPERATIONS CENTER
HSPD-5	HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 5
IAC	INCIDENT ADVISORY COUNCIL

IIMG	INTERAGENCY INCIDENT MANAGEMENT GROUP
IMAAC	INTERAGENCY MODELING AND ATMOSPHERIC ASSESSMENT CENTER
IND	IMPROVISED NUCLEAR DEVICE
INS	INCIDENT OF NATIONAL SIGNIFICANCE
JTF	JOINT TASK FORCE
MC 06-02	MARBLE CHALLENGE 2006-02
MCC	MASTER CONTROL CELL
MSEL	MASTER SCENARIO EVENTS LIST
NARAC	NATIONAL ATMOSPHERIC RELEASE ADVISORY CENTER
NCR	NATIONAL CAPITAL REGION
NDMS	NATIONAL DISASTER MEDICAL SYSTEM
NIAC	NATIONAL INFRASTRUCTURE ADVISORY COUNCIL
NICC	NATIONAL INFRASTRUCTURE COORDINATION CENTER
NICCL	NATIONAL INCIDENT COMMUNICATIONS CONFERENCE LINE
NIMS	NATIONAL INCIDENT MANAGEMENT SYSTEM
NJIC	NATIONAL JOINT INFORMATION CENTER
NOC	NATIONAL OPERATIONS CENTER
NPS	NATIONAL PLANNING SCENARIO
NRC	NUCLEAR REGULATORY COMMISSION
NRCC	NATIONAL RESPONSE COORDINATION CENTER
NRP	NATIONAL RESPONSE PLAN
NTSB	NATIONAL TRANSPORATION SAFETY BOARD
ONCRC	OFFICE OF NATIONAL CAPITAL REGION COORDINATION
OPM	OFFICE OF PERSONNEL MANAGEMENT
OSLGC	OFFICE OF STATE AND LOCAL GOVERNMENT COORDINATION
PDD	PRESIDENTIAL DISASTER DECLARATION
PFO	PRINCIPAL FEDERAL OFFICIAL
PIO	PUBLIC INFORMATION OFFICER
RDF	RAPID DEPLOYMENT FORCE
SCIF	SECURE COMPARTMENTALIZED INFORMATION FACILITY
SIMCELL	SIMULATION CELL
SITREP	SITUATION REPORT
SNS	STRATEGIC NATIONAL STOCKPILE
SOE	SENIOR OFFICIALS EXERCISES
SOP	STANDARD OPERATING PROCEDURE
SVTC	SECURE VIDEO CONFERENCE
T3	TOP OFFICIALS EXERCISE 3
T4	TOP OFFICIALS EXERCISE 4
TARU	TECHNICAL ASSISTANCE RESPONSE UNIT
TOPOFF	TOP OFFICIALS EXERCISE
UA	UNIVERSAL ADVERSARY
US&R	URBAN SEARCH AND RESCUE
USAR	URBAND SEARCH AND RESCUE
USCG	UNITED STATES COAST GUARD

USDA	UNITED STATE DEPARTMENT OF AGRICULTURE
USTRANSCOM	UNITED STATES TRANSPORTATION COMMAND
VNN	VIRTUAL NEWS NETWORK
WMD	WEAPONS OF MASS DESTRUCTION

APPENDIX B: CORRECTIVE ACTION PLAN

These actions were developed in coordination with a small group of interagency T4 CPX planners. They are intended to be further refined by DHS and the larger interagency into a corrective action plan.

Corrective Action	Description	Responsible Agencies	Timeline
EXERCISE PARTICIPATION			
Conduct pre-exercise training and education for senior leadership.	Conduct training and education for senior leaders prior to the next FSE to ensure they are engaged and have full awareness of their anticipated role.	DHS—Preparedness Directorate	6 Months
Write exercise CONPLANs for senior leadership.	Write a concept of operations (CONPLAN) for the next FSE. Senior leadership would be the target audience, and the intent would be to provide them with a description of their roles and responsibilities during the exercise.	DHS—Preparedness Directorate	6 Months
Expand exercise participant training.	Expand the training and information materials provided to players and field controllers to ensure they are aware of the expectations for coordination and interaction with participating and simulated organizations.	DHS—Preparedness Directorate	12 Months
OPERATIONAL SECURITY			
Develop alternatives to COGCON Level 1 in the COOP architecture.	Consider alternatives to COGCON level 1, such as creating operational depth by ensuring that geographically dispersed individuals are trained to carry out COOP roles and responsibilities or using devolution in place of moving all essential personnel.	DHS—FEMA	12 Months
Create additional measures in COOP plans to minimize impact on local communities.	Additional measures should be added to COOP plans to account for a deployment's impact on the local economy and infrastructure and for the logistical challenges associated with deployment. MOUs should be signed with the host communities.	DHS—FEMA	6 Months
Develop interagency playbook for NRP.	Develop interagency playbook for the NRP. This would be a companion piece to the NRP that would be prescripted with operational security considerations, user checklists, have a common set of questions, and would also be developed for the 15 National Planning Scenarios.	DHS—Preparedness Directorate	9 Months
Write operational plans for catastrophic scenarios.	Write specific operational plans that would complement the operational framework contained in the Catastrophic Incident Annex of the NRP and address operational security in specific scenarios.	DHS—NOC Planning Element	1 Year

Corrective Action	Description	Responsible Agencies	Timeline
COORDINATING PROTECTIVE ACTIONS			
Collaborate with the NCR to address protective action coordination.	Conduct exercises, workshops, and/or plan reviews in coordination with the NCR to ensure that Federal government plans for evacuation and other protective actions are fully synchronized with NCR plans.	DHS—Preparedness	6 Months
NRP CHANGES			
Establish SOPs for the IAC and NOC.	Establish SOPs for the IAC, the NOC Planning Element, and the NOC itself, making sure to integrate those plans with any changes to COOP plans and the functionality of the COP.	DHS—Office of Operations Coordination	3 Months
Establish procedures for publicizing changes to the NRP.	Develop and establish procedures, to include associated training and education, for publicizing and institutionalizing changes to the NRP so that FSL officials and responders are aware of changes to the response architecture.	DHS—Preparedness Directorate & FEMA	3 Months
Develop a training and education program for the NRP.	Develop a comprehensive, continuing training and education program for the NRP that is aimed at FSL levels—both for authorities and responders.	DHS—Preparedness Directorate & FEMA	6 Months
PERSONNEL SAFETY			
Clarify the responsible entity for providing guidelines for deployment into potentially contaminated areas.	Determine the responsible entity and roles of DHS/DOE and the Advisory Team for providing guidelines for deployment into potentially contaminated areas.	DHS/DOE	1 Month
SITUATIONAL AWARENESS			
Finish development and deployment of the COP.	Finish development and deployment of the COP system for use in the NOC.	DHS—Office of Operations Coordination	Ongoing
Develop parameters and standards for the COP, to include spot reports and SITREPS.	Develop parameters and standards so that D/As have established guidelines for accessing and contributing to the COP; development of these standards should be integrated with work on D/A-specific policies and procedures for HSIN.	DHS—NOC & Interagency	Ongoing
Establish video teleconference protocols for Incidents of National Significance.	Establish protocols for the use of SVTC during Incidents of National Significance to ensure that the necessary officials are included in the conferences and agendas, and to ensure that summaries of conclusions are distributed to all attendees.	DHS—Executive Secretary & Office of Operations Coordination	3 Months

Corrective Action	Description	Responsible Agencies	Timeline
Develop D/A-specific policies and procedures for HSIN.	Individual D/As should develop their own policies and procedures for the use of HSIN during a crisis and use those procedures during subsequent exercises.	DHS—NOC & Interagency	1 Year
Conduct a feasibility study of integrating HSIN with web-EOC.	Conduct a study of the integration of the two information-sharing systems—HSIN and web-EOC—so that FSL governments have access to the same information.	DHS—Preparedness Directorate & SLGC	1 Year
INTELLIGENCE SHARING			
Review intelligence sharing procedures.	Review intelligence sharing procedures and the role of the NOC to ensure that potential blockages in information flow are addressed.	DHS—NOC	6 Months
Develop reachback alternatives for senior leadership.	Investigate alternative approaches to providing leadership officials in COOP facilities access to reachback and additional support capabilities and resources.	DHS—Preparedness Directorate & NOC	3 Months
Ensure that all COOP facilities have SCIFs and can share information at the same level of classification.	For information-sharing purposes, ensure that all COOP facilities have SCIFs with SIPRNET and DSN access. Also ensure that all COOP facilities are cleared for the same level of classification to meet operational requirements.	DHS—Preparedness Directorate & NOC	12 Months
Develop a process for linking the NICC with public messaging during an emergency.	Develop protocols that describe NJIC and NICC communication and coordination in public messaging to ensure necessary information reaches the private sector.	DHS—Preparedness Directorate & AS Public Affairs	6 Months
PUBLIC INFORMATION			
Analyze options for a dynamic public messaging system and integrate with IPAWS work.	During a WMD event, different protective actions may need to be taken by the public, depending on where they are located. For instance, those in the fallout plume need to evacuate, while most others should shelter-in-place. Undertake an analysis of alternative means of delivering prescripted risk messages to different geographic segments of a population in order to communicate tailored recommendations for protective measures. This work should be integrated with the ongoing IPAWS initiative.	DHS—FEMA & DOC—NOAA	Ongoing
Standardize leave policy for nonessential government personnel in an emergency.	OPM should standardize emergency leave policy for nonessential government personnel with an elevation to COGCON Level 1 so that it is consistent among all D/As and is also consistent with expected guidance to the public.	OPM	3 Months

Corrective Action	Description	Responsible Agencies	Timeline
Develop D/A-specific HSAS playbooks.	Each D/A develop criteria/playbooks that outline what happens internally to their organizations when the HSAS threat level is raised.	DHS & Interagency	6 Months

APPENDIX C: COMPILATION OF D/A LESSONS LEARNED

The following table shows the list of participating agencies. "QL" indicates those that commented on the quick look report, "LL" indicates those that submitted lessons learned, and "DC" indicates those that had a data collector or member of the CPX Evaluation Team present at their location. **WE ALSO NEED TO INSERT THE LESSONS LEARNED HERE OR REFERENCE HOW THEY WILL BE PUBLISHED.**

Agency	QL	LL	DC
American Red Cross	X	X	
Central Intelligence Agency	X	X	
Defense Information Systems Agency			
Department of Agriculture			
Department of Commerce			
Department of Defense		X	
• Office of the Secretary of Defense	X		
Department of Education			
Department of Energy	X	X	X
Department of Health and Human Services			X
Department of Homeland Security			X (IAC, NJIC, NICC)
• FEMA			X (NRCC)
• Civil Rights and Liberties	X		
• Domestic Nuclear Detection Office	X	X	X
• Immigration and Customs Enforcement		X	
• Preparedness Directorate	X	X	
• National Communications System		X	
• Office of Science and Technology			
• Transportation Security Administration			
• U.S. Citizenship and Immigration Services			
• U.S. Coast Guard		X	X
• U.S. Customs and Border Protection			
• U.S. Secret Service			
Department of Housing and Urban Development	X	X	
Department of Interior			
Department of Justice			
• FBI			
• Criminal Division Counter Terrorism Section			
• Alcohol, Tobacco, Firearms, and Explosives			
• U.S. Marshals Service			
Department of Labor	X	X	
Department of State	X	X	
Department of the Treasury			
Department of Transportation			
• Federal Aviation Administration			
Department of Veterans Affairs			X

Environmental Protection Agency			
Executive Office of the President			
• Office of Science and Technology Policy			
Export-Import Bank of the US			
Federal Communications Commission	X		
Federal Reserve System			
General Services Administration	X		
Internal Revenue Service			
Landport SIMCELL Collective	X		
National Archives and Records Administration			
National Capital Region	X	X	
• DCEMA			X
• Virginia DEM			
• MEMA			
• Supporting Jurisdictions and Agencies			
National Labor Relations Board			
National Science Foundation	X	X	
National Transportation Safety Board			
Nuclear Regulatory Commission			
Office of Personnel Management			
Office of the Director of National Intelligence			
Office of the U.S. Courts			
Peace Corps			
Pension Benefit Guaranty Corporation			
Securities and Exchange Commission			
Small Business Administration			
Social Security Administration	X	X	
US Agency for International Development			
US Army Corps of Engineers			
US House of Representatives			
US Postal Service	X	X	
US Senate Office of the Sergeant at Arms			

APPENDIX D: REFERENCES

1. Department of Homeland Security, *Top Officials (TOPOFF) 4 (T4) Command Post Exercise (CPX) Exercise Plan (EXPLAN)*, June 2006.
2. Department of Homeland Security, *SOE 05-4, "Vulcan Warrior," After-Action Report (AAR).*
3. Department of Homeland Security, *National Response Plan*, December 2004.
4. Department of Homeland Security, *Notice of Change to the National Response Plan*, May 25, 2005.
5. Department of Homeland Security. *Interagency Integrated Standard Operating Procedure, Homeland Security Operations Center (HSOC), Version 5.0*, August 2005.

APPENDIX E: HSAS CONDITIONS

Threat Conditions	Procedures/Guidelines
Green (low), Blue (guarded), Yellow (elevated)	Under Threat Conditions Green through Yellow, the HSOC maintains direct connectivity with the NCTC and the FBI SIOC regarding the terrorist threat and maintains situational awareness through the continued monitoring of reported incidents.
Orange (high)	When threat conditions warrant, DHS activates the IIMG to review the threat information, coordinate interagency activity, and recommend additional precautions needed to prevent, prepare for, or respond to an attack. If the threat is elevated regionally or locally, DHS considers designating a PFO and activating emergency response teams and appropriate RRCC(s) to coordinate with regional, State, and private-sector entities and notify (or activate) regional resources (such as the ERT) as appropriate.
Red (severe)	When threat conditions warrant, DHS fully activates the NRCC, activates the RRCCs in the designated threat locations, implements Continuity of Operations plans, and places other appropriate assets on the highest alert status. If the threat is elevated regionally or locally, the IIMG provides recommendations for the deployment of special teams to the area and establishment of a JFO. In the absence of a JFO, special teams deployed in response to a terrorist threat operate in coordination with the FBI JOC.

APPENDIX F: COOP AND COGCON MATRIX

DEPARTMENT AND AGENCY COOP ALERT & DEPLOYMENT OPTIONS

Department & Agency (D/A) Continuity of Operations (COOP)	"GUARDED" Level of Concern "HIGH"			
	COGCON 4	COGCON 3	COGCON 2	COGCON 1
Operations	• Continue to perform headquarters business functions at normal location(s) • Maintain alternate operating facility(ies) in accordance with agency COOP plans to ensure ready for activation at all times • Conduct training and exercise activities in accordance with agency COOP and TTE plan(s) to ensure personnel readiness	• Continue to perform headquarters business functions at normal location(s) • Maintain alternate operating facility(ies) in accordance with agency COOP plans to ensure ready for activation at all times • Conduct additional training activities to increase personnel readiness (e.g. Team tabletops, review recall lists, review plans and procedures)	• Continue to perform headquarters business functions at normal location(s) • Monitor/track major HQ activities • Maintain alternate operating facility(ies) in accordance with agency COOP plans to ensure ready for activation at all times • Take appropriate steps to ensure alternate operating facility(ies) can be activated with 4 hours notice	• Continue to perform headquarters business functions at normal location(s) • Monitor/track major HQ activities • Perform day-to-day functions at alternate facility(ies) as appropriate • Take appropriate steps to ensure alternate operating facility(ies) can be activated with no notice
Staffing Level	• No staffing required at alternate operating facility(ies) • Maintain normal delegations and devolution of authority to ensure performance of essential functions in no notice event	• No staffing required at alternate operating facility(ies) unless necessary to meet 8-hour operational requirement. • Maintain normal delegations and devolution of authority to ensure performance of essential functions in no notice event	• Deploy sufficient staff to alternate operating facility(ies) to allow activation with 4 hours notice	• Deploy sufficient staffing to alternate operating facility(ies) to perform essential functions with no notice

DEPARTMENT AND AGENCY COOP ALERT & DEPLOYMENT OPTIONS

Department & Agency (D/A) Continuity of Operations (COOP)	"GUARDED" Level of Concern "HIGH"			
	COGCON 4	COGCON 3	COGCON 2	COGCON 1
Communications	• Test all internal agency communications capabilities between normal operating locations (HQ and other) and alternate operating facility(ies) no less than quarterly • Test all communications capabilities at all alternate operating facility(ies) with applicable interagency partners no less than quarterly (e.g. participate in Title Globe)	• Conduct at least one additional internal agency communications test between normal operating locations (HQ and other) and alternate operating facility(ies) within 24 hours	• Conduct internal agency communications tests between normal operating locations (HQ and other) and alternate operating facility(ies) within 24 hours and repeat NLT weekly. • Conduct communications tests at all alternate operating facility(ies) with applicable interagency partners within 48 hours and repeat NLT weekly	• Test internal agency communications between normal operating locations (HQ and other) and alternate operating facility(ies) daily • Conduct communications tests at all alternate operating facility(ies) with applicable interagency partners daily
Succession	• No special measures to protect or track location of agency leadership and successors • Ensure delegations of authority to lead D/A are in place for senior personnel located outside of national capital region.	• Track locations of agency leadership and their successors on daily basis	• Track locations of agency leadership and their successors on daily basis • Ensure at least one headquarters-level agency successor is out of national capital area at all times	• Track locations of agency leadership and their successors on daily basis • At least one headquarters-level agency successor at alternate operating facility(ies)
Time to Transition to Successive Stages	• Fully operational within 12 hours	• Fully operational within 8 hours • 4 hours to COGCON 2	• Fully operational within 4 hours (4 hours to COGCON 1)	• Agency headquarters COOP plan operational immediately
Impact on Departments & Agencies	• No additional requirements	• Additional staff time for communications testing and tracking agency leadership • Potential shorter response times for basic staffing of alternate facility(ies)	• Potential increased travel requirements for agency leadership • Some staff required to work from alternate location(s) • Potential shorter response times for additional staffing of alternate facility(ies)	• Some agency leadership work from alternate facility(ies) • Significant number of staff required to work from alternate location(s)
Notification Process	Step 1. White House Chief of Staff/Deputy Chief of Staff for Operations/WHMO Director notifies PEOC Step 2. PEOC notifies FOC Step 3. FOC notifies Department and Agency COOP Emergency Points of Contact and/or Emergency Operations Centers			

DEPARTMENT AND AGENCY COOP ALERT & DEPLOYMENT OPTIONS

COOP Notification Message	White House Chief of Staff/Deputy Chief of Staff for Operations/Director White House Military Office to PEOC — "This is a Continuity of Operations message. Direct all department's and agencies to assume a COGCON □-4, □-3, □-2, □-1 (designate COGCON) readiness posture with the exception of those departments and agencies circled below, who will assume a COGCON □-4, □-3, □-2, □-1 readiness posture." (designate COGCON) Central Intelligence Agency Department of Agriculture Department of Commerce Department of Defense Department of Education Department of Energy Department of Health & Human Services Department of Homeland Security Department of Housing & Urban Development Department of Justice Department of Labor Department of State Department of the Interior Department of the Treasury Department of Transportation Department of Veterans Affairs Environmental Protection Agency Executive Office of the President Federal Communications Commission Federal Emergency Management Agency Federal Reserve System General Services Administration National Aeronautics and Space Administration National Archives and Records Admin National Communications System Nuclear Regulatory Commission Office of Personnel Management Securities and Exchange Commission Social Security Administration US Army Corps of Engineers United States Postal Service

TOP OFFICIALS 4 (TOPOFF 4) FULL-SCALE EXERCISE (FSE)

October 15 – 20, 2007

AFTER-ACTION REPORT

March 15, 2008

This page is intentionally blank.

ADMINISTRATIVE HANDLING INSTRUCTIONS

1. The title of this document is Top Officials 4 (TOPOFF 4) After-Action Report / Improvement Plan (AAR/IP).

2. The information gathered in this AAR/IP is designated as ~~For Official Use Only~~ ~~(FOUO)~~ and should be handled as sensitive information. This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate security directives. Reproduction of this document, in whole or in part, without prior approval from the U.S. Department of Homeland Security (DHS) is prohibited.

3. At a minimum, the attached materials will be disseminated only on a need-to-know basis and when unattended, will be stored in a locked container or area offering sufficient protection against theft, compromise, inadvertent access, and unauthorized disclosure.

4. Points of Contact (POCs):

   Federal POC:

   Mr. Bill McNally
   Director, National Exercise Division
   FEMA National Preparedness Directorate
   U.S. Department of Homeland Security
   Washington, DC 20536
   William.McNally@dhs.gov

   Exercise Director:

   Ms. Sandra Santa Cosgrove
   FEMA National Preparedness Directorate
   U.S. Department of Homeland Security
   Washington, DC 20536
   Sandra.Santa@dhs.gov

This page is intentionally blank.

CONTENTS

Tables

Figures

EXECUTIVE SUMMARY

TOPOFF is a congressionally-mandated terrorism preparedness exercise program, involving top officials at every level of government, as well as representatives from the international community and the private sector. TOPOFF 4 (T4) was sponsored by DHS and is the fourth TOPOFF Exercise Series. Each TOPOFF series involves a two-year cycle of seminars, planning events, and exercises, and culminates in a full-scale assessment of the nation's capacity to prevent, prepare for, respond to, and recover from terrorist attacks involving weapons of mass destruction (WMDs).

More than one hundred organizations were involved in planning T4, including DHS and other federal agencies; state, territorial, tribal, and local agencies from the states of Arizona and Oregon and the U.S. Territory of Guam; private sector, and non-governmental organizations (NGOs); as well as three international partners: Australia, Canada, and the United Kingdom. The T4 FSE used a radiological dispersal device (RDD) scenario based on National Planning Scenario (NPS) 11 to test the full range of federal, state, territorial, and local capabilities. This scenario included coordinated attacks in Guam, Oregon, and Arizona.

A major goal of TOPOFF exercises is to test existing plans, policies, and procedures to identify planning and resource gaps, and ultimately to implement corrective actions to improve WMD preparedness. The following objectives guided planning for T4:

- **Prevention**: To test the handling and flow of operational and time-critical intelligence between agencies to prevent a terrorist incident.
- **Intelligence/ Investigation**: To test the handling and flow of operational and time-critical intelligence between agencies prior to, and in response to, a linked terrorist incident.
- **Incident Management**: To test the full range of existing procedures for domestic incident management of a terrorist WMD event and to improve top officials' (federal/state/local) capabilities to respond in partnership in accordance with the National Response Plan[1] (NRP) and National Incident Management System (NIMS).
- **Public Information**: To practice the strategic coordination of media relations and public information issues in the context of a terrorist WMD incident or incident of national significance (INS).
- **Evaluation**: To identify lessons learned and promote best practices.

Nearly every capability in the DHS Target Capabilities List (TCL) was exercised. This AAR focuses on national policy and planning issues related to five of those capabilities: On-Site Incident Management, Emergency Operations Center (EOC) Management, Emergency Public Information and Warning, Economic and Community Recovery, and Intelligence/Information Sharing and Dissemination. These capabilities were chosen because they relate to the objectives above and other criteria explained in Section 2. Other AARs completed by venues, agencies, and organizations evaluate additional capabilities. The purpose of this report is to analyze exercise results, identify strengths to be maintained and built upon, identify potential areas for further improvement, and support the development of corrective actions.

[1] The NRP was in effect at the time of the exercise, but was replaced by the National Response Framework (NRF) in January of 2008.

Major Strengths

Past TOPOFF exercises and actual disasters such as Hurricane Katrina have uncovered gaps in the nation's preparedness. T4 provided an opportunity to test corrective actions taken since previous exercises and Hurricane Katrina.[2] Our analysis highlighted several areas where improvement in response coordination was evident:

- New policies and procedures provided additional detail to national plans. A significant issue identified in TOPOFF 3 (T3) and Hurricane Katrina is that national plans lacked operational details. Since these events, a significant amount of planning has occurred, and T4 provided an opportunity to test changes to the NRP, new Emergency Support Function (ESF) Standard Operating Procedures (SOPs), and new scenario-based plans and playbooks.
- New federal teams and tools have been established to address specific shortfalls identified in past TOPOFF exercises and during Hurricane Katrina. For example, the DHS Crisis Action Team (CAT) and Homeland Security Information Network (HSIN) Common Operating Picture (COP) portal were established to address a lack of shared situational awareness among agencies and were rigorously tested during the exercise.
- There was robust private sector involvement in the exercise – more so than any previous TOPOFF exercise. This participation added realism to the exercise, helped identify areas where the private sector can contribute, and helped decision-makers consider and address the needs of the private sector in the context of this scenario.
- Disability and other special needs play was a major focus area in the exercise design. As a result, players gained critical practical experience regarding the additional support needed by individuals having special needs.

Some of the areas described above require further improvement. Nonetheless, these strengths represent progress in addressing previously identified gaps in the nation's preparedness.

Primary Areas for Improvement

Throughout the exercise, opportunities for improvement in the nation's ability to respond to a WMD incident were identified. These areas for improvement include recurring themes – issues that have been identified in previous TOPOFF exercises and during Hurricane Katrina – along with several new issues highlighted by this scenario. Many of the issues are intertwined. Four key areas for improvement that also impacted other areas are summarized here. The report provides a detailed discussion of all areas for improvement.

Unified Management of the National Response

The White House Hurricane Katrina report identified the process for establishing unified management of the national response as a key flaw in emergency response. This process, as defined in the NRP, NIMS, and the newly released National Response Framework (NRF) includes the state and local command and coordination structures, and the federal command and

[2] All references to previous TOPOFF exercises and Hurricane Katrina are drawn from the T2 and T3 AARs, and the White House Homeland Security Council's February 2006 report, *The Federal Response to Hurricane Katrina. Lessons Learned.*

coordination structures established to support them. This process, as implemented, did not account for the complex set of conditions experienced during Katrina – large-scale devastation, competing needs, and insufficient resources. The conditions during T4 were different but equally complex. The scenario included the occurrence of three terrorist strikes in different locations, the use of devices that caused radiological contamination, and the limited supply of federal radiological assets.

This complexity affected the establishment of unified command structures at the incident sites, where many local, state, territory, and federal responders arrived with different authorities, functions, and missions. It also impacted the larger coordination structure, which in addition to the incident site unified command, included local, state, and territory EOCs and Emergency Coordination Centers (ECCs); other unified commands; the federal Interim Operating Facilities (IOFs) and Joint Field Offices (JFOs); and other federal entities such as the Federal Radiological Monitoring and Assessment Center (FRMAC). Further contributing to the complexity, the Nuclear/Radiological Incident Annex was the guiding document for the response, and federal responders had difficulty merging the roles and responsibilities outlined in this annex with the roles and responsibilities established through the NRP ESF structure.

This problem was most evident in the Oregon venue, which established all components of the local, state, and federal response structure.[3] In Oregon, communication and coordination between the multiple command and control nodes varied. The structure did not promote effective information flow and had a significant impact on top official decision-making, especially regarding the implementation of protective actions and public messaging.

This complexity was also evident at federal headquarters command centers and the White House, where senior officials were deciding how to allocate scarce resources and implement protective measures to mitigate attacks in other locations. Although decisions were made and actions taken, there were no formal procedures that described how to support decision-making and disseminate the decisions to the federal interagency.

At the national level, improvement in doctrine and guidance is needed to help responders at all levels of government establish an effective unified management system in response to a complex event. Scenario-based plans and guidance are one step in addressing the factors unique to specific scenarios like an RDD event. These plans should also include processes for allocating scarce resources and include recommended protective actions. The implementation of the Nuclear/ Radiological Incident Annex within the ESF response structure and the NRF also needs review and clarification. Because every state and territory has its own unique structures, authorities, and requirements, this national guidance should be implemented at the regional level through existing planning programs, and supported through existing training and exercise programs.

Protective Action Decisions and Communicating Guidance to the Public

Faced with similar information and scenarios, leaders in Arizona and Oregon made different decisions about protective actions (evacuation versus shelter-in-place). These were difficult choices that required decision-makers to act quickly while assessing scientific model results and

[3] In Arizona, all field components were simulated, and in Guam, some field components/functions were simulated. In addition, Guam does not have a local level of government, making it less likely to experience these problems.

conditions specific to their locality. The mock media repeatedly questioned federal, state, and local officials about this disparity, and officials had difficulty explaining their decisions and why different actions were taken in different jurisdictions. Two factors contributed to this difficulty:

- Communicating these decisions required the explanation of complex scientific information, such as the differences between short-term and long-term radiation exposure, and the interpretation of technical products like plume model results and deposition measurements.
- It is the responsibility of local officials to explain their individual decisions, but no expert or official explained why different decisions were acceptable or why both sets of actions protected the public. Similar circumstances also occurred during T3.

While protective actions are the responsibility of local jurisdictions, the federal government and scientific community should develop additional strategies for supporting local officials in explaining these decisions that address both of these points.

Situational Awareness and the COP

As observed in T3 and during Hurricane Katrina, departments and agencies (D/As) at all levels of government had difficulty obtaining critical information and maintaining situational awareness. Although the HSIN and COP portal provided easy access to some information, other information elements were not readily available. Senior decision-makers were most interested in plume model results, casualty counts, information on protective actions, and the status of federal resources. With the exception of the plume model results, these information elements were among the most difficult for DHS to collect and disseminate. The use of multiple platforms, systems, and portals also complicated information sharing. Defining the most critical pieces of information, identifying the sources, and developing processes for obtaining and verifying the information are necessary to improve situational awareness and information sharing.

Homeland Security Advisory System (HSAS)

As observed during previous TOPOFF exercises, the purpose, definitions, and consequences of the HSAS threat levels are not clear. Changes to Red and Orange threat levels, in both specific locations and nationwide, led to many different interpretations of the intent of the change and few actions. However, sector-specific changes did cause specific protective actions to be taken by federal, state, territory, and local agencies. Better definitions of the HSAS levels are needed that include more detail about the actions to be taken with different changes in level and sector.

Conclusion and Next Steps

The overall exercise succeeded in highlighting improvements since previous exercises and Hurricane Katrina, as well as identifying areas requiring further development. At the After-Action Conference (AAC) held on January 15, 2008, participating agencies met to review the findings and recommendations in this AAR and draft corrective actions. The IP included in Appendix A lists the corrective actions. The DHS NEP has established a process for tracking and monitoring the implementation of these corrective actions.

SECTION 1: EXERCISE OVERVIEW

Exercise Details

Exercise Name

Top Officials 4 (TOPOFF 4)

Type of Exercise

Full-Scale Exercise (FSE) with functional and tabletop components

Exercise Dates

Arizona Prevention Component: September 17 – 28, 2007

Oregon Prevention Component: September 24 – October 10, 2007

Guam Prevention Component: October 1 – 12, 2007

FSE: October 15 – 20, 2007

Long-Term Recovery Tabletop Exercise (LTR TTX): December 4 – 5, 2007

Duration

Prevention Component: 26 days

FSE: 6 days (Guam and Oregon conducted discussion-based exercises during the following week)

LTR TTX: 2 days

Location

Arizona, Oregon, the U.S. Territory of Guam, the National Capital Region (NCR), other regional headquarters and commands, Australia, Canada, and the United Kingdom

Sponsor

Department of Homeland Security (DHS)

Program

National Exercise Program (NEP)

Mission

Prevent, Respond, and Recover

Capabilities

Intelligence/Information Sharing and Dissemination, On-Site Incident Management, Emergency Operations Center Management, Emergency Public Information and Warning, Economic and Community Recovery

Scenario Type

Radiological Dispersal Device (RDD)

Exercise Planning Team Leadership

The names of the T4 Executive Steering Committee (ESC) members are listed below:

- Mr. Bill McNally, chair, DHS FEMA National Preparedness Directorate
- Supervisory Special Agent (SSA) (b)(6) Federal Bureau of Investigation (FBI)
- Ms. (b)(6) Office of the Director of National Intelligence (ODNI)
- Mr. Steven Buntman, Department of Energy (DoE)
- Dr. Keith Holtermann, Department of Health and Human Services (HHS)
- Mr. Thomas MacKay (replaced Dr. Holtermann during the after-action process), HHS
- Mr. (b)(6) Office of the Secretary of Defense (OSD)
- LT COL (b)(6) Department of Defense (DoD), Joint Staff
- Mr. (b)(6) Department of State (DoS)
- Mr. (b)(6) Homeland Security Council (HSC)
- Mr. (b)(6) National Security Council (NSC)

Ms. Sandra Santa Cosgrove was the exercise director. The lead planners from the venues and international community are listed below:

- Arizona: Ms. (b)(6) Arizona Department of Emergency and Military Affairs, and Mr. (b)(6) DHS
- Guam: LT (b)(6) Guam Homeland Security, Office of Civil Defense and Mr. Nathan Rodgers, DHS
- Oregon: Ms. Kelly-Jo Craigmiles, Oregon Emergency Management, and Mr. Jeremy Greenberg, DHS
- Australia: Mr. (b)(6) Attorney-General's Department
- Canada: Mr. (b)(6) Public Safety Canada
- United Kingdom: Ms. (b)(6) Foreign & Commonwealth Office

Participating Organizations

The following federal departments, agencies, and offices participated in the T4 FSE:

- Central Intelligence Agency (CIA)
- Department of Agriculture
- Department of Commerce, National Oceanic Atmospheric Administration
- DoD
  - JFCOM
  - NORTHCOM
  - Office of the Secretary of Defense/J-7/ASD-HD
  - PACOM
  - STRATCOM
  - U.S. Army Corps of Engineers
- DoE
  - National Nuclear Security Administration
- HHS
  - Centers for Disease Control, Emergency Response Directorate
  - Centers for Disease Control, Strategic National Stockpile
  - Food and Drug Administration
  - Office of the Assistant Secretary for Preparedness and Response
- DHS
  - Customs and Border Protection

- Domestic Nuclear Detection Office
- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement
- National Citizen Corps
- National Cyber Security Division
- National Protection & Programs Directorate
- Office for Civil Rights and Civil Liberties
- Office of Health Affairs
- Office of Infrastructure Protection
- Office of Operations Coordination
- Private Sector Office
- Science & Technology
- Transportation Security Administration (TSA)
- Terrorism Prevention Exercise Program (TPEP)
- U.S. Coast Guard (USCG)

- Department of Housing and Urban Development
- Department of Interior
- Department of Justice (DoJ)
  - FBI
  - Bureau of Alcohol, Tobacco, Firearms, and Explosives
- Department of Labor
  - Occupational Safety and Health Administration
- DoS
- Department of Transportation (DoT)
  - Federal Aviation Administration (FAA)
- Department of Veterans Affairs
- Environmental Protection Agency (EPA)
- General Services Administration (GSA)
- National Communications System
- National Guard Bureau
- National Security Agency (NSA)
- Nuclear Regulatory Commission
- Office of Personnel Management (OPM)
- ODNI
- Small Business Administration
- White House Staff

The following private sector entities and NGOs participated at the national level:

Full Scale Exercise:

- American International Group, Inc.
- American Red Cross (ARC)
- AT&T
- BENS
- Cisco
- City of Dallas Convention/Event Services
- Computer Sciences Corporation (Simulation Cell (SIMCELL), VIP)
- Grocery Manufacturer's Association
- HMC SCC
- IIT
- IT-ISAC Operations Center
- Juniper Networks, Inc.
- L-3 Communications, Technical and Management Services Group
- Terre Star Networks Inc.
- Wal-Mart Stores, Inc.

Functional Exercise:

- AMWA
- Boeing Company, The

- FS-ISAC
- Nortel Government Solutions
- Water ISAC
- Water sector utilities (looking glass)

Tabletop Exercise:

- Accenture
- American Trucking Associations – Highway ISAC
- DRS Technologies
- International Association of Assembly Managers (looking glass)
- Raytheon
- U.S. Chamber of Commerce

Looking Glass:

- Access Systems Inc.
- Adidas America Inc.
- Admiral Security
- AIG
- Alliant Group, The
- ANSI
- Avon Products
- BAE Systems
- Beacon Capital
- Bechtel National, Inc.
- BOMA International
- Boston Properties
- BP North America
- Brookfield Properties
- CB Richard Ellis
- CellExchange
- Corporate Storyteller, The
- Cousins Properties Incorporated
- Cushman & Wakefield
- DRS-TSI Inc.
- Ericsson Inc.
- FSSCC
- General Electric
- GeoResources Institute, Mississippi State University
- Hines
- Honeywell
- Institute of Real Estate Management
- International Council of Shopping Centers
- Jones Lang LaSalle
- Lockheed Martin
- Macerich Company
- Marriott Employees' Federal Credit Union
- Marriott International
- Marsh
- Mississippi State University, GeoResources Institute
- Morgan Stanley
- National Apartment Association
- National Multi Housing Council
- National Petrochemical & Refiners Association
- National Sheriffs Association
- New Jersey Business Force - Business Executives for National Security
- NJ Resources
- Nuclear Energy Institute
- NYC DEP
- OOIDA
- Oracle
- PepsiCo, Inc.
- Port Authority of New York and New Jersey
- PREIT
- Previstar
- Professional Security Consultants
- Raley's Family of Fine Store
- Real Estate Roundtable, The
- Real Estate Roundtable/Real Estate ISAC
- Related Management
- SAIC

- Sentinel Real Estate Corp.
- Simon Property Group
- South Coast Plaza Security
- Starwood Hotels & Resorts Worldwide, Inc.
- Target Corporation
- Tishman Speyer
- UDR
- Washington Group International

International participating agencies included the following:

Australia

- Attorney-General's Department
- Australian Customs Service
- Australian Federal Police
- Australian Nuclear Science and Technology Organisation
- Australian Radiation Protection and Nuclear Safety Agency
- Australian Security Intelligence Organisation
- Department of Defence
- Department of Foreign Affairs and Trade
- Department of Health and Ageing
- Department of Immigration and Citizenship
- Department of Prime Minister and Cabinet
- Emergency Management Australia
- Inter-Departmental Emergency Task Force
- National Security Committee of Cabinet
- National Crisis Committee
- Protective Security Coordination Centre

Canada

- Agriculture Canada
- Canadian Nuclear Safety Commission
- Canadian Border Services Agency
- Canadian Security Intelligence Service
- Citizenship and Immigration
- Communications Security Establishment
- Department of National Defence
- Foreign Affairs and International Trade Canada
- Government Operations Centre
- Industry Canada
- Natural Resources Canada
- Public Health Agency of Canada
- Public Safety Canada
- Public Works and Government Services Canada
- Royal Canadian Mounted Police
- Service Canada
- Transport Canada

United Kingdom

- Cabinet Office (including Civil Contingencies Secretariat)
- Foreign & Commonwealth Office
- Home Office
- Department for Transport
- Department of Health
- Department for Culture, Media & Sport
- Health Protection Agency
- Metropolitan Police CT Cmd (SO15)

Participating agencies in Arizona included the following:

State and Local:

- Arizona Attorney General's Office
- Arizona Corporation Commission
- Arizona Counter Terrorism Information Center
- Arizona Department of Administration
- Arizona Department of Agriculture
- Arizona Department of Corrections
- Arizona Department of Economic Security
- Arizona Department of Emergency and Military Affairs
- Arizona Department of Environmental Quality
- Arizona Department of Health Services
- Arizona Department of Homeland Security
- Arizona Department of Housing
- Arizona Department of Juvenile Corrections
- Arizona Department of Occupational Safety and Health
- Arizona Department of Public Safety
- Arizona Department of Revenue
- Arizona Department of Transportation
- Arizona Department of Water Resources
- Arizona Fish and Game
- Arizona Health Care Cost Containment System
- Arizona Medical Board
- Arizona Office of the Governor
- Arizona Radiation Regulatory Agency
- Arizona Registrar of Contracts
- Arizona State University
- Business Operations Center – Arizona (approximately 20 participating organizations)
- City of Avondale
- City of Chandler
- City of Glendale
- City of Goodyear
- City of Litchfield Park
- City of Mesa
- City of Tempe
- City of Peoria
- City of Phoenix
- City of Scottsdale
- City of Surprise
- City of Tucson
- Fort McDowell Indian Community
- Fountain Hills
- Gila River Indian Community
- La Paz County
- Maricopa County Department of Emergency Management
- Maricopa County Public Health
- Metropolitan Medical Response System
- Phoenix Aviation (Sky Harbor International Airport)
- Phoenix VAMC
- Pima County Emergency Management
- Pima County Sheriff's Office
- Pinal County
- Salt River Pima Indian Community
- Town of Buckdale (limited participation)
- Town of Gilbert
- Tucson Airport Authority
- Tucson VAMC
- Yavapai County

Federal:

- EPA
- DHS
  - FEMA, Region IX
- DoJ
  - FBI
- TSA
- U.S. Customs and Border Protection
- U.S. Postal Service
- U.S. Postal Inspection Service
- U.S. Veteran's Affairs
- VA Network (VISN)

Private Sector/NGO:

- AT&T
- Banner Health Hospitals
- Boswell
- Cox Cable
- Del Web
- Grand Canyon Chapter of the ARC
- Intel Corp
- Phoenix Children's Hospital
- Southern Arizona Chapter of the ARC
- Sun Health Care Hospitals
- The Salvation Army
- Verizon Wireless

Participating agencies in Guam included the following:

State and Local:

- Guam Airport Authority
- Guam Airport Authority Police
- GUAMCELL
- Guam Customs and Quarantine
- Guam Department of Corrections
- Guam Department of Mental Health and Substance Abuse
- Guam Department of Public Health and Social Services
- Guam Department of Public Works
- Guam EPA
- Guam Fire Department
- Guam National Guard
- Guam Police Department
- Guam Port Authority
- Guam Telephone Authority
- Guam Visitors' Bureau
- Hawaii National Guard
- Guam Homeland Security/Office of Civil Defense (GHS/OCD)
- Judiciary of Guam
- Office of the Governor
- Public Schools System

Federal:

- DoD
  - U.S. Air Force
  - U.S. Army Corps of Engineers
  - U.S. Navy
  - U.S. Pacific Command/Joint Task Force – Homeland Defense
- DoE
- HHS
- DHS
  - FEMA
  - USCG
  - Office of Infrastructure Protection
  - Office of Public Affairs
- DoJ
  - Attorney General's Office
  - Bureau of Alcohol, Tobacco, Firearms, and Explosives
  - FBI
  - Secret Service

- Department of Labor
- DoS
- EPA
- Military Sealift Command, LLC
- National Weather Service
- Small Business Administration
- United States Postal Inspection Service

Private Sector/NGO:

- ARC
- Casamar, Incorporated
- Continental
- Goodwind Development Corp
- Group 4 Securicor
- Guam Hotel and Restaurant Association
- Guam Mami, Incorporated
- Guam Memorial Hospital
- Guam Power Authority
- Guam Surgical Center
- Hawaiian Rock Products
- Horizon Lines
- IConnect
- IT&E
- Janus Marketing
- Matson Shipping
- Micronesian Divers Assoc. Inc.
- Mobile
- Payless Markets
- Peterra, Inc.
- Shell
- South Pacific Petroleum Corporation
- The Salvation Army
- University of Guam Nursing Program

Participating agencies in Oregon included the following:

State and Local:

- Beaverton City Emergency Management
- Tigard City Emergency Management
- Clackamas County Emergency Management
- Clark Regional Regional Emergency Services Agency
- Columbia County 911
- Columbia County Emergency Management
- Columbia River Fire & Rescue
- Gresham Emergency Management
- Gresham Fire
- Gresham Police
- Hillsboro City Emergency Management
- Hillsboro Emergency Management
- Hillsboro Fire
- Multnomah County Health Department
- Multnomah County Sheriff
- Multnomah County Emergency Management
- Oregon Department of Agriculture
- Oregon Department of State Lands
- Oregon DoT
- Oregon Disaster Medical Assistance Team
- Oregon Health & Science University
- Oregon National Guard
  - 102nd Civil Support Team
- Oregon Occupational Safety and

Health Administration
- Oregon Office of Disability
- Oregon Office of Emergency Management
- Oregon Office of Vocational Rehabilitation Services
- Oregon Public Health
- Oregon State Fire Marshal
- Oregon State Police
- Oregon State Public Health
- OREN
- Port of Portland
- Portland Bureau of Emergency Communications
- Portland Department of Transportation
- Portland Fire
- Portland Metropolitan Exposition Center
- Portland Office of Emergency Management
- Portland Police
- Portland VAMC
- Washington County 911
- Washington County Emergency Management

Federal:
- Department of Agriculture
- Department of Commerce
  - National Oceanic and Atmospheric Administration, National Weather Service
- DoD
  - NORTHCOM-CAE
  - Defense Threat Reduction Agency (DTRA)
- DoE
- HHS
- DoJ
  - FBI
- DHS
  - Customs and Border Protection
  - FEMA
  - Federal Protective Service
  - TSA
  - USCG
- DoS
- EPA
- VISN 20 Network Control Center

Private Sector/NGO:
- ACS
- ARC
- Ashforth Pacific
- AT&T
- Columbia River Steamship Operators Assistance
- Easter Seals Oregon
- Glimcher
- Guide Dogs for the Blind
- Hilton Hotels
- Hospitals
  - Adventist Medical Center
  - Kaiser Interstate Clinic
  - Kaiser Regional Coordination Center
  - Kaiser Sunnyside Hospital
  - Legacy Coordination Center
  - Legacy Emmanuel Hospital
  - Legacy Good Samaritan Hospital
  - Legacy Meridian Park Hospital
  - Legacy Mount Hood Hospital
  - Legacy Salmon Creek Hospital
  - Providence Milwaukie Hospital
  - Providence Portland Hospital
  - Providence St. Vincent Hospital
  - Regional Hospital
  - Shriner's Hospital
  - SW Washington Hospital
  - Tuality Community Forest Grove Hospital
  - Tuality Community Hillsboro Hospital
  - Willamette Falls Hospital

- Independent Living Resources
- Intel
- Job Development Network
- Liberty Northwest
- Lloyd Center Mall
- Macy's
- Metro West Ambulance
- Nextel
- Northwest Natural
- Novation
- ON Semiconductor
- Oregon Convention Center
- Owens & Minor
- PacifiCorp
- PGE
- Qwest
- RAZ Transportation
- Rehabilitation Institute of Oregon
- Schnitzer Steel Corp
- Shaver Transportation
- Standard Insurance
- Terrestar
- T-Mobile
- TriMet
- TVF&R
- University Health System Consortium
- U.S. Bank
- Wal-Mart
- XEROX

Number of Participants

Participant[1]	Arizona	Guam	Oregon	Federal Interagency	International	Total
Players	2,000	1,890	10,640	3,280	280	18,090
Controllers	350	140	550	250	50	1,340
Evaluators	150	60	270	150	35	665
Observers	80	80	30	440	65	695
Victim Role Players	0	200	2,760	0	0	2,960
	2,580	2,370	14,250	4,120	430	23,750

[1] Private sector participant totals are contained within the totals shown.

SECTION 2: EXERCISE DESIGN SUMMARY

Exercise Purpose and Design

T4 was comprised of a series of exercises and activities, including seminars and conferences that took place over a two-year period and culminated in the FSE, conducted from October 15 through October 20, 2007. The T4 FSE was designed to serve several important functions: it addressed national counter-terrorism strategy; it exercised the national ability to prevent, respond to, and recover from a series of coordinated and geographically dispersed terrorist threats and acts; and it engaged senior officials from federal, state, territory, tribal, and local jurisdictions, as well as partner nations. The DHS FEMA National Exercise Division (NED) was the lead agency for T4 planning. Other agencies with counter-terrorism duties were invited to participate.

The T4 exercise design included three primary components:

- A series of national training seminars.
- Extended prevention-centered exercise play.
- An FSE designed to test the performance of products and processes.

The T4 FSE was a multi-agency, multi-site, domestic counter-terrorism event that simulated WMD terrorist incidents in Arizona, Guam, and Oregon. In addition, T4 included the participation of the governments of Australia, Canada, and the United Kingdom. T4 provided DHS and other federal, state, territory, tribal, and local D/As with an opportunity to exercise and evaluate the implementation of doctrine established in the NRP, the NIMS, and supporting policies and procedures.

Simulated RDD detonation in Guam on October 16, 2007.

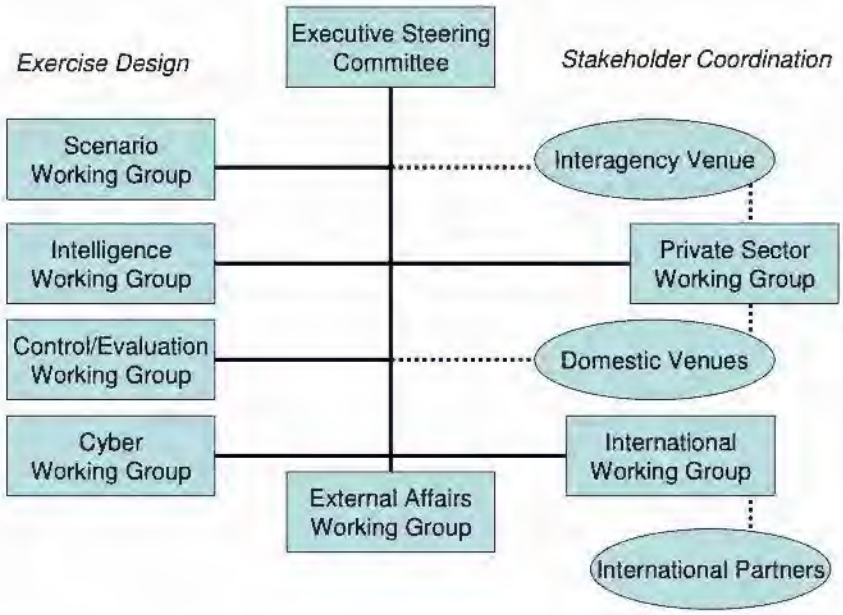
The FSE began with a simulated RDD detonation in Guam on the morning of October 16, 2007 (the evening of October 15 on the East Coast). Simulated detonations occurred in Oregon and Arizona on the following day (October 16). DHS planners worked with the venues and the interagency group to determine the best hours and days of exercise play. The end of the exercise (ENDEX) occurred on October 20, 2007. Hot wash and short-term recovery events followed in each of the venues. The LTR TTX was held on December 4 – 5, 2007, and addressed short- and long-term recovery issues.

Exercise Planning and Management

The planning and management of the T4 FSE was an integrated effort among the major exercise planners and sponsors. The exercise management structure and its working groups are illustrated in Figure 2.1. Each major planner and sponsor had a voting representative in each of the positions described below. This integrated planning approach provided a mechanism to

coordinate planning efforts by DHS and its components, DoD, DoE, DoS, EPA, FBI, HHS, and other T4 FSE interagency partners.

Figure 2.1: Exercise Management Structure



The ESC was responsible for overall exercise oversight. Members ensured that planning efforts were coordinated among the working groups, were communicated to policy makers, and reflected policy guidance. Specifically, the ESC supported the following functions:

- Coordinated and integrated the efforts of the working groups and venues to create a coherent exercise design that met the policy and strategic-level objectives of stakeholders.
- Provided guidance to working groups, including guidance for the adaptation of NPS 11 to support exercise objectives.
- Reviewed and approved working group products and exercise documentation, including the scenario, Universal Adversary (UA) threat models, exercise intelligence products, the Master Scenario Events List (MSEL), the Exercise Plan (EXPLAN), the Control Staff Instructions (COSIN), and the Evaluation Plan (EVALPLAN).
- Adjudicated conflicts or discrepancies among working groups regarding their products.
- Provided periodic updates on the progress of exercise design and development to senior policy makers.
- Ensured, through the exercise director, shared awareness of ongoing exercise design and development efforts among exercise planners.

The roles of the exercise working groups were as follows:

- The Control and Evaluation Working Group (CEWG) worked with agencies to ensure that the EXPLAN incorporated the respective D/A training objectives. The Master

EXPLAN contained all the essential exercise products, such as the COSIN and the EVALPLAN. Additionally, the CEWG planned and executed the training program for over 2,000 controllers and evaluators responsible for supporting the exercise.

- The Intelligence Working Group (IWG) planned and coordinated all aspects of intelligence play for the exercise.
- The Scenario Working Group (SWG) planned and coordinated all aspects of scenario development for the exercise, and ensured a plausible and realistic scenario that supported evaluation of selected national capabilities.
- The Cyber Working Group (CWG) designed and developed the cyber component of the T4 exercise.
- The Private Sector Working Group (PSWG) planned and coordinated all aspects of private sector play in the exercise.
- The External Affairs Working Group (EAWG) planned and coordinated all aspects of Public Information Officer (PIO) participation in and support of the exercise.
- The International Working Group supported the international partner and U.S. embassy involvement in the exercise, and coordinated international participation with U.S. government (USG) D/As.

Exercise Objectives, Capabilities, and Activities

The overarching T4 FSE exercise objectives were:

- **Prevention:** To test the handling and flow of operational and time-critical intelligence between agencies to prevent a terrorist incident.
- **Incident Management**: To test the full range of existing procedures for domestic incident management of a WMD terrorist event and to improve the capabilities of federal, state, territory, and local top officials to respond cooperatively and in accordance with the NRP and NIMS.
- **Intelligence/ Investigation**: To test the handling and flow of operational and time-critical intelligence between agencies prior to, and in response to, a linked terrorist incident.
- **Public Information:** To practice the strategic coordination of media relations and public information issues in the context of a WMD terrorist incident or incident of national significance.
- **Evaluation**: To identify lessons learned and promote best practices.

Based on these overarching objectives, the planning team selected specific objectives linked to top official/interagency decision-making, interagency coordination, and the execution of national-level plans. They were selected because they met one or more of the following criteria:

- They related to the T4 goals, objectives, and underlying themes.
- They related to HSC direction to exercise NPS 11.
- They have been identified as issues in past TOPOFF or other national-level exercises.
- They have been identified as issues following Hurricane Katrina.
- They related to the National Preparedness Goal and its priorities.

These specific objectives are the focus of this AAR and are listed below along with the corresponding capabilities and activities (for a more detailed description of these objectives, see the EVALPLAN):

- **Objective 1:** Test existing procedures for domestic incident management of a terrorist RDD event and top officials' capabilities to respond in partnership in accordance with the NRP and NIMS.
  - **On-Site Incident Management**: Implement on-site incident management; establish full on-site incident command; resource management; develop incident action plan, and evaluate/revise plans.
  - **EOC Management**: Identify and address issues; prioritize and provide resources; and support and coordinate response.
- **Objective 2:** Test the ability of command, operations, and intelligence centers to share intelligence and information and maintain a COP.
  - **EOC Management**: Gather and provide information.
  - **Intelligence/Information Sharing and Dissemination**: Conduct vertical flow of information; conduct horizontal flow of information.
- **Objective 3:** Exercise the authorities, responsibilities, and capabilities of the federal assets necessary to respond to and recover from a terrorist RDD incident.
  - **On-Site Incident Management**: Implement on-site incident management; establish full on-site incident command; and resource management.
  - **EOC Management**: Identify and address issues; prioritize and provide resources; and support and coordinate response.
  - **Economic and Community Recovery**: Direct economic and community recovery operations.
- **Objective 4:** Examine the handling of mental health and special needs issues that may arise during and after an RDD event.
  - **On-Site Incident Management**: Implement on-site incident management.
  - **EOC Management**: Identify and address issues; prioritize and provide resources; and support and coordinate response.
- **Objective 5:** Examine citizen protection and public warning activities in response to a terrorist RDD incident.
  - **Emergency Public Information and Warning**: Manage emergency public information and warning; activate emergency public information, alert/warning, and notification plans; establish Joint Information Center (JIC)/ Joint Information System (JIS); disseminate/issue emergency public information and alert/warnings; and conduct media relations.
- **Objective 6:** Examine public health, medical support, mass decontamination, and mass care requirements during a terrorist RDD incident.
  - **On-Site Incident Management**: Implement on-site incident management; establish full on-site incident command; and resource management.

  - **EOC Management**: Identify and address issues; prioritize and provide resources; and support and coordinate response.
- **Objective 7:** Exercise the coordination of a domestic and international media and public communications strategy and public messaging in the context of a terrorist RDD incident.
  - **EOC Management**: Gather and provide information; and support and coordinate response.
  - **Emergency Public Information and Warning**: Manage emergency public information and warning; activate emergency public information, alert/warning, and notification plans; establish JIC/ JIS; disseminate/issue emergency public information and alert/warnings; and conduct media relations.

These objectives link to five of the capabilities in the TCL. Additional capabilities were exercised that relate to specific agency missions and tactical level operations. They are evaluated in venue and other internal agency evaluations. Some of these evaluations are included as annexes to this report.

Scenario Summary

The T4 FSE Scenario was based on NPS 11 (*Radiological Attack – Radiological Dispersal Devices)* and its associated UA threat models. Used as a common foundation for exercise development, the scenario – complemented by current threat information about the UA – ensured that exercise participants focused on performing the appropriate critical tasks and assessed capabilities linked to specific homeland security mission areas.

In the T4 FSE Scenario, terrorist members of the UA group acquired radiological sources from foreign locations. The source materials were smuggled into the United States via separate shipments and then assembled. A Customs and Border Patrol exercise conducted prior to the start of the FSE focused on procedures in place to intercept radiological materials and is documented in Annex 2.

Two of the most visible features of the T4 FSE scenario were the Virtual News Network (VNN) Live news broadcast and VNN.com. VNN Live provided a satellite broadcast of news of events and interviews with subject matter experts (SMEs) as they occurred during the conduct of the T4 FSE. VNN.com complemented intelligence play by providing the media perspective on events that occurred prior to and during the T4 FSE.

The following scenario assumptions applied to the FSE:

- The scenario was plausible, and the events occurred as they were presented.
- Exercise players were well-versed in their own response operations, including plans and procedures.
- Exercise players responded in accordance with their existing plans, policies, procedures, and capabilities.
- All information provided in the narrative and/or by controllers was considered valid.
- There were no controlled time compressions, although the levels of play varied among agencies as discussed below.

The following artificialities and constraints were accepted to facilitate accomplishment of the exercise objectives. They may have detracted from exercise realism and also affect the analysis.

- Weather and atmospheric conditions at key points in the exercise were artificially defined to create a specific dispersal pattern of the agents involved in the exercise event. This was necessary to drive exercise play to meet the agreed-upon overarching and agency-specific exercise objectives determined during the T4 FSE planning process.
- Surrogates may have played in place of some key decision makers. The surrogates, in most instances, were junior to the principals they represented. Thus, the surrogates' actions during the exercise might not have depicted the same actions that would have been taken by their respective principals.
- Agencies, departments, and organizations not participating in the T4 FSE were simulated through the use of a SIMCELL. The SIMCELL representation of those non-participating agencies was determined by the agencies' published policies, procedures, and doctrine.
- VNN coverage was limited to eight hours per day, whereas real-world news outlets would have operated around the clock. This limitation was particularly significant in Guam, which, due to the time difference, received only four hours of live VNN average per day. In addition, the schedule of VNN was partly scripted, which limited the ability of PIOs to quickly air unscheduled statements and interviews.
- The levels and hours of play among agencies and organizations varied. Most agencies did not participate on a 24-hour basis. Some of the most notable gaps included the following:
  - There was no play overnight at the incident site in Oregon. Play halted on the evening of the first day just as some federal assets were arriving on scene.
  - Rescue play was halted on October 16 in Oregon because volunteer victims were in unsafe conditions due to inclement weather.
  - Play in Oregon was halted on October 18 at 1450 PDT until the following morning for safety reasons.
  - Coordination and communication between players in Guam and other venues was limited because of the time difference and lack of participation overnight in the other venues.
  - In Guam, the initial site assessment mission was completed within the first day of the exercise, but follow-on radiological deposition data collection activities were all notional due to a lack of players.
  - In Guam, the National Guard Civil Support Team (CST) completed their T4 objectives, and concluded their "boots on the ground" participation the morning of the second day of the exercise, prior to the initiation of the law enforcement activities and follow-on radiological deposition data collection (and before the other federal agencies arrived).
  - In Guam, Public Health reduced their level of play after their life saving/life safety mission was completed.
  - In Guam, representatives from DoE were deployed to represent full teams.
- There were several artificialities related to the collection of radiological data. Some of the most notable issues included the following:
  - In Oregon and Guam, radiological data collected in the field was often at a notional site. The Guam venue (unlike Oregon) did not have a pre-defined requirement or

sufficient resources to perform the conversion of location of field data gathered by local agencies and the CSTs.

- In Oregon, radiological data collection required a DoE controller equipped with a handheld device that provided GPS-linked data. There were not enough controllers to allow for simultaneous site assessment at both the incident site and downwind locations.
- In Arizona, radiological data collection activities were notional.

Exercise Evaluation Methodology

The evaluation approach for T4 is based on the methodology outlined in Homeland Security Exercise and Evaluation Program (HSEEP) doctrine and the methodology used in previous TOPOFF exercises. Observation and data collection identifies what happened during the exercise and when it happened. Findings and recommendations are then developed through reconstruction and analysis.[1] This overarching analysis focuses on interagency issues and coordination as put forth in the NRP, NIMS, and supporting policies and procedures. The analysis and AAR does not examine D/A-specific tasks, procedures, or performance. Many D/As conducted supporting evaluations and analyses of their exercise performance. This analysis uses and references some of these supporting evaluations.

HSEEP provides the common evaluation standards and was applied to the TOPOFF 4 evaluation as described in the EVALPLAN, Annex B of the T4 EXPLAN. The focus on interagency issues and coordination requires the synthesis and analysis of data collected from many different sites. For this reason, evaluation of T4 is a process that does not take place in individual exercise locations. Rather, data and observations collected from individual locations are consolidated, synchronized, and de-conflicted across locations so that evaluators can obtain a fact-based understanding of how agencies interacted to coordinate, make decisions, and execute national plans, policies, and procedures. Where gaps in the data existed, the evaluation team conducted post-exercise interviews with exercise participants to clarify exercise events.

This evaluation is limited by the quality of the data collected, by the exercise artificialities described above, and by exercise design and development decisions.[2] In the following analysis sections, it is noted where these limitations had an impact on the analysis.

[1] Appendix D provides a summary reconstruction of key events.
[2] Annex 1 provides a summary of lessons learned related to exercise design and development.

This page is intentionally blank.

SECTION 3: ANALYSIS OF CAPABILITIES

This section reviews national policy and planning issues related to the five exercised capabilities that are the focus of this report: On-Site Incident Management, EOC Management, Emergency Public Information and Warning, Economic and Community Recovery, and Intelligence/ Information Sharing and Dissemination.

The observations included in this report are organized by capability and corresponding activity, consistent with HSEEP guidelines. Within each activity are the related observations, including an analysis of that observation, and recommendations.[1] An IP based on the recommendations from this AAR and validated at the AAC is found in Appendix A. References are compiled in Appendix C and a timeline of key exercise events is included in Appendix D. Exercise artificialities are noted in the previous section on exercise design (Section 2).

Common themes linking observations and recommendations across capabilities are evident. For example:

- The challenges implementing incident site unified commands described under On-Site Incident Management form the basis of some of the coordination problems identified within the larger response structure (of which the incident site is one node), and are discussed under EOC Management.
- These command and coordination problems affected decision making, information sharing, and public messaging, and link to other issues described under EOC Management and Public Information and Warning, such as the allocation of low density/ high demand (LD/HD) assets, the demanding federal interagency operational cycle, and the communication of protective action guidelines.
- Information sharing and situational awareness challenges, described in EOC Management, affected all components of the response as well. One specific information management challenge, information overload experienced by PIOs, is also described under Public Information and Warning. Similar problems occurred in the sharing of intelligence information and are summarized under Intelligence/Information Sharing and Dissemination.
- Under Public Information and Warning, the difficulty explaining to the public why different jurisdictions took different actions is described. A similar issue could arise during the recovery phase, where the site optimization process for selecting clean-up standards could lead to different outcomes across jurisdictions, and is discussed in Economic and Community Recovery.

Capability 1: On-Site Incident Management

Capability Summary: On-site incident management is the capability to effectively direct and control incident management activities by using the incident command system (ICS) consistent with NIMS.

This capability was exercised in Guam and Oregon as local agencies responded to the incident

[1] Recommendations are included for all improvement areas and those strengths that lead to recommendations.

scene to direct and control incident management activities. Local response lasted from several hours to several days as federal assets deployed to the incident sites in Oregon and Guam. Incident commands transitioned to unified commands to manage resources and coordinate with on-scene agencies and appropriate EOCs and ECCs.

In both Guam and Oregon, the initial life safety mission was well executed, and first responders showed familiarity with basic incident command principles. In addition, National Guard WMD CSTs, which are state or territory assets that are federally trained and supported, were well integrated in the response. However, as the response management became more complex and nuanced, and the impact more widespread, local, state, territory, and federal personnel had more difficulty implementing incident/unified command principles. The table below provides a summary of the observations described under this capability along with associated recommendations, where applicable.

Table 3.1 Summary of On-Site Incident Management Observations

Observation	Recommendation
Activity 1.1: Implement On-Site Incident Management	
1.1.1 **Strength**: The initial life safety mission was well-executed by local, state, and territory responders.	
Activity 1.2: Establish Full On-Site Incident Command	
1.2.1 **Area for Improvement**: While the basic principles of NIMS-ICS are familiar to all emergency responders, there were challenges in implementing a command structure that met the needs of this complex RDD scenario.	More detailed procedures and training are necessary to implement unified command in complex scenarios. This should be addressed within the federal family of plans under development as well as within regional planning and training programs.
Activity 1.3: Resource Management	
1.3.1 **Strength**: National Guard WMD CSTs were valuable state and territory assets during these RDD incidents.	Further develop the ability of CSTs to effectively integrate into specific WMD Hazardous Materials (HAZMAT) responses.

Activity 1.1: Implement On-Site Incident Management

Observation 1.1.1 Strength: The initial life safety mission was well-executed by local, state, and territory responders. Local law enforcement personnel integrated with other first responders to perform site security and evidence protection, which supported the FBI-led law enforcement investigation that followed.

Analysis: Several first responders and homeland security policymakers in Guam and Oregon stated that first responder equipment, training, and exercising had progressed over the last several years, and greatly enhanced the ability of local assets to respond to a HAZMAT event.

In Guam, the life safety mission began soon after detonation at 6:03 p.m. EDT on Monday, October 15 (8:03 a.m. on October 16 in Guam). During the first three hours,

multiple D/As were involved, including the Guam Fire Department (GFD), Guam Police Department (GPD), Guam Emergency Medical Services (EMS), Guam Public Health, and the Guam National Guard 94th CST (see Figure 3.1). All teams reported to the incident commander, a member of the GFD. Additionally, Air Force and Navy Emergency Response Teams (ERTs) (HAZMAT, Explosive Ordnance Disposal (EOD), and firefighting) responded to the scene to provide support. The incident site command was supported by GHS/OCD through a mobile command center and an EOC Liaison Officer (LNO).

Portland Fire and Rescue begins establishing Incident Command.

The life safety mission proceeded in a similar fashion in Portland. The Portland Police Bureau (PPB) responded to the incident within minutes after the explosion, and implemented incident command soon after. Incident command passed from the PPB to Portland Fire and Rescue (PFR) within an hour of the explosion. At that point, local PFR HAZMAT units were on scene, and were joined hy the Oregon State Department of Human Services Public Health Division Radiation Protection Services (RPS) ERT and the Oregon National Guard 102nd CST within three hours. Together, they performed gross and technical decontamination on more than 150 casualties. PPB kept the incident site secure and preserved as much of the scene as possible for the ensuing law enforcement investigation.

Activity 1.2: Establish Full On-Site Incident Command

Observation 1.2.1 Area for Improvement: While the basic principles of NIMS-ICS are familiar to all emergency responders, there were challenges implementing a command structure that met the needs of this complex RDD scenario. These complexities included the following:

- The long-term and technical nature of the response due to the presence of radiological contamination.
- The requirements for many different types of missions, including establishing initial and ongoing scene safety, law enforcement incident investigation, evidence collection, radioactive deposition data collection, scene stabilization and hazard mitigation, and on-going scene recovery planning.
- Participation by many different local, tribal, state, territory, and federal agencies in the response.

As a result, responders in both venues had difficulty establishing clear unified command structures that met the needs of all participating agencies, coordinating multiple missions, and transitioning between missions. This led to delays in gathering and consolidating information to support decision making about issues, such as protective action recommendations and resource needs, as well as planning for recovery.

Analysis: Figure 3.1 shows the progression of missions accomplished at the incident sites in both venues, along with the command structures that were established to support each response phase. For the most part, the three basic missions of life safety, law enforcement incident investigation, and scene recovery occurred sequentially with little overlap.[2]

Figure 3.1 Incident Site Mission Area Activities and Assets

		+1 hour	+24 hours	+48
Guam		**Life safety**	**Crime scene investigation**	**Site assessment**
	IC	GFD	FBI	*DOE/EPA***
	Personnel/ Teams	GFD, 93rd/94th CST, GPD, Navy EOD	93rd/94th CST*	93rd/94th CST*, GFD*, DOE RAP*, EPA RERT
	Other missions	Very limited incident site assessment	Very limited incident site assessment	Robust rad. deposition data collection*

		+1 hour	+4 hours	+35 hours
Oregon		**Life safety**	**Crime scene investigation**	**Site assessment**
	IC	PPB → PFR	FBI and PFR	FRMAC
	Personnel/ Teams	PPB, PFR, RPS ERT	HMRU, 102nd CST, EPA NCERT	PFR, RPS ERT, 102nd CST, DoE RAP, EPA (inc. NCERT, RERT, NDT, ERT), USCG Strike team
	Other missions	Limited incident site assessment	Impact site closed, Radiological deposition data collection begins	FRMAC coordinates radiological deposition data collection

*Field work was notional (see the discussion in Section 2 artificialities for more information).
**DOE SEO at EOC/IOF; EPA On-Scene Coordinator for environmental response at incident site

Two key issues emerged:

- **Distinction between incident/unified command and site control:** In both venues, the FBI took control of the incident site after the conclusion of life safety activities to manage the law enforcement investigation. In Oregon, the FBI was part of a unified command; while in Guam, the FBI was the sole agency within incident command. In both cases, the FBI was perceived to be the lead agency for the entire response, and other activities, such as site assessment, were put on hold pending transition of command from the FBI to another agency.
- **Lack of flexibility to conduct missions simultaneously:** The NIMS-ICS structures established initially for life safety, and later for the law enforcement investigation, did not allow for the flexibility to begin activities unique to an RDD incident, such as site assessment. Site assessment includes defining the

[2] In Guam, the timing and sequence of missions during the exercise was impacted by the availability and participation of key response agencies. However, participants indicated that the observed missions would still have occurred sequentially if this had been a real-world event.

radiological "footprint", which includes the size, scope, and boundaries of the deposited material, to support the leadership when making decisions about public health and environmental protective actions and recovery. Although local responders in Guam (such as Navy EOD and the 94th CST) were available to begin initial site assessment and did collect some data, there was no comprehensive plan to define the size and scope of the incident until the EPA began developing a formal site assessment plan two days after the explosion. [3] In Portland, CST and EPA responders initially assisted in the life safety mission. When DoE personnel arrived, site command was in transition from PFR to FBI. As a result, DoE, EPA, Multnomah County Health Department, Oregon State RPS, and PFR HAZMAT met separately to discuss the public health component of the response and the necessary site assessment mission.[4] Soon thereafter, the incident site was shut down for the evening, which stalled the initiation of site assessment activities.[5] The following day, the Federal Radiological Monitoring and Assessment Center (FRMAC) assumed responsibility for the site assessment mission.[6]

The two issues described above led to delays in gathering and consolidating information to support decision making and issue identification and resolution. For example, additional site assessment data could have supported the development of protective action recommendations, prevented post-blast contamination of personnel and equipment, and supported federal resource requests. These problems also delayed clean-up and recovery planning and the consideration of issues such as the storage, transport, and disposal of contaminated material, and the need for additional laboratory surge capacity.

Similar problems establishing efficient on-site incident command structures were observed in T2 and T3. Furthermore, these problems are part of a larger issue of unified coordination across all levels of government, of which incident sites are one such node. This issue is discussed further in observation 2.3.4.

Recommendations: This exercise demonstrated that more detailed planning is necessary to prepare local, state, and territory responders to implement on-site unified command in complex scenarios. This should be addressed within the federal family of plans under development, as well as within regional planning and training programs. Regional planning is important for developing unified command structures that meet the needs of all agencies and missions within specific scenarios and account for the unique characteristics of different localities.

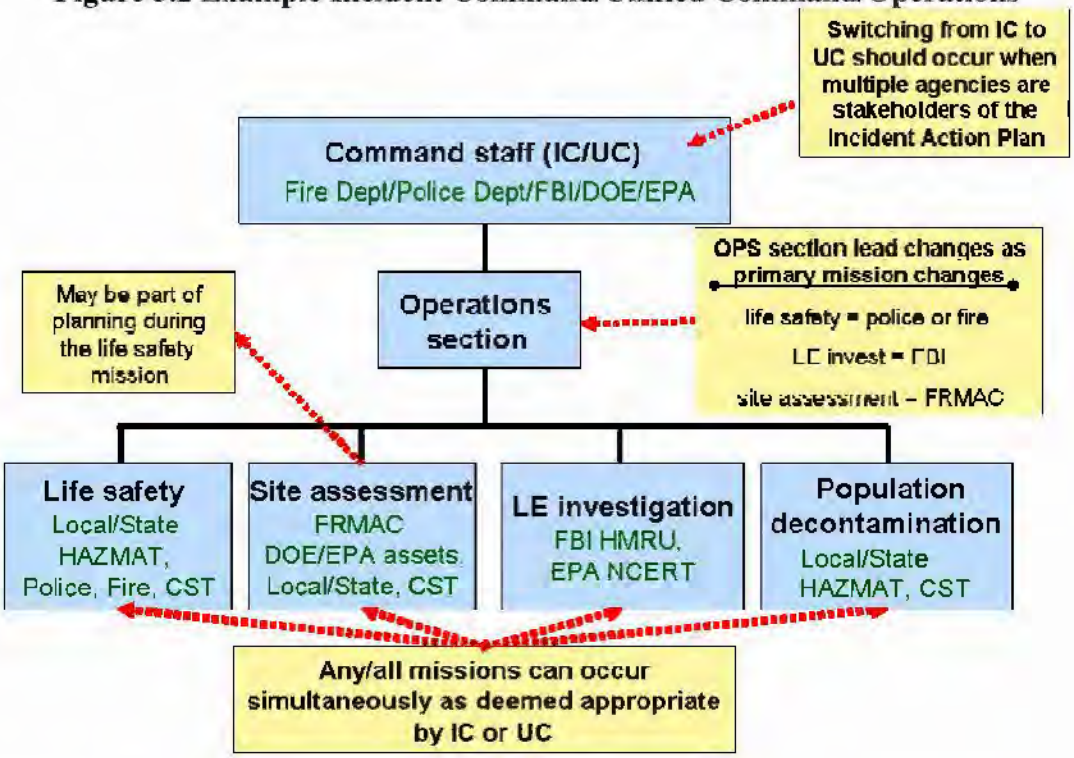
1. National scenario-based guidance (linked to the national planning scenarios) should be developed to support NIMS implementation. DHS should establish an interagency working group with appropriate SMEs and first responders from the local, state, tribal, territory, and federal levels to help develop this guidance. The

[3] See Section 2 for a discussion of artificialities related to data reporting by the CST.
[4] Coordination between the incident site unified command and the public health unified command is discussed in more detail in observation 2.3.4.
[5] See Section 2 for a discussion of artificialities related to radiological data collection in Oregon.
[6] FRMAC management of site assessment is discussed in more detail in observations 2.1.3 and 2.1.4.

guidance should identify scenario-specific mission needs and provide a more detailed framework for establishing unified command structures that address all of these needs. Figure 3.2 shows an example of such a command structure; one that provides flexibility to support the needs of multiple missions in the context of this scenario. In this context, once a mission is established under operations, one D/A could be designated as the lead, depending on current capabilities and response time to the scene, but the command staff would remain consistent.

2. Because every state and territory has its own unique structures, authorities, and requirements, this national guidance should be implemented at the regional level, and supported through regional planning, training, and exercise programs, such as FEMA's Regional Interagency Steering Committees (RISC).

Figure 3.2 Example Incident Command/Unified Command/Operations



Activity 1.3: Resource Management

Observation 1.3.1 Strength: National Guard WMD CSTs were valuable state and territory assets during these RDD incidents.

Analysis: The capabilities of the CST teams that responded to Oregon and Guam were well suited to the response, and the teams integrated easily with local capabilities. In Oregon, the 102nd CST was on-site within three hours after the detonation. This team gave assistance to HAZMAT, Bomb Squad, FBI, and DoE RAP personnel in the decontamination line and joined the radiological data collection teams that worked jointly

within the FRMAC. In Guam, the 94th CST was on-site one and a half hours after the detonation. This team provided assistance during the first joint site entry with GFD and Navy EOD, and conducted a relief in place with the Hawaii National Guard 93rd CST deployed from Honolulu.[7]

The standard operating guidelines for how the CSTs function is well-defined in the document, "Weapons of Mass Destruction Civil Support Team Tactics, Techniques, and Procedures."[8] However, similar to the issues with NIMS described previously, this document does not provide scenario-specific guidance or operational-level details, such as specific mission examples.

Recommendations: To improve the ability of CSTs to effectively integrate into WMD HAZMAT responses, consider the following:

1. Integrate CSTs into national and regional planning initiatives to align CST SOPs and tactics, techniques, and procedures (TTPs) with national and regional response plans for specific scenarios. Clarify CST functions in national-level doctrine, such as the NRF and the Nuclear/Radiological Incident Annex.
2. Review and consider enhancements to the current CST equipment caches. For example, the 94th CST in Guam did not have enough radiological detection meters or communication equipment to properly carry out its mission. In Portland, the 102nd CST did not have enough meters.
3. Continue joint training and exercising between CSTs and FBI, EPA, DoE, and various HAZMAT teams at all jurisdictional levels.

Capability 2: EOC Management

Capability Summary: EOC Management is the capability to provide multi-agency coordination for incident management by activating and operating an EOC for a pre-planned or no-notice event. EOC Management includes: EOC activation, notification, staffing, and deactivation; management, direction, control, and coordination of response and recovery activities; coordination of efforts among neighboring governments at each level and among local, regional, state, and federal EOCs; coordination of public information and warning; and maintenance of the information and communication necessary for coordinating response and recovery activities. EOCs may include the National (or Regional) Response Coordination Centers (NRCC or RRCC), JFOs, National Operations Center (NOC), Joint Operations Centers (JOCs), Multi-Agency Coordination Centers (MACCs), and Interim Operating Facilities (IOFs).

During T4, EOCs and ECCs activated at all levels of the government to deploy assets, coordinate the response, and share information. At the local, state, and territory levels, EOCs and ECCs activated in response to the explosions. At the federal level, agencies such as DHS, DoS, the FBI, HHS, DoE, and the EPA stood up their headquarters operations centers along with NGOs.

[7] The CST in Guam could have been available for follow-on radiological data collection during the law enforcement incident investigation and preliminary recovery operations. However, they had completed their T4 objectives, and concluded their participation the morning of the second day (before the other federal agencies arrived). For more on this issue, see the exercise artificialities in the exercise design section.
[8] FM 3-11.22, Department of the Army Headquarters, June 2003.

such as the ARC, and private sector entities, such as the Business Operations Center (BOC) in Arizona. Later in the response, IOFs and JFOs were established in the venues to coordinate federal support to state and local responders.

The observations discussed under this capability focus on response management, direction, and control (including decision making), the coordination of response activities among all levels of government, and information sharing. For example, there were new teams and tools introduced during the exercise, which were intended to improve information sharing, but D/As at all levels of government still had difficulty obtaining accurate and consistent critical information. The federal interagency battle rhythm was overly demanding throughout the exercise, which contributed to these information management challenges. Radiological data collection and distribution of IMAAC products was well coordinated, but key decision making nodes were not always well coordinated or well integrated into a unified coordination and management structure. This delayed decision making and made it difficult to develop clear public messages. In addition, the requirements for LD/HD assets were stressed.

The table below provides a summary of the observations described under this capability along with associated recommendations, where applicable.

Table 3.2 Summary of EOC Management Observations

Observation	Recommendation
Activity 2.1: Gather and provide information	
2.1.1 **Strength:** New teams and tools designed to improve coordination, information sharing, and real-time planning, were tested at all levels of government.	
2.1.2 **Area for Improvement:** D/As at all levels of government, as well as international participants, had difficulty obtaining critical information and maintaining situational awareness.	Continue to develop and test situational awareness tools and supporting processes and procedures. Focus first on the most critical pieces of information desired by leadership.
2.1.3 **Strength:** Radiological deposition data collection and management in Oregon was well coordinated.	
2.1.4 **Strength:** IMAAC provided consequence predictions to agencies and officials in all three venues and the federal interagency, and there were no conflicting plume models as was observed during T2.	
Activity 2.2: Prioritize and Provide Resources	
2.2.1 **Area for Improvement:** The exercise was designed to stress the requirements for LD/HD assets like the FRMAC, the Domestic Emergency Support Team (DEST), and other protection assets.	Incorporate more details in the national family of plans on the allocation of specific LD/HD response and protection assets that could be required to respond to multiple incidents. Identify assets that can partially replicate LD/HD capabilities, and consider alternative means to augment these capabilities.
Activity 2.3: Support and Coordinate Response	

Table 3.2 Summary of EOC Management Observations

Observation	Recommendation
2.3.1 **Area for Improvement:** The federal interagency operational cycle was overly demanding throughout the exercise.	Establish a framework for the federal interagency operational cycle that can be adapted during times of emergency
2.3.2 **Area for Improvement:** The purpose, definitions, and consequences of HSAS threat levels are not clear.	Review and clarify policy surrounding the HSAS. Clarify the purpose of the HSAS, its link to threat information, and its intended consequences.
2.3.3 **Strength:** There was effective coordination between DoE and EPA field teams and officials that deployed to Guam and Oregon.	
2.3.4 **Area for Improvement:** There were significant challenges in Oregon regarding implementation of an effective unified coordination structure that linked all coordination nodes and addressed the complexities of the event.	Develop concepts and mechanisms within the national family of plans to facilitate a "unified management of the federal response." Clarify the relationship between ESF-10 and the Nuclear/Radiological Incident Annex in the NRF. Develop national-level guidance on how best to integrate the FRMAC into the overall coordination structure.
2.3.5 **Area for Improvement:** Some agencies had difficulty integrating their Senior Federal Officials (SFOs) into the JFO structure.[9]	Review and clarify the roles and responsibilities of SFOs in the policies, procedures, and training that support the JFO.
2.3.6 **Strength:** The participation by private sector and Critical Infrastructure/Key Resources (CI/KR) organizations was the largest of any national-level exercise to date.	Continue to institutionalize and formalize relationships between government, private sector, non-government, and CI/KR organizations.
2.3.7 **Area for Improvement:** The mechanisms for private sector and NGO integration into emergency response structures are not clear.	Clarify private sector and NGO partnerships in policies and the national family of plans. Articulate and institutionalize a process for private sector and NGO engagement in national-level exercises.
2.3.8 **Strength:** Disability and other special needs play was a major focus area in the exercise design.	Continue to incorporate and expand special needs play within national-level exercises.
2.3.9 **Strength:** Foreign consular involvement and consular operations were successfully exercised.	
2.3.10 **Area for Improvement:** The procedures for accepting cash donations and diplomatically critical donations through the International Assistance System (IAS) are unclear.	Clarify the relationship of the IAS Concept of Operations (CONOPS) and the procedures for accepting both diplomatically critical and cash donations.

[9] The new NRF released after the exercise shortened this term to Senior Official (SO) to be inclusive of state, territorial, tribal, and local officials.

Activity 2.1: Gather and Provide Information

Observation 2.1.1 Strength: New teams and tools designed to improve coordination, information sharing, and real-time planning, were introduced at all levels of government. For example, DHS posted the National Situation Report (SITREP), Interagency Modeling and Atmospheric Assessment Center (IMAAC) plots, and other event information to the HSIN COP portal for other D/As to access. This information sharing tool was not available during Hurricane Katrina and previous TOPOFF exercises.

Analysis: DHS and other agencies have been working to address information sharing shortfalls that occurred during the response to Hurricane Katrina. Similar problems were also observed in previous TOPOFF exercises. T4 provided an opportunity to rigorously test these improvements. As discussed below, further improvement is necessary to support and maintain situational awareness among agencies. Nonetheless, these entities and tools did not exist previously, and are a step in the process of addressing this issue.

The DHS CAT stood up in the NOC to monitor and consolidate information into National SITREPs and to conduct real-time planning. The NOC components, including the NRCC and National Infrastructure Coordinating Center (NICC), also activated and supported the development of the National SITREP. HSIN and the new COP portal were used to provide situational awareness to the federal interagency. T4 provided an opportunity to test new processes and procedures for maintaining HSIN and the COP. The COP was used primarily to display information about the events and to produce and disseminate the National SITREP. It provided a readily accessible source for many agencies to read or download the SITREP, obtain copies of IMAAC consequence predictions, and access basic information about the events. Other portals within HSIN served as repositories for additional event documentation.

Similar tools were used and tested at other federal agencies as well as at the state, territory, and local levels. For example, DoS used a web-based crisis management portal, which provided key information and reference materials to DoS personnel. The FBI operated four Law Enforcement Online Virtual Command Centers (VCCs), which allowed for transmission of sensitive but unclassified information between the participating FBI field offices and territorial authorities in Guam. HHS used WebEOC, to which it has been adding functionality and capability. Portland used WebEOC to share information with other local and federal agencies, and Guam used DisasterLAN to share information with other federal and territory agencies.

Observation 2.1.2 Area for Improvement: D/As at all levels of government had difficulty obtaining critical information and maintaining situational awareness. Although the HSIN and COP provided easy access to some information, other information was not readily available. Senior decision-makers were most interested in IMAAC model results, casualty counts, information on protective actions, and the status of federal resources. With the exception of the IMAAC model results, this information was among the most difficult for DHS to collect.

Analysis: Table 3.3 shows the draft Critical Information Requirements (CIRs) defined as part of the RDD Strategic Plan.[10] As shown, these CIRs fall into two basic categories: information that originates at the local level and information that originates at the federal level. In some cases, information originates at both levels.

Table 3.3 RDD Critical Information Requirements

CIR	Local	Federal	Primary Source
*Initial/Updated Assessments	X		State/Local EOCs
Initial/Updated Hazard Data Products		X	IMAAC
*Protective Actions Taken or Suggested	X	X	Multiple State/Local/Federal
Law Enforcement Activities/Actions	X	X	Multiple, compiled by LNO
Threat Assessments		X	Multiple, compiled by LNO
Transportation Corridors Affected	X	X	NICC
Infrastructure Damage Assessment	X		NICC
Status of First Responders	X		State/Local EOCs
*Contamination Control Centers/Lines	X		State/Local EOCs
COOP/COG Issues (Federal, State, Local)	X	X	Multiple State/Local/Federal
*Status of Federal Capabilities and Resources		X	Multiple Federal
Recommended Location of JFO		X	FEMA
Status of Search and Rescue Operations	X		*Not defined*
Status of Fire Suppression Operations	X		*Not defined*
Evacuation Routes	X		Multiple State/Local/Federal
Status of Local Medical Communities	X		*Not defined*
Medical Resources Deployed		X	*Not defined*
Nuclear Incident Response Team Assets Deployed		X	DoE, FEMA
Red Cross Housing Centers		X	ARC
International Impacts		X	DoS

The CAT assumed the role of collecting these CIRs and incorporating them into various products and tools, such as the National SITREP, HSIN/COP, and briefings. As components of the NOC, the NRCC and NICC play a primary role in collecting the CIRs and other information defined in the National SITREP. The timeliness and accuracy of this information varied. CIRs noted with an asterisk (*) were the most problematic. Often these same CIRs were also of the most interest to senior leadership and decision makers.

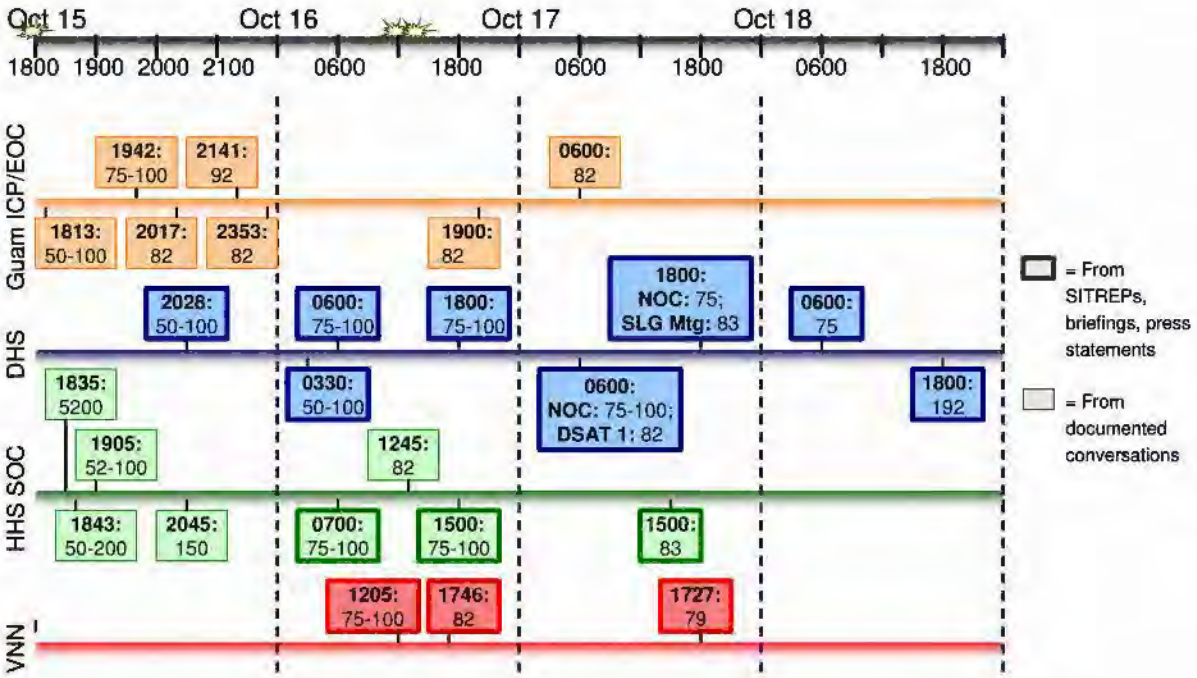
Information originating at the local level is collected from a variety of sources. Initially, the NOC contacts state and local EOCs or obtains information via the RRCC and NRCC. Once the JFO stands up, it becomes the primary conduit for this information. Figure 3.3 tracks one example of local information – the number of casualties reported in Guam.

In Guam, initial reports of casualties were ranges: 50 to 100 and 75 to 100. The final number of casualties reported at the local level was 82. Although this number was reported as early as the evening of October 15, it never appeared in the National SITREP, which continued to report the range of 75 to 100, and then settled on 75. Note that DHS

[10] These CIRs were drawn from a briefing presented during CAT training, and represent a draft set of CIRs that were presented to the group. Some CIRs were not yet fully defined, and did not include information on the source.

field elements, including the DHS Situational Awareness Team (DSAT) and the Principal Federal Official (PFO), had information reporting 82 and 83 casualties, respectively.

Figure 3.3 Guam Casualties



The CAT worked to provide exact numbers of casualties, injuries, and fatalities. However, reporting the range of 75 to 100 casualties was not incorrect since the actual number fell within this range. One main reason for collecting information on casualties is that it is an indicator of the need for federal support. As such, it is the magnitude of the number that matters, and the difference between 75 and 82 is not significant. However, the initial misreporting of 5,200 casualties by HHS, reported at 6:35 p.m. EDT on October 15 in the Secretary's Operation Center (SOC) (their interpretation of the spoken "50 to 100") was significant. This misreport was quickly corrected (shown in Figure 3.3).

Reports of casualties are also problematic because the terms reported often vary. Casualties typically include all injuries and fatalities. Sometimes, just injuries are reported, and these may be broken down by their severity or whether or not they were hospitalized. Reports of fatalities were generally more consistent than reports of injuries and casualties. Other information originating locally often varied in consistency and included numbers of persons evacuated, sheltering in place, or decontaminated, as well as the locations of evacuation and shelter-in-place areas.

Information originating at the federal level that was of interest to senior leaders and decision makers included IMAAC model results, threat assessments, and the types of federal capabilities at the scene. In general, information with a designated federal source was readily available. One example is the IMAAC models. CAT members could

download these products directly from HSIN or the IMAAC website and include them in the SITREP.

Information requiring the consolidation of data from multiple agencies was the most difficult to obtain. Examples include federal assets on scene, referred to as "blue forces" on HSIN/COP, and the protective measures being taken by federal agencies in response to HSAS levels. The CAT sent out requests for information (RFIs) for these CIRs on multiple occasions during the exercise, but received little information in response. Within the COP portal, the information available under blue forces was incomplete.

HSIN and the COP portal are relatively new tools that are not yet fully developed. Many users lacked experience and training on the tools. In the NRCC, a critical node for collecting and posting much of the information on HSIN, much of the staff spent the early part of the exercise gaining familiarity with the system which delayed other actions like future planning. Technical issues contributed to problems with gathering and displaying information. The terrorism SITREP could not he generated directly within the COP portal at the time of the exercise, although this upgrade is planned. During the exercise, staff had to cut and paste information from COP and other sources into a separate document, which added time to the development of the National SITREP and left less time for review and editing. These technical issues have been documented by the DHS Office of Operations Coordination and corrective actions are being implemented.

Although information accuracy and timeliness varied for the CIRs, a great deal of information was available on HSIN that was not available during previous TOPOFFs or Hurricane Katrina. Still, many agencies complained that they did not have situational awareness and that it was too hard to find information on HSIN. HSIN contains many different portals, and often different information was available in each. Agencies had to monitor these multiple portals in addition to their own systems and there was not a single comprehensive source for incident information. The most substantive source of information on HSIN/COP was the National SITREP. This document was often close to 30 pages in length, and information about the CIRs was sometimes located within the extensive ESF reports or other sections, requiring the reader to review the entire document in search of particular pieces of information. Although there is an Executive Summary, the HSC and other users were not satisfied with its content.[11]

As it was for many agencies, information overload was an issue for the CAT, which had to mine various e-mail inboxes and HSIN sites for information to include in the SITREP and in the COP. Observation 3.1.2 in the Public Information and Warning capability provides a more detailed account of information overload experienced by PIOs.

Recommendations: Continue to develop and test situational awareness tools and supporting processes and procedures. The DHS Office of Operations Coordination is already taking action on a lengthy list of recommendations derived from internal AARs which focused on many of the issues raised above.[12] In addition:

[11] Homeland Security Council T4 Lessons Learned, DHS Action Items, November 9, 2007.
[12] DHS/OPS T4 Corrective Action Prioritization Tool, December 13, 2007.

1. Work with the federal interagency through the existing HSIN working group to further develop the requirements for situational awareness and the federal COP. Consider focusing first on the few key elements of information that were of primary interest to decision makers and then developing the processes and procedures for collecting, validating, and displaying this information. Consider graphical displays or other ways to make information easier to find and understand.
2. Consider reporting numbers as ranges, rather than point estimates, during the first 48 to 72 hours of a response.

Observation 2.1.3 Strength: Radiological deposition data collection and management in Oregon was well coordinated.[13]

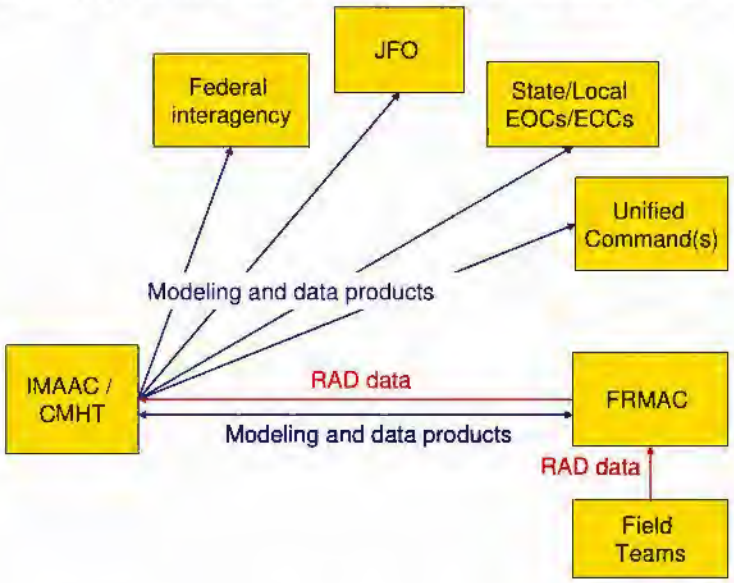
Analysis: Prior to the arrival of federal assets in Oregon, radiological data collection was managed by PFR HAZMAT. Data collected were sent to IMAAC and the National Nuclear Security Administration (NNSA) Consequence Management Home Team set up for the Oregon incident (CMHT/OR)[14] and used to refine the preliminary plume model results. EPA responded under statutory authority of the National Oil and Hazardous Substances Pollution Contingency Plan after the EPA Region X Emergency Operating Center (REOC) observed reports of the explosion on VNN. DoE RAP Region 8 was activated by NNSA and was contacted en route by PFR HAZMAT and EPA. Upon arrival, DoE and EPA coordinated with PFR HAZMAT, as well as the 102nd WMD CST and the Oregon State Department of Human Services Public Health Division RPS ERT, to manage radiological data collection at the incident site.

Upon arrival, the FRMAC took over responsibility for the coordination and management of all radiological deposition data collection efforts in accordance with general FRMAC operating guidelines and the Nuclear/Radiological Incident Annex. This is shown in red in Figure 3.4. All radiological field teams, including PFR HAZMAT, Oregon State RPS ERT, 102nd CST, DoE RAP teams, EPA National Counter-Terrorism Response Team (NCERT), EPA Radiological Emergency Response Team (RERT), EPA National Decontamination Team (NDT), EPA Environmental Response Team, and USCG Pacific Strike Team, were fully integrated into the FRMAC structure and tasked for data collection missions by FRMAC leadership. Data collected at the incident site and data collected to characterize the radiological footprint were sent to the FRMAC. The FRMAC continued to share radiological data with IMAAC and the CMHT/OR to further refine the deposition models.

This represents significant improvement over what was observed during T2, where deposition data collection efforts were haphazard and data management was uncoordinated and decentralized.

[13] Radiological data collection efforts were notional in Arizona. In Guam, data was collected on the first day of the exercise, but was notional once DoE and EPA arrived.
[14] CMHTs provide logistical support, develop initial effects predictions and assessments, and provide expert advice to field teams.

Figure 3.4. Radiological Data Collection and Product Distribution in Oregon



Observation 2.1.4 Strength: IMAAC provided consequence predictions to agencies and officials in all three venues and the federal interagency, and there were no issues with conflicting plume models as was observed during T2.

Analysis: Processes established after T2 to minimize differences in plume model outputs and provide one source for consequence predictions appeared to be effective. The product distribution process for Oregon is also shown in Figure 3.4. An IMAAC consequence prediction was requested by PFR HAZMAT soon after the initial explosion. Radiological deposition data were collected and shared with IMAAC and the CMHT/OR to further refine the model results. Once products were approved, they were posted to the IMAAC website and on HSIN in accordance with IMAAC SOPs. There were also regular conference calls hosted by IMAAC and the CMHT/OR to discuss radiological data collection strategies, product development, and interpretations and assessments.

Upon arrival, the FRMAC continued to coordinate with IMAAC and the CMHT/OR to further refine the deposition models. Once enough radiological data was collected, the FRMAC produced a deposition data product, which depicted the actual radiological deposition footprint. The FRMAC deposition data product was also available on the IMAAC website and posted on HSIN.

While data collection and management was partially simulated in Arizona and Guam, there was still coordination between the venues, IMAAC, and CMHTs set up for the Arizona and Guam incidents, respectively. IMAAC consequence predictions were requested soon after the explosions in Guam and Arizona, and IMAAC modeling and data products were distributed in the same manner as in Oregon.

Observation 2.2.1 Area for Improvement: The exercise stressed the requirements for LD/HD assets like the FRMAC, the DEST, and other protection assets. Limited availability of first-line assets like the FRMAC was addressed by using assets from other agencies. However, because much of the outcomes were pre-scripted and notionalized in the exercise (the FRMAC was scripted to go to Oregon, no products were developed in Guam and Arizona using deposition data), it is unclear whether the gaps were adequately filled. Plans for deploying protection assets, such as DoE search teams and DHS Visual Intermodal Protection and Response (VIPR) teams were developed by the CAT in response to taskings that arose in senior leadership meetings. Although decisions were made and actions taken, there was no formal process for adjudicating competing needs for LD/HD assets.


FRMAC members conduct sampling in Oregon.

Analysis: T4 stressed the requirements for LD/HD assets like the FRMAC, the DEST, and other protection assets.

FRMAC. Table 3.4 shows how FRMAC-like capabilities were assembled in Guam using available radiological response assets.[15]

Table 3.4 FRMAC Capabilities Replicated in Guam

Capability	FRMAC	Used in Guam
Monitoring	Field monitoring	Local HAZMAT, CST, DoE RAP (notional), EPA
Monitoring	Aerial Measuring System (AMS)	DoD (notional)
Assessment	Dose assessment	DoE and EPA officials
Assessment	GIS	No indication that Guam had GIS capability
Assessment	Data management	CMHT
Assessment	Modeling and deposition data products	IMAAC, CMHT (modeling only)
Health and Safety	Medical (REAC/TS)	Accessed by phone
Health and Safety	Safety	Guam and federal OSHA
Laboratory	Laboratory analysis	No laboratory analysis available

[15] Since Arizona field activities were all notional, no meaningful comparison can be made.

The FRMAC capabilities are separated into the four primary response categories of monitoring, assessment, health and safety, and laboratory analysis:[16]

- **Monitoring.** Guam HAZMAT, the 93rd and 94th National Guard WMD CSTs, and notional DoE RAP teams and EPA field teams fulfilled monitoring responsibilities during the exercise, although on a much smaller scale than the FRMAC. In addition, DoD notionally provided aerial monitoring before DoE and EPA arrived.
- **Assessment.** Assessment consists of several functions, including data management, Geographic Information System (GIS) modeling, and the provision of subject matter expertise. DoE and EPA senior officials provided dose assessment and interpreted IMAAC products for decision makers in Guam. Additional support was available via the Guam CMHT. The Guam CMHT also fulfilled data management responsibilities (although these activities were mostly notional). IMAAC, as discussed earlier, in coordination with the Guam CMHT, provided modeling capability.[17] Finally, Guam did not use any GIS assets during the exercise, and this capability did not appear to be available within the local government.
- **Health and safety.** DoE and EPA officials in Guam were in telephone contact with Radiation Emergency Assistance Center/Training Site (REAC/TS) personnel, who provide treatment and medical consultation for injuries resulting from radiation exposure. Guam OSHA and federal OSHA were also present to monitor safety concerns.
- **Laboratory analysis.** This function went unfulfilled in Guam, and it was recognized as a significant shortfall during the exercise.

The response in Guam was able to replicate some of the FRMAC capabilities, but there clearly would have been shortfalls in a real-world response to multiple incidents. Potential additional sources for FRMAC capabilities are shown in Table 3.5.

Table 3.5 Additional Sources for FRMAC Capabilities

Capability	FRMAC	Potential Additional Sources
Monitoring	Field monitoring	DoD, international
Monitoring	Aerial Measuring System (AMS)	
Assessment	Dose assessment	
Assessment	GIS	DoD, private sector
Assessment	Data management	
Assessment	Modeling and deposition data products	CMHT (modeling and data products)
Health and Safety	Medical (REAC/TS)	
Health and Safety	Safety	
Laboratory	Laboratory analysis	International

[16] National Nuclear Security Administration, FRMAC Operations Manual, December 2005.
[17] As discussed earlier, due to exercise constraints, IMAAC and CMHT only provided plume modeling products during the exercise. No attempt was made to generate data products based solely on deposition data.

They include:

- **Monitoring.** DoD assets could be requested, and international support could augment this function in areas that are a significant distance away from the U.S. mainland.
- **Assessment.** Providing GIS capability presents a challenge, but it is plausible that this function could be obtained from DoD or the private sector. The CMHT has the capability to provide FRMAC-like data products based on deposition data. Another potential solution is not to deploy the early-phase assessment functions. Leaving some capabilities to be conducted by the CMHT, and not forward deployed, would enable those capabilities to be available for other incidents in the event of multiple events.
- **Laboratory analysis.** Several ideas were suggested during the exercise to provide this capability, including putting together an EPA mobile lab and/or arranging for international support.

DEST.[18] The DEST is an interagency on-call team of terrorism experts who provide support to the FBI Special Agent in Charge (SAC) during domestic WMD terrorist threats or incidents.

During T4, the DEST deployed to Oregon in real time. The DEST mobilized one hour after the explosion in Oregon and departed for Oregon within four hours. Upon arrival in Portland, the DEST experts integrated into the FBI JOC. DEST personnel coordinated with their own agency response elements on scene to provide information flow to and from the FBI SAC/JOC, which is in accordance with DEST procedures.[19] In addition, DEST personnel worked with their own agency counterparts on scene to transition support to the JFO after the JOC ended operations.[20]

There were limited discussions in senior leadership meetings about deploying the DEST to any of the incident sites. Soon after the explosion in Guam, a decision was made to put the DEST on standby rather than deploy it to Guam. However, no formal decision was made to deploy the DEST the following day after the explosion in Oregon and Arizona.[21] FBI controllers suggested that senior leadership did not have enough familiarity with the capabilities of the DEST to support decision-making regarding activation and allocation.

Protection assets. Several types of protection assets were employed during the exercise:

- The DHS CAT Planning Section developed a search plan using DoE teams, which were notionally deployed on October 17.
- The DHS CAT Planning Section also developed a VIPR plan to provide security and visual deterrence at CI sites in four cities. It was developed overnight on October 18, but the exercise ended before these teams were notionally deployed.

[18] This observation was drawn from FBI input into the AAR process.
[19] Due to the artificial nature of the deployment, some DEST personnel were underutilized in Oregon.
[20] The FBI JOC ceased operations when the law enforcement phase of the exercise concluded, which was an exercise artificiality.
[21] The deployment of the DEST to Oregon was pre-scripted, and the asset deployed despite the fact that senior leaders at the deputy and principal level never formally decided to deploy the DEST.

- DHS proposed Immigration and Customs Enforcement (ICE) support to FBI to enact a "round up" plan to arrest and question persons with possible links to terrorism.

These actions were driven by discussion and decisions in senior leadership meetings, and were unanticipated by some of the players that were called on to develop deployment and other plans to support the decisions. The draft RDD Strategic Plan, which many DHS players used as a road map for the response, does not currently address protection activities. Plans for deploying protection assets were developed by the CAT in response to taskings that arose in senior leadership meetings. Some meeting participants were unfamiliar with the CAT and were surprised to see it play an active role in developing protection plans.

SOs participating in the Principals SVTC felt that there was an unnecessary delay in deploying these protection assets. Although decisions were made, there was no formal process for adjudicating competing needs and making and disseminating decision outcomes (see related observation 2.3.1). In addition, decisions and actions were not well linked with exercise intelligence. For example, the cities selected for VIPR deployment were not based on exercise intelligence, although this could have been an artificiality of the exercise.

Recommendations: Decisions regarding scarce resources should be incorporated into scenario-based plans. The DHS Office of Operations Coordination is already implementing corrective actions raised by the HSC and its own after-action process that address some of these recommendations:

1. DHS, in coordination with the federal interagency, should incorporate contingency plans for multiple RDD/IND incidents into the Strategic Plans and identify assets that can partially replicate LD/HD capabilities. In addition, the HSC called for a database of radiological assets to be developed.[22]
2. DoE and EPA should investigate the cost/benefit of NOT deploying the early phase assessment functions of the FRMAC to an incident site. In addition, DoE and EPA, in coordination with DHS, DoD, and DoS, should explore options to bolster monitoring and laboratory capabilities through Memoranda of Understanding (MOU) or pre-scripted mission assignments with DoD and foreign countries that are closer to U.S. states and territories.
3. DHS, in coordination with the federal interagency, should account for protection assets and capabilities in the national family of plans, including the RDD Strategic Plan, NRF, and the Nuclear/Radiological Incident Annex.
4. DHS, in coordination with the federal interagency, should clarify agency roles and responsibilities regarding protection assets, as well as the role of CAT in developing deployment plans.
5. DHS, in coordination with the federal interagency, should develop a training package and decision matrices for senior leadership describing the capabilities

[22] There have been past efforts to develop similar databases, such as the Response Resource Inventory System. Efforts to develop a new database of radiological assets should begin with this and other existing databases.

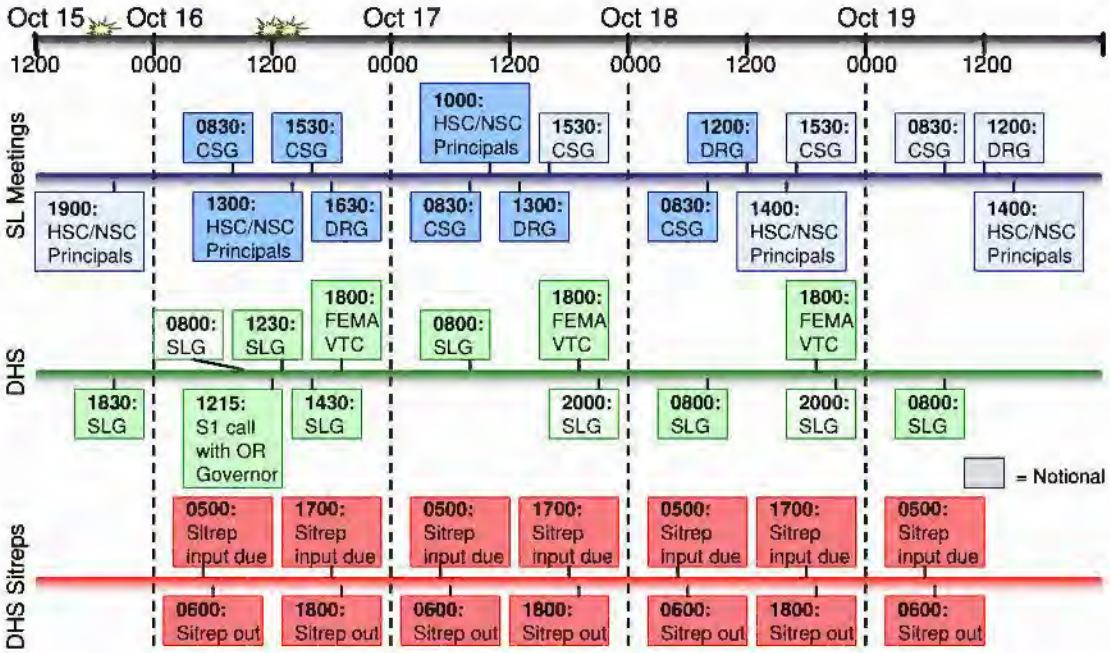
and deployment of existing radiological response assets, including the DEST, and protection assets.

Activity 2.3: Support and Coordinate Response

Observation 2.3.1 Area for Improvement: The federal interagency operational cycle (often termed battle rhythm) was overly demanding throughout the exercise. Senior leadership meetings, such as the Domestic Readiness Group (DRG) and Counterterrorism Security Group (CSG), coupled with SITREP deadlines and press briefings, created an unrealistic workload for interagency operations center staff such as the DHS CAT and the HHS Emergency Management Group (EMG). In addition, formal summaries were not distributed from these meetings, requiring staffs to rely on informal back-briefs from participants. Both of these problems contributed to inaccuracies and inconsistencies in the information conveyed in products such as situation reports and leadership briefs (discussed in 2.1.2).

Analysis: Figure 3.5 shows the main components of the operational cycle. Senior leadership meetings are shown along the top and include the HSC/NSC principals meetings along with the CSG and DRG. Although this schedule was pre-set for the exercise, it is thought to be similar to what would occur during an actual emergency.

Figure 3.5 T4 Operational Cycle



DHS-hosted meetings are shown in the middle of the figure. The Senior Leadership Group (SLG) was a conference call hosted by the NOC and included the DHS components and the PFOs and Federal Coordinating Officials (FCOs). The FEMA Video Teleconferences (VTCs) are operational-level calls hosted by the NRCC that include ESF partners and FEMA field components. Other agencies, like HHS and EPA, hosted their

own operational-level calls with their components and field teams. National SITREP reporting deadlines are shown along the bottom.

As shown in Table 3.6, there was considerable overlap in the topics discussed at all of the senior leadership meetings. Documentation of meeting participation was not available; however, it was reported to the evaluation team that there is little overlap in the membership of these groups.

Table 3.6 Topics Discussed in Senior Leadership Meetings

Principals SVTC	CSG	DRG	DHS SLG
• Intelligence and law enforcement • Situation updates • HSAS • Continuity of Government Readiness Conditions (COGCON) • Federal resource allocation • Protection activities • International issues	• Intelligence and law enforcement • Intelligence sharing • Situation updates • HSAS • COGCON • Federal resource allocation • Protection activities • International issues	• Intelligence and law enforcement • Situation updates • HSAS • COGCON • Federal resource allocation • Protection activities	• Intelligence and law enforcement • Situation updates • HSAS • COGCON • Federal resource allocation • Protection activities • Declarations

Prior to meetings, staffs needed to provide updates and products to leadership, such as agendas, talking points, and briefings. With back-to-back meetings on October 16, the demand for updates was continuous and consumed a large part of staff time. Within the CAT, the development of senior leadership products was not well-integrated with National SITREP development. Because of the schedule, these products had to be developed in parallel by different staff members. This led to some inconsistencies in information reported in meetings and included in the National SITREP.

During meetings, there was no formal process for adjudicating competing needs and courses of actions. Although the CAT had a process for developing courses of action and did so for a few decisions, such as HSAS level changes, this process was only used to support making recommendations for DHS leadership to consider in preparation for senior leadership meetings.

Following senior leadership meetings, summaries were not formally disseminated.[23] Instead, meeting outcomes were informally briefed back to agencies by their participants. This led to several instances where participants left meetings with different understandings of decisions:

- At several senior leader meetings on October 15 and 16, changes in HSAS were discussed. The first decision announced at the October 15 SLG was to change the HSAS to Red in Guam. Several times after these decisions, players were not sure if

[23] This was an issue in previous TOPOFF exercises.

Red was for all of Guam or the Port of Guam, and it was reported both ways. At this meeting and in meetings the next morning, the decision to go to Orange nationwide was made, but the announcement was delayed until the next morning so that DHS could gather information on protective actions. This resulted in two different interpretations of the decision:

1. The HSAS is not at Orange; the level will increase to Orange tomorrow and will be announced to the public.
2. The HSAS is at Orange and D/As should pursue activities that are required by the change; the change will be announced to the public tomorrow when D/As are ready.

- After the Principals SVTC at 1:00 p.m. on October 16, some agencies thought it was decided that the DEST would not deploy. At the 3:30 p.m. CSG later that day, they were surprised to find that the DEST was making preparations to deploy.
- Following the same Principals SVTC on October 16, some participants thought that the White House had ordered a change to COGCON level two. This change was announced at the 2:30 p.m. SLG and formally communicated by the NOC to other agencies at about 4:30 p.m. that same day. Shortly thereafter, the NOC found the order to be erroneous and made another notification at 5:45 p.m. restoring the COGCON level to four.

Updated information not available on HSIN or within the CAT was occasionally briefed in senior leadership meetings. With no formal meeting summaries, this information was not passed on to the CAT. An example of this is casualty numbers and is described earlier under observation 2.1.2.

Recommendations: Establish a framework for the federal interagency battle rhythm that can be adapted during times of emergency. The DHS Office of Operations Coordination is already implementing corrective actions raised by the HSC and its own after-action process that address some of these recommendations:

1. Convene an interagency working group to share information on internal agency meeting and reporting schedules. This information can help the federal interagency align reporting and meeting schedules and facilitate development of the National SITREP.
2. Review the purpose, audience, and scope of various senior leadership meetings and deconflict them.
3. Include policies and procedures for formally disseminating meeting summaries that include key information, decisions, and taskings.

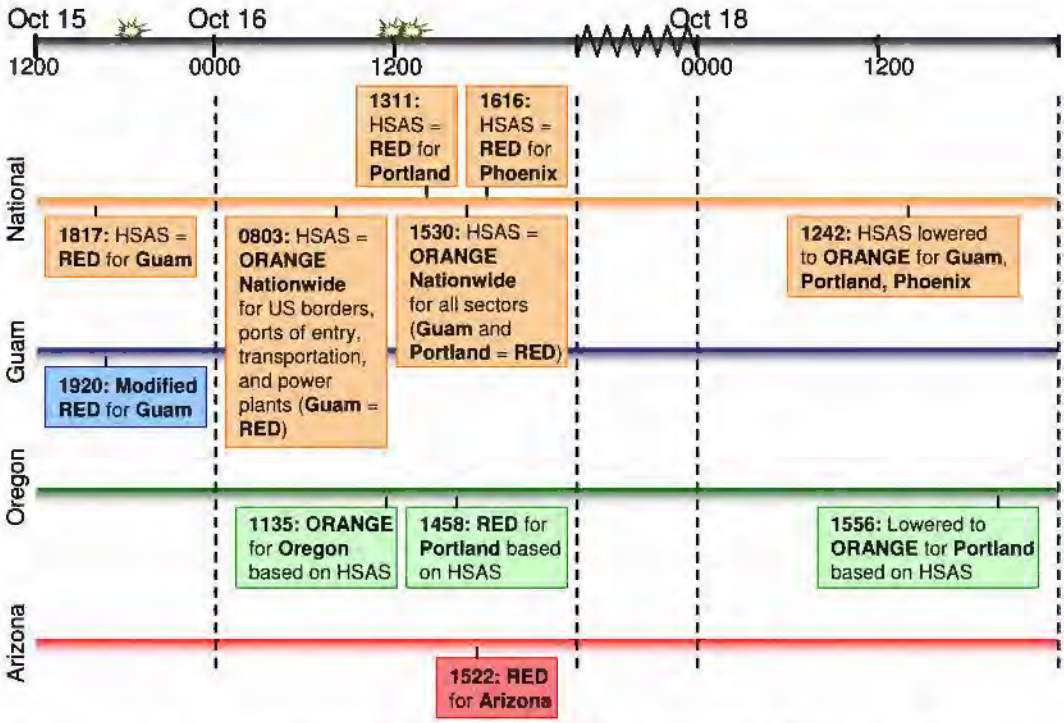
Observation 2.3.2 Area for Improvement: The purpose, definitions, and consequences of HSAS threat levels remain unclear. As observed in past TOPOFF exercises, T4 players at all levels of government, as well as international players, raised questions about the meaning and implications of HSAS level changes. In addition, state and territory agencies set their own threat levels that differed at times from the HSAS level. Interpretation of Red in Guam, Portland, and Phoenix, as well as the change to Orange nationwide, raised the most questions. Sector-specific changes were clearer and resulted in specific protective measures.

Analysis: Figure 3.6 compares HSAS level changes with state, territory, and local threat level changes.

The first HSAS level change was a change to Red in Guam shortly after the explosion on the island. The reasoning for this change was described in several ways:

- In e-mails, DHS stated, "raising the threat level to Red will provide first responders and local officials with the ability they need to carry out enhanced security measures and undertake rescue and recovery operations."
- In a senior leadership meeting, it was stated that "Red allows the responders to move, but not the terrorists."
- In an interview with VNN, the DHS secretary was asked if the change to Red had shut down the island. He responded that it had, and that it was intended to help reduce the danger of contamination.

Figure 3.6 Timeline of HSAS and State/Territorial Threat Level Changes



Guam enacted its own "modified Red" shortly after the HSAS change. The reasoning given to a mock media representative was to "allow emergency response vehicles to move in and out of the incident site." Yet, the intention of DHS was not to impact first responder movement. Several times during the exercise, reports of Guam's "modified Red" were mistaken for the DHS HSAS level.

After the explosion in Oregon, the DHS secretary appeared on VNN again and discussed the HSAS level change to Red in Portland. He said that he had conferred with the Oregon governor about raising the HSAS level to Red. Furthermore, he acknowledged the likely

economic impacts and said that this was a temporary change designed to limit the ability of terrorists to carry out additional attacks in that area. He asserted that it gave first responders the authority and freedom of movement to carry out their response. Later in the day, several county command centers recorded Portland's alert level as Red to match the HSAS level. In addition, several hours after DHS changed the HSAS level to Orange for specific sectors nationwide, Oregon raised its state-wide level to Orange as well, according to the State ECC. However, the Oregon governor reported at 7:21 p.m. EDT on VNN that the state threat level was Orange with no mention of Portland. This discrepancy may have been caused by the coordination challenges discussed later under observation 2.3.4.

Arizona raised the entire state to Red shortly after the explosion, while the HSAS was Red only for Phoenix. The Arizona governor appeared on VNN at 4:38 p.m. EST on October 17. When asked about the investigation surrounding the man who detonated the explosion, the Arizona governor said one of the reasons that they were at Red was because the suspect (or an accomplice) had not yet been apprehended. Further, the explosion was actually at the intersection of Routes 101 and 202, which is outside of the City of Phoenix. Although this area is considered to be part of the greater Phoenix area, it was unclear whether the HSAS was red for the greater Phoenix area or just for the city itself.

The sector-specific change to Orange nationwide for borders, ports of entry, transportation nodes, and power plants resulted in documented protective actions. U.S. Customs and Border Protection (CBP) increased security at the border, TSA increased security at airports, and Arizona increased security at a nuclear power plant.[24] On VNN, the DHS secretary said that the reason for this change was the potential for future attacks. He urged the public to become informed, make preparations for additional attacks, and referenced *ready.gov* as a source of information. He also said that additional security measures were being taken at airports, mass transportation nodes, and other CI sites, and advised that governors and local officials take additional measures such as limiting public gatherings. There were few recorded closures in response other than canceled college classes in Arizona and a few public school closings.

The impact of the change to Orange nationwide for all sectors is less clear. Although it was reported that the DHS secretary was inclined to raise the HSAS to Orange nationwide as early as the evening of October 15, this change was delayed until the CAT could collect information on what protective measures would go along with the change, indicating that checklists and procedures for changing HSAS are still inadequate. The CAT encountered significant difficulty collecting this information. It sent out RFIs to the federal interagency on two occasions and received very little information in return. Once the level was raised to Orange nationwide for all sectors, there was no apparent change in the message to the public.

There are at least two instances when other federal agencies recommended additional HSAS changes in senior leadership meetings. Neither recommendation led to a change. In one example, TSA requested that DHS increase the transportation threat level to Red

[24] CBP conducted an internal detection exercise in conjunction with T4 and its activities are described in Annex 2.

for specific cities several times on October 16. This recommendation was passed to the CAT for analysis, although no results of this analysis were reported.[25] The planning section of the CAT, made up of members of the Incident Management Planning Team (IMPT), was responsible for developing recommended changes in HSAS and considered many different HSAS scenarios. One of its major concerns was the economic impact of sustained HSAS level changes, and it never recommended any additional elevations to Red. There was also one recorded instance supporting this economic concern at the local level. On October 18, Phoenix officials said that they would seek reimbursement through the federal emergency declaration for "security costs of Red."

Recommendations: Review and clarify policy surrounding the HSAS through an interagency working group led by DHS. The DHS Office of Operations Coordination is already acting on a similar recommendation.

1. Clarify the purpose of the HSAS, its link to threat information and other alert condition systems like COGCON and Defense Readiness Condition (DEFCON), and its intended consequences.
2. Define the purpose of specific changes in HSAS (e.g., the purpose behind raising the HSAS to Red at an incident site following an event) and how changes are managed.
3. Compile recommended protective measures linked to different changes in HSAS. Include federal, state, local, CI/KR, and the public. This information can be used to issue scenario-specific guidance during an event.
4. Incorporate HSAS level changes in national scenario-based plans.

Observation 2.3.3 Strength: There was effective coordination between DoE and EPA field teams and officials that deployed to Guam and Oregon.[26]

Analysis: In Guam, DoE was the coordinating agency, in accordance with the Nuclear/Radiological Incident Annex of the NRP. Due to resource constraints, both DoE and EPA senior officials recognized that they would need to coordinate their efforts to manage the response. At the incident site, DoE and EPA officials worked together to fulfill notional mission assignments and complete radiological deposition data collection tasks.

In Oregon, DoE was also the coordinating agency, in accordance with the Nuclear/Radiological Incident Annex of the NRP. DoE and EPA worked together at the FRMAC to assign and complete radiological deposition data collection tasks. The EPA deputy Radiological Emergency Response Team (RERT) commander was the senior EPA representative at the FRMAC. As described above, all radiological field teams were fully integrated into the FRMAC structure, including DoE and EPA field teams, and tasked by FRMAC leadership. Several officials from DoE and EPA who deployed to

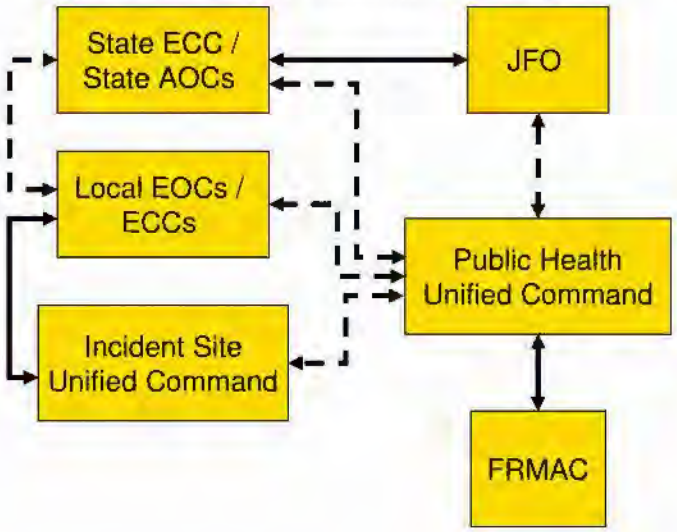
[25] This apparent lack of follow-through indicates again that formal processes for decision making (discussed in 2.3.1) and disseminating results are inadequate.
[26] Since field teams in Arizona were all notional, we did not explore EPA and DoE coordination there.

Oregon stated that the coordination between DoE and EPA officials and their respective field teams was the best that they had ever observed.

Observation 2.3.4 Area for Improvement: In Oregon, there was no unified coordination structure that linked all components of the response. This issue was observed in past TOPOFF exercises and highlighted as a critical challenge during the response to Hurricane Katrina. The response to the RDD event in Oregon was complex and involved many D/As at the local, state, federal, and international levels with many different authorities, functions, and assets. These D/As established multiple decision-making nodes with varying degrees of coordination, which did not promote information flow. This lack of coordination had a significant impact on top official decision making, especially regarding the implementation of protective actions and public messaging. This section focuses on the Oregon venue, which established a complete response structure. In Arizona, all field components were simulated, and in Guam, some field teams and response functions were simulated. In addition, Guam does not have a local level of government, making it less likely to experience some of the problems described below.

Analysis: Figure 3.7 shows the coordination diagram that emerged once federal assets arrived and integrated into the response structure. Solid arrows indicate integrated coordination (e.g., formal mechanism established such as LNO exchange or joint planning), while dotted lines indicate limited or intermittent coordination. There were six key decision-making nodes: local EOCs/ECCs, state ECC/Agency Operations Centers (AOCs), the FRMAC, the incident site unified command, a public health unified command, and a JFO. For the most part, these six nodes operated independently of each other, and there was no overarching body to unify the response.

Figure 3.7. Oregon Coordination Diagram[27]



[27] This figure is based on the reconstruction of exercise information flow among sites. It reflects what actually happened during the exercise, rather than what might be depicted in plans and procedures.

The following examples illustrate coordination challenges:

- **Lack of strategic direction.** Late in the afternoon on October 16, leadership of the unified command at the incident site was transitioning from PFR to the FBI as the primary mission shifted to law enforcement.[28] At approximately 9:45 p.m. EDT, there was a coordination meeting between DoE, EPA, FRMAC, Oregon State RPS, Multnomah County Health Department, and PFR HAZMAT to discuss the status of the public health response, formalize a coordination plan, and develop a site assessment strategy. This meeting led to the formation of a second unified command at the Multnomah County Health Department EOC, which was focused on public health, long-term protective actions, and recovery issues. However, there was no mechanism in place to coordinate activities across both unified commands. Rather, they operated independently and communicated infrequently with each other. On the second day of the exercise, the incident site unified command decided to focus on blast site issues, but for the most part both unified commands still operated independently of each other. Late in the afternoon on October 17, as the FBI was approaching the completion of the law enforcement investigation, the decision was made to terminate the incident site unified command. Authority over the incident site was transferred to the public health unified command that evening.

  Further, there was no evidence that a representative from DHS or the JFO was present at either of the unified commands. This is particularly significant since, under the new September 2007 version of the Nuclear/Radiological Incident Annex (which must be noted was not in effect for the exercise) DHS is designated the coordinating agency for an RDD incident and therefore is expected to participate in the unified command.

- **Delayed information sharing and decision making.** The Oregon State Department of Human Services Public Health Division is the lead agency for radiological incidents under Oregon statute. The Oregon State Department of Human Services Public Health Division RPS ERT deployed to incident site at approximately 1:30 p.m. on October 16 and coordinated with PFR HAZMAT. An RPS representative participated at the coordination meeting discussed above and at the ensuing public health unified command. However, the representative was a health physicist, who was not authorized to make decisions for the state. Furthermore, it is not evident whether protective action recommendations developed at the public health unified command and long-term implications were relayed to Oregon state agency leadership and decision makers. Surprisingly, the first time that the Oregon governor saw the FRMAC deposition data product was when it was shown on VNN on the final day of the exercise.

  Although the Portland Office of Emergency Management (OEM) ECC was well integrated with the incident site unified command, Portland representatives were not a major component of the public health unified command, which limited their access to public health expertise and data products. Portland was represented at the initial coordination meeting by PFR HAZMAT. After that meeting, there was no

[28] Command and control at the incident site is discussed in more detail in section 1.2.1.

representation from Portland at the public health unified command until the last day of the exercise, when an incident commander from the Portland OEM ECC went to the public health unified command. On the same day, the DoE Deputy SEO (a member of the public health unified command), a FRMAC scientist, and personnel from the EPA RERT went to the Portland OEM ECC to brief the FRMAC data product to the mayor of Portland and other city officials. This was the first time that Portland OEM leadership saw the FRMAC deposition data products. Furthermore, there is no evidence that long-term protective action recommendations were relayed to Portland leadership until the morning of October 19.

Similarly, the JFO and PFO cells did not have ready access to technical expertise and data products. As discussed earlier, these products were posted to HSIN, but JFO personnel had difficulty downloading information from HSIN. On the last day of the exercise, a FRMAC scientist was also sent to the JFO to brief the FRMAC deposition data products to JFO leadership.

- **Conflicting public messages.** The Oregon Department of Human Services Public Health Division issued a press release on October 16 at 7:20 p.m. EDT, which identified shelter-in-place boundaries. This press release was developed independently and contradicted previously released guidance and recommendations from the Multnomah County Health Department, Portland OEM, and the mayor of Portland. This lack of coordination was particularly surprising given the regular conference calls between the mayor of Portland, the Multnomah County commissioner, and the Oregon governor.

  In addition, until the morning of October 19, public messages in Oregon were focused on short-term protective actions (e.g., shelter-in-place, immediate health concerns, immediate actions people could take). When the FRMAC deposition data product was released on October 19 and discussed on VNN by local and federal officials, there had not been any public messages to prepare the public for the possible longer-term consequences, such as the contamination of agriculture and dairy products and the likely relocation of a significant area within one year.

Below are some factors that may have contributed to the lack of integration:

- Participation in the public health unified command may not have been a high priority for the City of Portland because the city has no public health agency and relies on Multnomah County for public health expertise. Multnomah County Health Department deployed a liaison to the Portland OEM ECC. However, the liaison was not a radiological SME, and it took 24 hours for this representative to arrive.
- The JFO structure did not support execution of the requirements stipulated in the Nuclear/ Radiological Incident Annex. Under the July 2007 version of the annex, which was the version used during the exercise, DoE is the coordinating agency.[29] However, the JFO structure only includes DoE personnel at ESF-12, which is responsible for energy infrastructure. As a result, the DoE personnel at the JFO were

[29] This has since been revised. In the September 2007 draft of the Nuclear/Radiological Incident Annex, DHS is the coordinating agency for RDD terrorist incidents.

not necessarily qualified to provide subject matter expertise regarding radiological response and protective actions to JFO leadership. ESF-10 (HAZMAT response), for which EPA is the coordinating agency, contains more relevant functions but was not tasked by JFO leadership to provide subject matter expertise.

- Prior to the exercise, DoE and EPA exercise planners agreed to incorporate the FRMAC within the planning function of a unified command ICS. However, the FRMAC is composed of multiple capabilities that align to different ICS components. The tactical components of the FRMAC, such as the AMS and the field data collection teams, are operational; while the technical, analysis, and advisory components are more consistent with planning functions.

Recommendations: Effective coordination between all levels of government is necessary for the federal government to provide timely and adequate support to local jurisdictions. Outside of actual disasters, TOPOFF provides the only opportunity to establish the entire local, regional, state, tribal, federal, and international command and coordination structure in response to a complex event. The full participation of all components in Oregon at the incident site and at local, state and federal command centers, helped to uncover considerable challenges.

1. DHS should convene an interagency working group to address methods for improving coordination between federal, state, and local jurisdictions and identify concepts and mechanisms to facilitate a "unified management of the national response" as called for in the Hurrieane Katrina Lessons Learned report.
    - One recommendation from the Hurricane Katrina Lessons Learned report that should be further considered is to improve planning and coordination at the regional level.
    - DHS should develop scenario-specific training modules for response personnel to improve coordination between federal, state, and local jurisdictions.
    - DHS should continue to sponsor periodic exercises that examine all components from the field to the national level to evaluate the effectiveness of improvements.
2. DHS should convene an interagency working group to clarify the relationship between ESF-10 and the Nuclear/Radiological Incident Annex in the NRF.
    - Review the JFO structure and clarify how elements of incident-specific annexes should be incorporated.
    - The September 2007 version of the annex designates DHS as the coordinating agency for a terrorist incident throughout response and recovery. It also documents some procedures for ESF-10 when the annex is activated. Nevertheless, the role of DHS as the coordinating agency is still unclear, and the NRF does not address the composition of the JFO for scenario-specific incidents when incident annexes are activated.

- National-level guidance is needed to address how best to integrate the FRMAC into the overall coordination structure during a radiological incident.

3. Future RDD exercises should investigate ongoing changes to the Nuclear/Radiological Incident Annex and the transition to environmental clean-up and site restoration activities.

Observation 2.3.5 Area for Improvement: Some agencies had difficulty integrating their SOs into the JFO structure.

Analysis: There were several instances where agencies noted difficulty integrating their SOs into the JFO. Examples include the following:

- The JFO staff was unfamiliar with the role of the Senior Federal Law Enforcement Official (SFLEO).[30]
- The DoE SO in Oregon was asked to support the PFO, which made it difficult for the SO to carry out his or her role as part of the JFO coordination group. In addition, the JFO and PFO cell were physically separated, further contributing to this difficulty.[31]

Recommendations: Review and clarify the roles and responsibilities of SOs in the policies, procedures, and training that support the JFO and PFO cell. The PFO program was recently moved to the DHS Office of Operations Coordination, and this office is already working to improve the program. The newly revised NRF does contain more detailed descriptions of the roles and responsibilities of SOs as part of the Unified Coordination Group.

Observation 2.3.6 Strength: The participation by private sector and CI/KR organizations was the largest of any national-level exercise to date.[32] These organizations participated at the national level and in the venues, and helped demonstrate areas where they can most effectively contribute to the response.

Analysis: The exercise demonstrated areas where private sector leaders can add significant value to situational awareness and support decision making processes. At the national level, this occurred through Office of Infrastructure Protection (OIP)-sponsored conference calls and other communication methods. In addition, nine CI/KR sectors tested a SIMCELL in the Master Control Cell (MCC) for the first time with industry SMEs. By conducting a cross-sector analysis of unfolding events, they recommended injects explaining possible business decisions and consequences from government decisions.

In the venues, private sector organizations coordinated with government agencies in a variety of ways. In Guam, the private sector was represented in the Territorial EOC and

[30] This observation was drawn from FBI input into the after-action process.
[31] This observation was drawn from DoE input into the after-action process.
[32] Findings from this section are drawn in part from the DHS OIP AAR/IP.

actively participated in the response. In Arizona, seven of the nineteen sectors identified in the NRP co-located in a BOC to assess the disaster's impact on local industries, assist with available resources for incident response and recovery, and pass this information on to the state. Officially a private sector entity, the BOC kept a watchful eye on the health of CI and businesses in the aftermath of the RDD incident. The formal incorporation of the private sector into disaster response and recovery operations resulted in regular phone and e-mail communication with the Arizona SEOC, and in many ways was a success. For example:

- The BOC responded to numerous RFIs from the Arizona SEOC regarding private sector activities, including the identification of business continuity of operations issues, key businesses in the contaminated area, and critical resource capabilities within the BOC.
- The BOC represented industries offered search and rescue, damage assessment, and structural decontamination expertise to the Arizona SEOC.
- The BOC built an inventory of all impacted businesses within the industries represented at the BOC.

Recommendations: Continue to institutionalize and formalize relationships between government, private sector, NGOs, and CI/KR organizations.

Observation 2.3.7 Area for Improvement: Although it was demonstrated that there is much the private sector can contribute, the mechanisms for integration into emergency response structures are not clear. At the federal, state, territory, and local levels, there were challenges to effective private sector integration.

Analysis: There are many federal, state, territory, and local agencies with similar and overlapping responsibilities for private sector coordination. This complicates private sector participation in response and recovery activities. Private sector offices within DHS include the DHS Private Sector Office (PSO), OIP Partnership and Outreach Division (POD), and the FEMA PSO. The roles and responsibilities of each office are not clear to private sector entities, and there is uncertainty on how to best integrate with them during emergencies.[33]

At the local level, communications and information sharing challenges limited the ability of the Arizona BOC to support the response. T4 was the first time a BOC had been established in Arizona, so it lacked formal policies, plans, and systems. In Guam, the private sector could have been more effectively integrated into initial discussions and decisions about port closure and tourism held at the EOC. Coordination improved later in the exercise.

Recommendations: Clarify private sector partnership models in national policies and the national family of plans. The National Infrastructure Protection Plan (NIPP) lays out a partnership model.

1. DHS should clarify and articulate the purpose, roles, and responsibilities of its

[33] Findings from this section are drawn in part from the DHS OIP AAR/IP.

various PSOs. No DHS office has singular, vested authority and responsibility for organizing, leading, planning, programming, or budgeting for private sector integration. This issue remains unresolved in the CI/KR and Private Sector Supporting Annexes of the NRF.

2. State, territory, and local agencies should formalize arrangements with private sector partners and develop the policies, plans, and systems necessary to support their use in times of emergency.
3. Articulate and institutionalize a process for private sector and NGO engagement in national-level exercises, including authority for planning, programming, and budgeting for national and venue working groups.

Observation 2.3.8 Strength: Disability and special needs play was a major focus area in the exercise design. As a result, players gained critical practical experience regarding the additional support needed by individuals having special needs.

Analysis: Accommodations for special needs populations were managed in a variety of ways. In Guam, Oregon, and Arizona, press releases were prepared in languages other than English. In Guam, for example, press releases were translated into five different languages: Chinese, Japanese, Tagalog, Chamorro, and Chuukese. In Arizona, protective action guidance was released to the Native American community in the Navaho language.

First responder provides guidance at assisted living.

Victim actors at the Oregon site included individuals with hearing, sight, mental, and mobility disabilities and limited English proficiency. Responders had to identify and accommodate these victims in the course of the response. In another example, the DHS Office for Civil Rights and Civil Liberties (CRCL) collaborated with the Oregon Multnomah County Health Department to ensure that consideration was given to individuals requiring home healthcare, medical care, or supervision when the decision was made to shelter-in-place over several days.

Arizona addressed the needs of special populations in the contaminated area through play that included individuals with disabilities attending a charity function and the residents of an assisted living facility who required evacuation.

Recommendation: Continue to incorporate special needs play within national-level exercises with additional objectives to focus specifically on decisions regarding special needs.

Observation 2.3.9 Strength: Foreign consular involvement and consular operations were successfully exercised.[34]

Analysis: The addition of foreign consular involvement in T4 added realism to exercise play and stressed the capability of domestic responders to handle the international dimension of a crisis. Inclusion of consular operations allowed DoS to train federal, state, and local authorities on their reporting responsibilities under the Vienna Convention on Consular Relations (VCCR). The VCCR obligates competent U.S. authorities, including federal, state, and local government officials, to notify foreign consuls "without delay" of the arrest and detention of foreign nationals, deaths of foreign nationals, the appointment of guardians for minors or incompetent adults who are foreign nationals, and related issues pertaining to the provision of consular services to foreign nationals in the United States.

Consular Response Teams deployed from the three participating countries to Portland. DoS also deployed a representative to the JFO in Portland to assist with consular activities and to coordinate information sharing. Thus, there was a single source for international participants to access and transmit consular information to appropriate, national-level stakeholders.

Observation 2.3.10 Area for Improvement: DoS received a wide range of international offers of assistance to the USG during the exercise, but did not accept any because FEMA did not activate the IAS. In some cases, accepting these offers may have had diplomatic benefits for the USG, but FEMA determined that domestic resources met all incident needs, and no international offers were needed. DoS personnel separately considered accepting cash donations, which are easy to manage, but the procedures to do so were not clear to FEMA or DoS personnel.

Analysis: DoS received a wide range of international offers of assistance to the USG during the exercise that included commodities, personnel, and cash donations. DoS forwarded all offers of assistance to FEMA, and FEMA responded with the recommendation to urge the donations be made to NGOs. FEMA determined that domestic resources met all incident needs and thus, did not activate the IAS.

The IAS is designed primarily for offers of commodities and services. The IAS CONOPS outlines the procedures for activation and use of the IAS. Managing the acceptance of such offers can be challenging for several reasons: liability or licensing concerns may preclude assistance by foreign personnel, and commodities require logistical arrangements to be made. Additionally, there may be cases when the USG should accept non-cash donations from countries deemed Diplomatically Critical (DC) by a DoS policy decision. In this situation, DoS provides FEMA with a list of countries designated as DC, and the two coordinate with USAID to identify particular items that can be accepted. FEMA makes the final decision on items to be accepted.

Cash donations, whether from a DC country or not, are easier to manage, and DoS considered accepting cash donations during the exercise. The "*Procedures for Foreign*

[34] This observation was drawn from DoS input into the after-action process.

Cash Donations Offered in Response to a Disaster Affecting the United States", June 22, 2007, describes procedures for cash donations. Unlike the IAS activation, the procedure for accepting international cash donations requires joint agreement among the secretaries of state and homeland security, together with the assistants to the president for national and homeland security. In the absence of this top-level decision being made during the exercise, participants came to the conclusion that IAS activation was required to accept cash donations.

On October 18, the fourth day of the exercise, DoS asked FEMA to make a determination about accepting cash donations. If FEMA agreed, DoS was prepared to convene a cash donations working group to evaluate whether accepting cash donations was advisable on a country-by-country basis, as called for in the procedure. FEMA replied that before activating foreign cash donations procedures, it would like DoS to verify that it had responded to each financial offer with the recommendation that the host government transmit the donation via NGOs per the list on FEMA.gov. If a host government insisted on making cash donations directly to the USG, FEMA agreed to discuss activating the foreign cash donations procedures. DoS had already responded to each offer with this recommendation. The exercise ended before DoS received a response from FEMA regarding activation of the IAS for cash donations.

Recommendations: DoS, DHS, and the interagency working group that developed the IAS CONOPS should review both the CONOPS and cash donations procedure, and clarify these two documents and the procedures for considering and accepting both cash donations and donations from DC countries. Merging the documents into a single CONOPS for clarity may be useful.

Capability 3: Public Information and Warning

Capability Summary: This capability includes the development, coordination, and dissemination of accurate alerts and emergency information to the media and the public before, during, and after an emergency.

Public information and warning was a critical component of the T4 exercise. JICs, which consisted of federal, state, territory, and local PIOs, were set up in each of the incident locations. The JICs in Guam and Arizona were established in pre-existing joint information facilities; the Oregon JIC was set up in a hotel. In addition, ESF-15 was activated and functioned as the external affairs arm of the Guam and Arizoua IOFs and the Oregon JFO. DHS Office of Public Affairs (OPA) selected external affair officers based on their background in law enforcement and terrorism. A senior FBI public affairs official was selected as the external affairs officer for Oregon and an ATF public affairs officer was chosen as the deputy external affairs officer for Arizona. At the national level, the National JIC operated at DHS Headquarters in Washington, DC. The National JIC included representatives from FEMA, NORTHCOM/DoD, FBI, ARC, EPA, DHS CRCL, DHS PSO, CI/KR organizations, and Canada. The communication methods employed by public affairs officials included e-mail, press releases, public statements, and interview appearances on VNN.

T4 demonstrated improved coordination among PIOs, which is partly the result of improvements implemented after Hurricane Katrina. One key challenge was that officials had difficulty

explaining why different protective actions were taken by jurisdictions in different locations. Also contributing to this issue was that decision makers and PIOs had difficulty integrating and explaining scientific information like plume model results. Similar problems were observed during T3.

The table below provides a summary of all of the observations described under this capability along with associated recommendations, where applicable.

Table 3.7 Summary of Public Information and Warning Observations

Observation	Recommendation
Activity 3.1: Establish JIC/ JIS	
3.1.1 **Strength:** The National JIC coordinated regular teleconferences that facilitated information sharing and strategic guidance.	Continue the use of teleconferences to share information and consider further methods to share information and coordinate messaging.
3.1.2 **Area for Improvement:** Information overload was a problem among public affairs officials.	Continue to develop and streamline information sharing tools, processes and procedures.
Activity 3.2: Disseminate/ Issue Emergency Public Information and Alerts/ Warnings	
3.2.1 **Strength:** Statements from federal and relief agencies were consistent in their messaging for local populations to look to their local-level governments for protective action guidance.	
3.2.2 **Strength:** Statements from federal, territory, state, and local governments, as well as relief agencies, were consistent in their recommendations of how to seek protection from radioactive contamination while sheltering-in-place.	
3.2.3 **Area for Improvement:** Public officials had difficulty explaining the reasoning behind the protective action guidelines to evacuate and shelter-in-place.	Consider the role of the federal government in coordinating the explanation of different actions by local jurisdictions. Review and update related policies and procedures for strategic communications. Investigate ways to facilitate the integration of scientific information into public messaging and decision making.

Activity 3.1: Establish a JIC/ JIS

Observation 3.1.1 Strength: The National JIC coordinated several regular teleconferences that facilitated the exchange of information and strategic guidance.

Analysis: Public information coordination mechanisms have matured both through use in previous exercises and actual incidents. The following calls were well-attended and deemed valuable by participants:

- National Incident Communications Conference Line (NICCL) Calls
- White House Communications Calls
- Special Media Line Calls

These calls are examples of strategic and operational-level calls that contribute to the federal interagency operational cycle discussed in observation 2.3.1. The focus of these calls was public messaging and the primary participants were public affairs personnel.

NICCL Calls: According to the July 2006 ESF-15 SOPs, the NICCL is "used for transmission and exchange of critical and timely incident information among federal and affected state, local, and tribal authorities." Two calls were held each day with federal agency PIOs and the affected venues (ESF-15 leads and state PIOs). The ESF-15 and federal and state JIC directors reported that the calls were valuable because they were well organized, provided an overview of federal agency activities, and provided an opportunity to communicate issues. A few shortcomings were identified, including that the calls were lengthy, there were a large number and variety of attendees (making some participants uneasy about information they should share), and there was some misunderstanding about which agencies should participate in the call.

White House Communications Calls: Each morning, leadership from the White House, the National JIC, and ESF-15 conducted a conference call to discuss strategic messaging guidance from the White House and to provide venue updates.[35] ESF-15 leads felt that it was very valuable to have this line of communication directly with the White House. (Note that due to time differences, the Guam venue was not able to participate in all calls.)

Special Media Line Calls: First used during the response to Hurricane Katrina, these calls were coordinated by the DHS press secretary to provide information to the media and answer questions. PIOs from DHS and other federal agencies participated in the calls. Participants felt that these calls helped reduce the call volume from the media and increased the situational awareness of activities in other agencies.

Recommendations: Continue the use of teleconferences to share information with the media and among PIOs.

1. To reduce the length of NICCL calls, consider virtual tools (such as chat rooms or web conferencing) where participants can post briefing points.
2. For multi-venue incidents, consider adding ad-hoc small group calls for ESF-15 leads to coordinate messaging.

Observation 3.1.2 Area for Improvement: PIOs reported that information overload was a problem. Managing the large volume of e-mail communications drew the attention of PIOs away from other duties and hindered information sharing and situational awareness.

Analysis: The National JIC employed several mechanisms to support ESF-15 and PIO coordination through written means, including:

- National JIC e-mails.

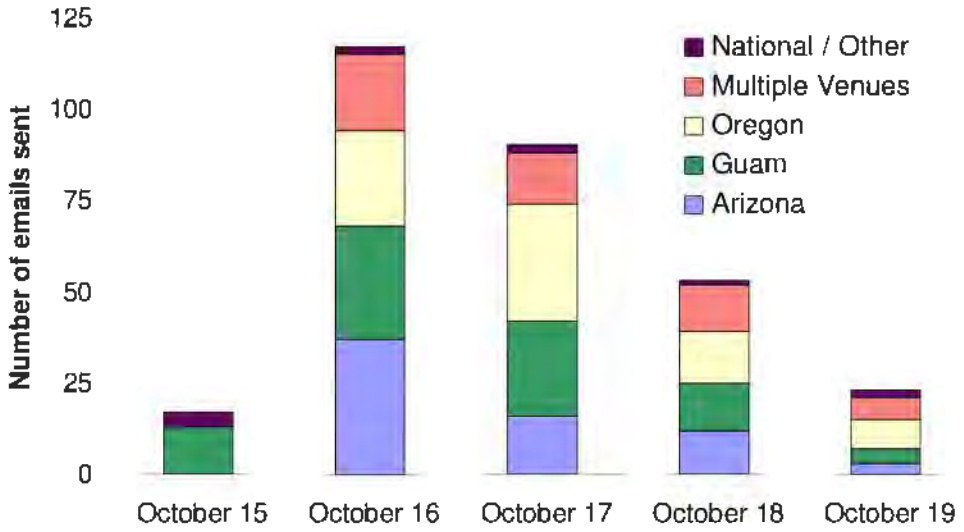
[35] Though strategic communications was addressed, many strategic activities, such as presidential statements, were notional.

- Posting materials on HSIN.

These coordination mechanisms have also matured through use in previous exercises and actual incidents. However, PIOs still could not effectively manage the volume of information being pushed to them through e-mails and often did not use mechanisms that required information to be pulled, like HSIN.

Summaries of the NICCL calls, ESF-15 daily communications summaries, press releases generated by the National JIC, and venue press releases sent to the National JIC were distributed to a large e-mail distribution list, which consisted of ESF-15 national leadership, National JIC contacts, and venue contacts (ESF-15 leadership and staff, JFO leadership, JIC leadership and staff, state PIOs, and several other related PIOs). Figure 3.8 shows the large number of e-mails sent by the National JIC to this distribution list. The total e-mails by day are broken down by their primary content.

Figure 3.8: Number of E-mails Sent by the National JIC to the Distribution List



Participants reported that e-mail was useful to see what issues other venues were addressing. However, the biggest drawback to the National JIC e-mails was information overload. T4 PIOs received hundreds of e-mail messages and some did not have time to read the releases. Many times the messages went unread or were simply deleted.

A considerable amount of the information was duplicative. For example, venues often received their own press releases from the National JIC. The same information also appeared in a variety of press releases. It is important to note that although the duplication increased the volume of information, some found it useful because they felt that repeated information provided an indication of what was important and also served as a confirmation that the National JIC received what they had sent.

Smart practices evolved to manage the volume of information:

- The Arizona JIC created an update release that was distributed every two hours. Information was organized by topic (e.g., health, law enforcement, etc.) and new information appeared in bold text. The format enabled readers to easily identify the

new information, while still providing comprehensive information to those who did not read the previous release. This process was repeated each day of the exercise. As a result, the number of press releases issued was significantly reduced from approximately 50 on the first day of the exercise to six on the following day. Because of its success, the practice was adopted by the other two T4 venues and the National JIC. Two key elements were necessary:

  - The JIC needs to he up and running. Before this coordination mechanism is in place, independent press releases would still be needed to fill the information void. As the incident transitions to greater management, consolidated messaging becomes possible.
  - Update releases requires buy-in of JIC participants. Some participants were initially reluctant because they wanted to disseminate their own information. However, they agreed to the process when they understood that a consolidated release would ensure that their information did not get lost in a larger number of releases, it would decrease their workload, and that statements could still be sent out separately when needed (emphasizing their importance).

- Arizona developed a media monitoring report that also covered the Guam venue. This reduced the workload required in Guam.
- Some public affairs officials assigned staff to read e-mails and notify ESF-15 and JIC leads of important information. If staff is available to do this, it frees directors to spend time with operations and other coordinating officers.
- Oregon sent the e-mails to a common mailbox and sorted them into different folders for action.

T4 PIOs also made suggestions based on their experience:

- Establish definitions for routine, priority, and immediate messages and label them. People receiving the messages would then have an indication of the importance of the messages and could handle them accordingly.
- Post press releases on a website for review and retrieval. A media monitor could watch for information and organize it in a logical manner.
- Conduct small group discussions (conference calls) among ESF-15 leads to coordinate messaging across locations (also a recommendation under observation 3.1.1).
- The National JIC could play a greater role in consolidating the messages.

Information from each venue was posted on HSIN, however, ESF-15 leads and PIOs reported that they did not use this resource. There were several reasons for this: some exercise participants did not have accounts on HSIN, organizations used different software (e.g., WebEOC), or they did not have time or resources to pull the information. This was an issue in general for the entire response community as described in observation 2.1.2.

Recommendations: Continue to develop and streamline information sharing tools with supporting processes and procedures.

1. Evaluate smart practices and suggestions on information management that emerged during T4 to reduce the information overload problem. Update relevant ESF-15 SOPs and training.
2. Develop information technology solutions that support e-mail distribution lists so that recipients can be easily added or removed. Consider developing alternate lists for bigh and low volumes to accommodate different stakeholders.

These improvements might also help address similar issues experienced by other response personnel.

Activity 3.2: Disseminate/ Issue Emergency Public Information and Alerts/ Warnings

Observation 3.2.1 Strength: Statements from federal and relief agencies were consistent in their messaging for local populations to look to their local governments for protective action guidance.

Analysis: Throughout the exercise, and noticeably in the early phases of the response, officials from public and private agencies consistently communicated that state and local authorities were the decision makers. On occasions, when asked to comment about the response in different localities, officials repeated the fact that local officials were in charge and residents should look to them for specific protective action guidance. This consistency was reflected in press releases from government and relief agencies, communications from the National JIC, and in VNN interviews featuring senior-level federal and state officials as well as technical SMEs.

Observation 3.2.2 Strength: Statements from federal, territory, state, and local governments, as well as relief agencies, were consistent in their guidance about how to seek protection from radioactive contamination while sheltering-in-place.

Analysis: Authorities in the different incident locations issued shelter-in-place instructions, in the immediate aftermath of the RDD explosions. Without exception, all authorities offered the same protective action guidelines to minimize contamination while sheltering-in-place. These guidelines included finding shelter inside a building, closing the windows, turning off any heating or ventilation system, removing clothing and placing it in an isolated plastic bag, and taking a shower.

Observation 3.2.3 Area for Improvement: Public officials had difficulty explaining the reasoning behind the protective action guidelines to evacuate and shelter-in-place. Faced with similar information and scenarios, different decisions about protective actions (evacuation versus shelter-in-place) were made in each of the venues. These were difficult choices that required decision makers to act quickly while assessing scientific model results and conditions specific to their locality. The mock media repeatedly questioned federal, state, territory, and local officials about this disparity.

Analysis: At all three incident sites, territory, state, and local authorities issued

protective action guidelines in response to the explosions and radiation detection. As the response to the incidents progressed, authorities in each location adjusted their recommendations accordingly:

- In Guam, after several hours of sheltering-in-place, officials ordered and executed (notionally) the evacuation of the 300 personnel at the incident site (Cabras power plant) and surrounding area.
- In Arizona, residents were initially advised to shelter-in-place. Within two hours, state officials advised residents to shelter-in-place and said that state personnel were assisting with evacuations from the immediate area of the incident. Over the next few hours, conflicting messages about evacuation and sheltering-in-place appeared in press releases, Arizona's informational website (AZ211.org), and in reports on VNN.com. However, within seven hours of the incident, specified regions of Tempe and Mesa were being evacuated. Residents outside the immediate area were advised to stay indoors. By the evening of October 17, residents were instructed that no further evacuations would be called and that they should remain in their homes.
- In Oregon, local officials immediately recommended that all residents in the city (including businesses) shelter-in-place. While public officials stated during VNN interviews that evacuation plans would be ready by late in the afternoon on October 16, no evacuation plans were released; instead, a new shelter-in-place zone was delineated that more specifically defined the plume area. Early on the morning of October 17, a refined shelter-in-place boundary was released and residents outside the emergency zone were notified that they need not take any specific protective actions; residents inside the emergency zone were instructed to continue to shelter-in-place. By the morning of October 18, residents in the emergency zone were allowed to voluntarily evacuate to decontamination centers but were still encouraged to shelter-in-place.

Portland Mayor addresses the media with Oregon Governor Kulongoski and DHS Secretary Chertoff.

The most notable difference in protective actions was an early decision to evacuate in Arizona while Oregon issued a shelter-in-place order for the entire city. Public officials were pressured by VNN and other simulated media to explain why recommendations to evacuate or shelter-in-place were not consistent across the incident locations. No press releases from any of the locations provided a direct explanation for these differences even

when VNN coverage aggressively pursued this issue. Public officials at all levels of government were called upon to explain the different responses.

There were several challenges to effective public messaging in this scenario:

- Federal officials were repeatedly asked to comment on and explain local protective action decisions, which is the responsibility of local officials.
- The reluctance of some officials to provide and explain technical products like plume model results was interpreted as "withholding information", especially after officials in other locations had chosen to release them.
- Protective action decisions were based on scientific concepts that are difficult to explain.

Specific examples of these challenges follow:

- During an interview with VNN on October 17, a DHS senior official stated that it was up to the local government officials to work with the best scientific information to make decisions about their localities. He was pressed to explain why the different cities and states adopted different guidelines, and while he repeatedly stated the decisions were up to local officials at each location, he mentioned that the decision makers would take into a "host of factors", specifically citing weather and geography. VNN focused on the weather-related aspect, later commenting that the different reactions "must suggest that the weather is on two different planets."
- In a VNN interview on the evening of October 16, a local official from Portland indicated that plume model results would be forthcoming and shared with the media that the city was considering an evacuation. In an interview early in the next day's VNN broadcast, the official explained that the models were not released as promised because they kept changing throughout the afternoon. The VNN anchor challenged the local officials' decision to continue to shelter-in-place, positing that evacuation would have made common sense. The official defended his position by saying he did not want residents outside "walking in the plume."
- Federal officials were consistent with officials in Oregon in reasoning that plume model results should not be released. On October 17, Secretary Chertoff stated, "We do not generally release the plume model. "He explained that because of the technical expertise required to interpret them, there is a risk that residents could misread the plume model results and put themselves in jeopardy. Officials in Guam and Arizona, however, did release plume model results. During the first joint press conference with the Arizona state officials at 4:55 p.m. EDT on October 16, they displayed a map of the plume, stating that the yellow area contained the radiation. Guam officials also released plume model results to their residents. This fact was not lost on the VNN news anchors, who asked: If the plume model was released in Guam, why was it not released in Oregon? In concluding the discussion about the unreleased plume model results, one anchor remarked that, "I'm pretty sure I could look at a plume and not go crazy."

- Officials from IMAAC and National Oceanic and Atmospheric Administration (NOAA) were also pressed for information on plume model results during a VNN interview at 12:50 p.m. EDT on October 17. To the consternation of the VNN anchor, the officials expressed their concern about releasing the plume model results to the public because of their technical nature and then deferred many questions to the local incident commanders.
- A local public official refused to discuss technically-focused information without the assistance of an SME, even though he held the printed information in his hands during the interview on VNN.

Contributing factors common to all of the above examples are the scientific terms and definitions (e.g., rems, isotopes, gamma rays, Roentgens) necessary to explain radiation exposure, and the need for SMEs to explain the findings. A particular difficulty in communicating radiation warnings through public information channels is the automatic association of the word "radiation" with "nuclear." Factors such as time of exposure, distance to the radiation source, and strength of the radiation source all affect the health consequences of radiation exposure. One approach to discussing radiation that was adopted by the various public officials was to discuss the exposure in familiar terms such as chest x-rays and CAT scans. However, reporters then questioned why minor contamination levels triggered the evacuation of thousands of people. It was only when a FRMAC official appeared on VNN at 3:36 p.m. on October 17 that the differences between short- and long-term exposure to low levels of radiation were explained.

The reluctance to release technical information could be explained by the inherent trade-offs between releasing information as quickly as possible (i.e., the motive of the public affairs community) and releasing the most accurate information possible (i.e., the motive of the scientific community). Plume model results are particularly susceptible to this problem; initial maps are only predictions and become more accurate over time as additional data are collected.

The challenges faced by public affairs officials could have been at least partially alleviated with some coordination in messaging among the incident locations. While the ESF-15 directors in each location had discussions in morning briefings with the White House and during NICCL calls, the state and local officials in different venues did not have much opportunity to talk with one another. While local officials were aware that the other locations adopted different guidelines, there is no evidence that they made an effort to deconflict their messaging. On occasions when officials defended their respective decisions, they stated confidently that they had made the right decision for their residents. The media questioned how Oregon and Arizona could both be correct in offering differing guidelines. The National JIC addressed this issue on one occasion: on the evening of October 17, it distributed the ESF-15 Daily Communications Strategy for October 18 via e-mail that included some general guidance on how to message the disparate protective action guidelines.

Recommendations: The effective incorporation of scientific information into public messaging is vital to mitigate the issues discussed above. In addition, officials should

work to improve the transparency of their operations before the media becomes openly skeptical of their actions.

1. Clarify the role of the federal government in coordinating the explanation of different actions by local jurisdictions and review and update related policies and procedures for strategic communications. According to the NRF: "the Federal team must operate and speak with a unified voice and consistent message that is coordinated not only with the different Federal authorities involved in an incident, but also with affected State, tribal, and local authorities."
2. The federal government should investigate ways to facilitate the integration of scientific information into public messaging. This integration requires the support of SMEs. Potential actions include the following:
   - Conference calls could be a forum for experts to explain technical products to PIOs and work with them to develop an appropriate message for the public.
   - Public affairs agencies could identify SMEs to provide support to JICs. The National JIC made use of one such SME. States may be able to identify and provide their own SMEs.

The DHS-led IMAAC Working Group and the FRMAC are currently developing recommendations for hazard area graphics (maps and summary language) for RDDs that can be more easily understood by local, state, and federal officials.

Capability 4: Economic and Community Recovery

Capability Summary: Economic and Community Recovery is the capability to implement short- and long-term recovery and mitigation processes after an incident. This includes identifying the extent of damage caused by an incident, conducting thorough post-event assessments, and determining and providing the support needed for recovery and restoration activities to minimize future loss from a similar event.

Recovery activities began during the FSE as recovery planning cells were established in the venues and at the FEMA NRCC. Discussion about recovery issues continued through short-term recovery (STR) TTXs and worksbops conducted after the FSE concluded. On December 4 – 5, 2007, DHS held an LTR TTX to discuss key technical, operational, and policy challenges surrounding recovery from an RDD incident 50 days after the detonation.

The presence of radiation affects all aspects of recovery. It would complicate debris removal, storage, transportation, and disposal; cause populations to be displaced to other locations; create a complex environmental clean-up situation; lead to the long-term monitoring of workers and affected populations; and raise insurance and liability issues. One key gap noted across all exercise events was the lack of comprehensive planning for recovery. The table below provides a summary of the observations described under this capability along with associated recommendations, wbere applicable.

Table 3.8 Summary Economic and Community Recovery Observations

Observation	Recommendation
Activity 4.1: Direct Economic and Community Recovery Operations	
4.1.1 **Strength**: Recovery planning cells were established early in all of the venues and at the federal level.	
4.1.2 **Area for Improvement**: Current written plans lack a comprehensive approach to recovery operations.	Incorporate recovery into national family of plans and regional planning efforts.
4.1.3 **Area for Improvement:** Participants were unfamiliar with the *Protective Action Guides for Radiological Dispersal Device (RDD) and Improvised Nuclear Device (IND) Incidents* and the site optimization process for setting clean-up standards.	Provide detailed guidance for implementing the site optimization process.
4.1.4 **Area for Improvement:** There is limited laboratory capacity for clinical, environmental, and food sample analysis in the event of an RDD incident.	Develop plans that include strategies for maximizing existing and expanding clinical, environmental, and food laboratory capacity.

Activity 4.1: Direct Economic and Community Recovery Operations

Observation 4.1.1: Strength: During the FSE, recovery planning cells were established in all of the venues and at the federal level.

Analysis: At the conclusion of the FSE, STR and LTR issues were discussed and preliminary draft plans were being developed in all of the venues. For example, the FEMA NRCC established a recovery planning cell that included expertise across all ESFs. In Oregon, the governor established a recovery planning cell on the day of the explosion, and subsequently established a recovery cabinet to focus on the transition from STR to LTR. In Guam, preliminary plans were developed to ensure delivery of goods and services, and disaster assistance specialists were part of the first cadre of personnel that arrived in venue. In Arizona, a plan for establishing a state-wide recovery task force was discussed.

Observation 4.1.2 Area for Improvement: Many participants across federal, state, territorial, and local D/As cited the lack of comprehensive recovery planning.

Analysis: Participants in the STR and LTR TTXs raised concerns about the lack of a comprehensive, unified strategy and plan for both STR and LTR. The general conclusion of these discussions was that the NRP did not adequately address the recovery phase. Although DHS organizes preparedness and emergency response in terms of four missions (i.e., "prevent, protect, respond, recover") the emphasis of the NRP is evident in its title. The NRP/NRF does assign the recovery mission to ESF-14, the Emergency Support Function for *Long-Term Community Recovery and Mitigation*. But the mission of ESF-14

is to provide: 1) funding resource identification and coordination, 2) technical assistance in the form of impact analyses, and 3) planning support to the state recovery authorities. Given the complexity of recovery operations at all levels of government and in coordination with the private sector and with NGOs and voluntary organizations, the NRP falls short. Similarly, the NPSs in the DHS Capabilities-Based Planning construct fail to adequately address LTR.[36]

Other related issues concern the role of the federal government in LTR as well as the capabilities and resources it can bring to bear. During an incident response, ESF-14 functions most prominently within the operations section of the JFO. Many participants said that they were not effectively integrated into this JFO function during past responses. Once the response is over, the JFO stands down, and ESF-14 is deactivated, there are no comparable organizations or entities to take over their roles during the recovery phase. In the past, entities such as the President's Gulf Coast Recovery and Rebuilding Council have been created, but only on an ad-hoc basis. The absence of response-like recovery entities led some LTR TTX participants to ask, "Who's in charge?"[37] Others noted the difficulty of navigating the myriad of individual assistance programs provided by federal D/As, determining what programs are available, and how they can be accessed.

The LTR TTX also highlighted additional challenges during the recovery phase. These included:

- There is limited availability and capacity for disposal of radioactively-contaminated waste, including debris. Participants identified the need to identify available disposal capacity and potential gaps for radiological waste.[38] All agreed that coordination between the federal agencies that regulate radioactive waste disposal and the states that allow temporary storage and long-term disposal will be important.
- There is an increased demand on the infrastructure/services outside of the incident site due to evacuated and displaced populations. Because of mass evacuations, jurisdictions away near the incident site would likely experience high demands on infrastructure and services for an extended period of time. Because of restrictions to areas that experience damage, the Stafford Act may not cover locations that receive evacuees.
- Reliance on single sources of CI results in unnecessary vulnerability. Although the RDDs did not contaminate the water supplies in the affected states, it would have been useful to consider the potential challenges that local, state, territory, and federal governments would have faced if any of the water plants were in the contaminated area. States and responsible agencies addressed the various risks of only having a single source of water, and the need to develop alternative plans

[36] Some additional information regarding recovery planning and coordination at the federal, state, and local levels has been added to the NRF. However, the NRF still maintains that LTR is outside the scope of the document.
[37] The NRF describes some examples of federal, state, and local coordination, but maintains that responsibilities shift to individual agencies with primary recovery responsibilities after the JFO closes.
[38] One lesson learned from the Goiana (Brazil) Cs-137 clean-up is that early identification of disposal paths for clean-up waste is necessary to prevent delay of clean-up.

for drinking water. Participants agreed that all water systems needed to establish contingency plans for how to respond if the primary water source became contaminated.

- There is a need to coordinate access control within contaminated areas. Participants expressed concern about past difficulties that truckers would experience in gaining credentials and permission to access affected areas. The resulting delays would adversely affect the delivery of needed supplies and materials, and would ultimately increase LTR costs. The group debated whether this would remain a problem at D+50 and whether this was properly the role of the federal government, since local law enforcement agencies are generally responsible for area control.
- There is a requirement to conduct long-term monitoring of workers and the exposed population. Plans and procedures should be developed to rapidly mobilize monitoring equipment and collect samples.
- Many participants were unfamiliar with the Environment, Food, and Health Advisory Team's (A-Team) function because it is not well-defined. The A-Team is an interagency group, but it lacks a single point of leadership. The initial purpose of the A-Team was to advise decision makers on questions regarding food and health. However, this resource was not used effectively during the FSE because states and agencies were unaware of the group.
- State and local governments are unfamiliar with federal disaster mental health operations and disaster surge capability. Participants unanimously agreed that an RDD attack would require different approaches than responses to any other types of disaster. Although there are many disaster mental health programs in place, often they are underutilized because agencies and governments are unaware of their existence. Representatives of states and agencies also saw public messaging as key to addressing disaster mental health issues. Conveying guidance and information to the public and explaining the government's response to the attack should reassure citizens that authorities are in control of the situation, reducing the psychological impact. This need for consistent public messaging also raises the issue of how long a JIC would continue to function after an incident.
- Private sector recovery challenges to an RDD attack include concern about the liability risk for remediation contractors and reluctance of businesses to return to a contaminated area. There was uncertainty regarding the process for property condemnation, reimbursement, and subsequent reoccupation of condemned and contaminated structures after receiving certification for reoccupation. Participants identified the need to clarify the roles and responsibilities of federal, state, territory, and local jurisdictions, as well as the role of the private sector. In addition, participants noted that decision makers should manage public expectations through pre-incident education and strategic public messaging.

The delegation from Guam repeatedly emphasized the need to address the unique challenges faced by their island community and by other territories, islands, and tribal

areas as well. Although Guam was spared island-wide contamination because of the western location of the simulated RDD attack and the prevailing westerly winds, the effects of the attack were nevertheless particularly severe for the territory. Guam relies on imports via ocean transportation for most of the goods and materials it needs. The closure of the commercial port, even with the stopgap opening of the pier facilities of the U.S. naval base for commercial activity, would have had a drastic effect on the economy. Furthermore, a large component of the economy in Guam is dependent upon the tourism industry. The stigma of radioactive contamination poses a real threat to that industry. In addition, the Cabras port complex is the primary transshipment hub for Micronesia and the larger Western Pacific island region. While the port of the Commonwealth of the Northern Mariana in Saipan could have absorbed some of this function after the attack, its cargo handling capacity does not match Guam's.

Recommendations: Decision makers should consider implementing the following:

1. Expand the NRF to include recovery operations, which should address:
   - The organizational structure for LTR.
   - The role of government, NGOs, and private sector organizations.
   - Strategic communications and continued activation of the JIC.
   - The needs of unique entities (e.g., territories, islands, and tribal lands).
2. Develop supporting policies and procedures for implementing recovery activities following an event and incorporate recovery into scenario-based plans like the RDD Strategic Plan. These should include policies and procedures to address disposal of contaminated waste, the impact of displaced populations on surrounding communities, reliance on single sources of CI, coordination of access control within contaminated areas, long-term monitoring of workers and the exposed population, mental health operations, and private sector concerns.
3. Develop appropriate training programs for private and public sector entities to support policies and procedures for implementing recovery operations.
4. Develop guidance documents – in particular for individual assistance programs – to help state and local organizations navigate and access the variety of programs available through FEMA and other agencies.
5. Expand the scope of the interagency NPSs to include LTR needs, with particular attention to the unique needs of non-contiguous geographic states/territories.

Observation 4.1.3 Area for Improvement: Participants were unfamiliar with the January 2006 DHS Preparedness Directorate's; *Protective Action Guides for Radiological Dispersal Device (RDD) and Improvised Nuclear Device (IND) Incidents* regarding the site optimization process for setting and implementing clean-up standards following an RDD incident. This document has undergone a public comment period and will he finalized soon.

Analysis: During the LTR TTX, participants voiced concern regarding DHS guidance for responding to, and recovering from, an RDD event. Some participants felt that the guidelines should more clearly define a predetermined range of clean-up standards. However, one of the purposes of the 2006 guidance is to describe federal interactions

with state and local governments, and to establish the principle of site-specific optimization. Site-specific optimization allows for state and local governments to determine acceptable risk for their community/jurisdiction and account for factors such as land use and background levels of radiation. The guidance also urges state and local decision makers to consider the societal, economic, medical, and environmental impacts of a range of site clean-up levels. For example, an acceptable level of risk for a rural area will most likely be different than an acceptable level of risk for a densely populated (urban) environment.

Once the site-specific clean-up level is established, decision makers should develop a strategic plan to ensure consistency of public messaging, and to manage public expectations. The federal government needs to be prepared to explain and support different clean-up choices. Similar circumstances were observed during the FSE when jurisdictions took different protective actions immediately following the explosions, and caused significant public messaging problems.

Recommendation: Develop detailed interagency guidance for implementing the optimization process.

Observation 4.1.4 Area for Improvement: There is limited national laboratory capacity for clinical, environmental, and food sample analysis in the event of an RDD incident.

Analysis: During the FSE, the venues had limited laboratory capacity to assess radionuclides in clinical, environmental, and food samples. This issue was discussed further during the STR and LTR TTXs, where participants identified this as a federal responsibility.

Clinical: Currently, the Centers for Disease Control and Prevention (CDC) has no valid method to test clinical specimens in a radiological emergency for seven of the thirteen highest priority radioisotopes most likely to be used in a terrorist scenario. For those isotopes with existing validated methods, screening 100,000 clinical specimens in the wake of a radiological attack could take more than four years to complete.[39] The existing Laboratory Response Network (LRN) supports chemical and biological testing, but has limited capacity for radionuclide analysis in clinical and non-clinical specimens. Only the CDC and the National Institutes of Health (NIH) labs within HHS can perform this analysis. As such, a need to develop a pre-screening process to determine the segment of the population that would require further radionuclide analysis was identified. This prescreening process would decrease the number of samples sent to laboratories, and allow jurisdictions to obtain the necessary lab results to rapidly distribute medication to those individuals that were exposed.

The CDC dispatched an aircraft to fly 100 samples from Oregon to NIH to test NIH's laboratory capacity. Although NIH was able to provide initial results to the state in 36 hours, it became evident that 100 samples was a stress on NIH's capacity. NIH estimated that it would be able to completely process and assess approximately 65 – 100 samples a

[39] U.S. Representative Brad Miller. *Radiological Response: Assessing Environmental and Clinical Laboratory.* U.S House of Representatives Committee on Science and Technology. October 25, 2007.

day. HHS does not have sufficient capacity to determine the level of exposure for a large population.

The Arizona Department of Health Services (ADHS) also requested CDC laboratory assistance for radiological testing since it did not have this capability. This created additional strain on CDC and NIH resources and caused a backlog of samples for testing that remained at D+50. Without the necessary laboratory assessments, the states were unable to provide an accurate estimate of the number of individuals who might require Prussian Blue following these events. This led to the venues to request excess doses of Prussian Blue and push requests for federal financing of the unused doses.

Environmental: The EPA predicts that it could take as long as two years to analyze the 350,000 samples necessary to conduct a thorough environmental analysis, given the nation's current radiochemistry laboratory infrastructure.[40] Limited availability and access to qualified laboratory technicians to perform the necessary analyses create a significant shortfall in laboratory capacity. Environmental sampling requires specific expertise, qualification, and equipment, depending on the type of sampling to be performed. During an RDD event, it is imperative that state D/As are aware of which laboratories are available for the needed environmental assessments.

In addition, LTR TTX participants discussed the importance of developing clear objectives for sampling and then developing a sampling plan that achieves those objectives efficiently. Such planning can help minimize the number of samples requiring analysis.

Food: Laboratory capacity for testing radionuclides in foods is also limited. At D+50, the FDA was still assessing the first set of samples it had received. At present, there are only three labs in the nation equipped to conduct food testing following an RDD event.

Recommendations: Develop plans to maximize existing clinical, food, and environmental laboratory capacity.

1. Define and communicate current clinical and food laboratory capacity (EPA has defined and communicated environmental laboratory capacity).
2. Investigate the use of the Integrated Consortium Laboratory Network (ICLN) as a formal coordinating entity during times of emergency.
3. Develop a CONOPS plan that includes strategies for maximizing existing clinical, environmental, and food laboratory capacity as well as expanding existing laboratory networks for clinical, environmental, and food samples.

Capability 5: Intelligence/ Information Sharing and Dissemination

Capability Summary: Intelligence/Information Sharing and Dissemination is the multi-jurisdictional, multidisciplinary exchange and dissemination of information and intelligence among the international, federal, state, local, and tribal layers of government, the private sector, and citizens. The goal of sharing and dissemination is to facilitate the distribution of relevant,

[40] U.S. Representative Brad Miller. *Radiological Response: Assessing Environmental and Clinical Laboratory*. U.S House of Representatives Committee on Science and Technology. October 25, 2007.

actionable, timely, and preferably declassified or unclassified information and/or intelligence that is updated frequently to the consumers who need it. Related to this capability are information gathering activities, such as the collection, consolidation, and retention of raw data and information from both human sources and open sources. When analytical products are disseminated, they are the result of synthesis of data and information for the purpose of creating timely and actionable intelligence with an emphasis on the larger public safety and homeland security threat picture. The information provided in this section is summarized from a classified annex to this report

Activity 5.1 Conduct Vertical/ Horizontal Flow of Information

Observation 5.1.2 Area for Improvement: The Common Intelligence Picture/COP varied considerably at the different venues.

Analysis: The intelligence picture varied. Further analysis will be conducted on data collected via the ODNI Evaluator Team and Intelligence Control Cell.

Recommendations: See classified annex.

Observation 5.1.3 Strength: T4 provided a valuable format to examine horizontal and vertical flow of intelligence.

Analysis: The T4 exercise scenario provided the Intelligence Community (IC) an opportunity to share and disseminate intelligence and information among law enforcement, intelligence, emergency management, and other D/As at the local, territorial, state, federal, and international levels.

Observation 5.1.4 Area for Improvement: Intelligence dissemination shortfalls occurred at all levels.

Analysis: Participants failed to receive several key intelligence reports due to classification/tearline and/or information sharing system technology issues. Further analysis will be conducted on data collected via the ODNI Evaluator Team and Intelligence Control Cell.

Recommendations: See classified annex.

Observation 5.1.5 Area for Improvement: Multiple RFI processes and procedures created an inefficient and ineffective system.

Analysis: Multiple RFI processes and procedures created confusion among participants, and resulted in incomplete or slow RFI responses. Further analysis will be conducted on data collected via the ODNI Evaluator Team and Intelligence Control Cell.

Recommendations: See classified annex.

SECTION 4: CONCLUSION

More than one hundred organizations were involved in planning T4, including DHS and other federal agencies; state, territory, and local agencies from the states of Arizona and Oregon and the U.S. Territory of Guam; private sector entities and NGOs; and three international partners: Canada, the United Kingdom, and Australia. The T4 FSE used an RDD scenario to test the full range of federal, state, territorial, and local capabilities. This scenario included coordinated attacks in Guam, Oregon, and Arizona.

A major goal of T4 was to test existing plans, policies, and procedures to identify planning and resource gaps, and ultimately to implement corrective actions to improve the state of the nation's WMD preparedness. Nearly every capability in the DHS TCL was exercised. This AAR focused on national policy and planning issues related to five of those capabilities: On-Site Incident Management, Emergency Operations Center Management, Emergency Public Information and Warning, Economic and Community Recovery, and Intelligence/Information Sharing and Dissemination. The overall exercise was successful in highlighting improvements since previous exercises and Hurricane Katrina, as well as identifying areas requiring further improvement.

Considerable planning and preparedness efforts have been underway to address shortfalls identified in previous TOPOFF exercises and during real-world events. The exercise clearly identified places where the nation's preparedness has improved. It also identified a considerable number of areas that need further improvement. These improvement areas include recurring themes – issues that have been identified in previous TOPOFF exercises and real-world events – along with several new areas highlighted by this scenario.

At the AAC held on January 15, 2008, participating agencies met to review the findings and recommendations in this AAR and draft corrective actions. The IP included in Appendix A lists the corrective actions. The DHS NEP has established a process for tracking and monitoring the implementation of these corrective actions.

This page is intentionally blank.

APPENDIX A: IMPROVEMENT PLAN

This IP has been developed specifically for the T4 FSE conducted on October 15 – 20, 2007 and the LTR TTX conducted on December 4 – 5, 2007. These recommendations draw on the AAR, LTR TTX Quick Look Report, and the AAC. In many cases, these corrective actions will require the establishment of interagency working groups. This IP assumes that the primary responsible agencies will determine the appropriate support agencies and establish working groups, as required. This IP does not include corrective actions already entered into the CAP system or being separately tracked and monitored.

Table A.1 *Improvement Plan Matrix*

Capability	Observation Title	Recommendation	Corrective Action Description	Capability Element	Primary Responsible Agency	Support Agency
On-site Incident Management/ EOC Management	1. Incident Command/ Unified Command	1.1 Establish scenario-based guidance to support national-level plans	1.1.1 Convene an interagency working group to develop concepts and mechanisms to facilitate "unified management of the national response."	Planning	DHS IMPT	
			1.1.2 Review existing national-level planning initiatives (e.g., NIMS, NRF, Incident Annexes, Strategic Plans, Operational Plans, Field Manuals) to identify the appropriate places within the federal family of plans (strategic, operational, and tactical) to incorporate more detailed scenario-based information and better account for the complexities of large-scale emergency response management (such as those involving radiological contamination or multiple levels of government response teams). Specifically address the establishment of multi-jurisdictional unified command structures to support NIMS implementation.	Planning	DHS IMPT	

			1.1.3 Develop scenario-specific training modules for response personnel to improve coordination between federal, state, and local jurisdictions.	Training	DHS NIC	
		1.2 Engage in regional planning, training, and exercise efforts	1.2.1 Incorporate national scenario-based guidance into regional planning, training, and exercise programs such as the RISC or the Regional Assistance Committee (RAC).	Planning	DHS IMPT	
			1.2.2 Document how the FRMAC will incorporate with specific state/local agencies responsible for radiological response in national guidance.	Planning	DHS IMPT	DoE NNSA, EPA
		1.3 Clarify how Incident and Support Annexes are executed within the federal incident management structure executed by the FEMA regions	1.3.1 Review the JFO structure described in the NRF and supporting SOPs to clarify how elements of specific Incident and Support annexes can be incorporated.	Planning	DHS IMPT	
			1.3.2 Develop national-level guidance on how to integrate the FRMAC into the overall command structure during a radiological incident.	Planning	DHS IMPT	DoE NNSA, EPA
On-site Incident Management	2. National Guard WMD CSTs	2.1 Further develop the ability of the CSTs to effectively integrate into WMD HAZMAT responses	2.1.1 Integrate the CSTs into national and regional planning, training, and exercise initiatives described under recommendation 1.1 (such as the review of the NRF and incident annexes).	Planning	States, National Guard Bureau, DHS IMPT	FBI Laboratory Division, HAZMAT Response Unit
			2.1.2 Assess CST equipment caches and TTPs for shortfalls and compatibility to support and complement EPA and DoE site assessment teams.	Equipment	States, National Guard Bureau	EPA, DoE NNSA, FBI Laboratory Division, HAZMAT Response Unit

EOC Management	3. LD/ HD Assets	3.1 Develop contingency plans for multiple RDD/IND incidents	3.1.1 In the review of national planning initiatives, incorporate more details in the federal family of plans on the allocation of specific LD/HD response and protection assets that could be required to respond to multiple incidents.	Planning	DHS IMPT	
			3.1.2 Clarify the roles and responsibilities of different agencies and coordination nodes (e.g., NRCC, CAT) in supporting the process noted above.	Planning	DHS IMPT	
			3.1.3 Develop a training package for senior leadership describing the capabilities of radiological response and protection assets.	Training	DHS NIC NPT	DoE, EPA, FBI, DoD, DHS ICE
			3.1.4 Develop decision matrices for senior leadership for the activation and deployment of radiological response and protection assets.	Planning	DHS IMPT	DoE, EPA, FBI, DoD. DHS ICE
		3.2 Identify assets that can partially replicate LD/HD assets	3.2.1 Investigate the cost/benefit of NOT deploying the early phase assessment functions of the FRMAC to an incident site and augmenting CMHT capabilities to increase the FRMAC's ability to support multiple incident sites.	Planning	DoE NNSA	EPA
			3.2.2 Identify contingencies where specialized DoD assets would likely be requested to support FRMAC operations and develop pre-scripted mission assignments/pre-scripted formal requests for assistance under the Economy Act to expedite the request and response process in an emergency.	Planning	DoE NNSA, DoD	EPA
			3.2.3 Request DoD planners (JFCOM) evaluate Collaborative	Planning	DoD	

			Force Analysis, Sustainment and Transportation (CFAST) sourcing of units in a crisis to ensure answers are provided in hours vs. the current deliberate planning process which takes days.			
			3.2.4 Identify contingency circumstances where MOUs or other agreements with foreign countries would be appropriate and required to support FRMAC operations.	Planning	DoE NNSA, DoS	EPA
	4. Federal Interagency Operational Cycle	4.1 Establish a framework for the federal interagency operational cycle	4.1.1 Review and align meeting and reporting schedules.	Planning	DHS Office of Operations Coordination	Federal interagency
			4.1.2 Consider scope, attendance, and classification level of senior leadership meetings, as well as procedures for capturing and disseminating discussions, decisions, and taskings.	Planning	DHS Office of Operations Coordination	Federal interagency
			4.1.3 Summarize working group recommendations in a draft policy for review and approval by the HSC.	Planning	DHS Office of Operations Coordination	Federal interagency
	5. Federal SOs	5.1 Review and clarify the roles and responsibilities of SOs in the policies, procedures, and training that support the JFO cell	5.1.1 Clarify SO roles/ responsibilities in JFO SOPs and incorporate in training.	Planning	DHS NIC	
	6. Private Sector Integration	6.1 Continue to institutionalize and formalize relationships between government, private sector, non-	6.1.1 Clarify private sector partnership models in policies, plans, and procedures in accordance with national response and recovery policies.	Planning	DHS OIP, DHS PSO, DHS/FEMA PSO	Private sector organizations, S/L
			6.1.2 Review and update policy documents to clarify the purpose,	Planning	DHS OIP, DHS PSO,	Private sector organizations,

		government, and CI/KR organizations	roles, and responsibilities for various private sector NGOs.		DHS/FEMA PSO, DHS CRCL	S/L
			6.1.3 Articulate and institutionalize a process for private sector and NGO engagement in national-level exercises, including authority for planning, programming, and budgeting for national and venue working groups.	Planning	DHS OIP, DHS PSO, DHS/FEMA PSO, DHS CRCL	Private sector organizations, S/L
	7. Special Needs Integration	7.1 Continue to incorporate special needs play within national-level exercises	7.1.1 Articulate and institutionalize a process for special needs engagement in national-level exercises with additional objectives to focus specifically on decisions regarding special needs.	Planning	DHS NEP, DHS NIC, DHS CRCL	
	8. International Assistance	8.1 Clarify the relationship of the IAS CONOPS and the procedures/ authorities for considering and accepting cash donations	8.1.1 Address issue through the working group that created these procedures (currently underway).	Planning	DoS	
Public Information and Warning	9. Information Sharing	9.1 Continue teleconferences and consider further methods to share information	9.1.1 Consider the use of virtual tools (such as web conferencing and chat rooms) to supplement NICCL calls.	Planning	DHS OPA	
		9.2 Develop additional information sharing tools and processes	9.2.1 Evaluate smart practices and suggestions on information management identified in the AAR.	Planning	DHS OPA	
			9.2.2 Investigate information technology solutions that support e-mail distribution lists that can be easily modified.	Equipment	DHS OPA	
	10.	10.1 Investigate	10.1.1 Continue work underway by	Planning	IMAAC	DoE/FRMAC

	Incorporating Scientific Information Into Public Messaging	ways to facilitate the integration of scientific information into public messaging	the interagency IMAAC and FRMAC Working Groups to develop hazard area graphics (maps and summary language) for RDDs that can be easily understood by local, state, and federal officials and to highlight key information such as the IMAAC operations center phone number.		Working Group	
			10.1.2 Investigate ways to provide subject matter expertise to JICs and other public affairs personnel; consider arrangements with the private sector and universities in addition to using government experts.	Planning	F/S/L public affairs agencies	IMAAC Working Group
			10.1.3 Conduct IMAAC training exercises as standalone events or in coordination with national-level exercises to help institutionalize IMAAC process/procedures at the state/local level as IMAAC funding permits or with external funding (e.g., from NEP).	Training	DHS NEP, DHS NIC NTP	IMAAC Working Group
		10.2 Investigate ways to help local, state, territorial, and federal government officials explain and clarify different actions across jurisdictions	10.2.1 Consider mechanisms to promote cross-jurisdictional coordination by public affairs officials, such as ESF-15 coordination calls (in addition to NICCL calls).	Planning	DHS OPA	
			10.2.2 Develop and promulgate written Strategic Communication Planning guidance, establish and exercise interagency strategic communication team to address: a) national themes, effects, and tasks b) international engagement strategy c) processes and procedures.	Planning	HSC	Federal Interagency

Economic and Community Recovery	11. Recovery Planning	11.1 Fully incorporate recovery into national-level policies and plans	11.1.1 Expand the national planning scenarios to provide more details on recovery.	Planning	DHS IMPT	
			11.1.2 In the review of national planning initiatives, incorporate recovery into the federal family of plans, (strategic, operational, and tactical).	Planning	DHS IMPT	
			11.1.3 Clarify the role and responsibilities of governments, NGOs, and private sector organizations and entities in recovery.	Planning	DHS IMPT	PSO, FEMA/ PSO, and IP
			11.1.4 Develop and incorporate policies for communications to support recovery efforts.	Planning	DHS OPA	
			11.1.5 Ensure that the needs of unique entities, such as territories, islands, and tribal lands, are adequately addressed in recovery documents.	Planning	DHS IMPT	
			11.1.6 Develop a guidance document for state, territory, tribal, and local agencies on available federal interagency individual assistance programs and how to access them.	Planning	DHS DAD	
			11.1.7 Address the coordination of access control and credentialing in SOPs and plans.	Planning	DHS IMPT	Federal interagency, S/L, private sector organizations
			11.1.8 Establish a national policy to encourage redundancy in CI systems (e.g., water supply).	Planning	DHS OIP, DHS PSO, DHS/FEMA PSO	Private sector organizations, S/L, SSAs
			11.1.9 Pre-develop options for private sector and NGO incentives	Planning	DHS OIP, DHS PSO,	Private sector organizations,

			as well as liability protections that could be offered to attract private sector and NGO involvement in restoring infrastructure.		DHS/FEMA PSO, DHS CRCL	S/L
			11.1.10 Identify options (legislative, regulatory, or federal policy) to provide federal support to other jurisdictions outside of the incident site that sustain what could be long-term spikes in demand on infrastructure due to mass migrations and displacement.	Planning	DHS NPPD	Federal interagency, S/L
			11.1.11 Identify available disposal capacity and potential gaps for radiologically contaminated waste from an RDD. Include the assessment of existing DoE sites, and any limitations that might exist on using them for RDD waste.	Planning	DoE, NRC, EPA, USACE	
			11.1.12 Clarify statutory authority and roles and responsibilities for all jurisdictions in dealing with issues surrounding property condemnation, reimbursement, and subsequent reoccupation of condemned and contaminated structures after receiving certification for reoccupation.	Planning	DHS FEMA	S/L, private sector organizations, EPA, USACE
			11.1.13 Develop an interagency plan for assistant states in conducting health monitoring and leveraging resources from other federal agencies.	Planning	HHS	DoE, S/L
			11 1.14 Develop an HHS deployment, tracking, screening, and surveillance program that can serve as a best practice for other responder agencies.	Planning	HHS	Federal interagency

			11.1.15 Develop a policy for helping state and local agencies establish registries for tracking health effects in affected populations.	Planning	HHS	OSHA, S/L
			11.1.16 Develop policies and procedures for A-Team activation and operation.	Planning	HHS	DoE NNSA, EPA, USDA
			11.1.17 Identify and utilized existing funding, programs, and training to address the disaster mental health planning.	Planning	HHS/ SAMHSA	S/L
	12. RDD/IND Protective Action Guides	12.1 Provide guidance for implementing the site optimization process	12.1.1 Develop detailed guidance for implementing the site optimization process.	Planning	EPA	
	13. Laboratory Capacity	13.1 Develop plans to maximize existing clinical, environmental, and food laboratory capacity	13.1.1 Define and communicate current laboratory capacity for clinical and food (EPA has defined and communicated environmental laboratory capacity).	Planning	HHS	USDA
			13.1.2 Investigate the use of the ICLN as a formal coordinating entity during times of emergency.	Planning	DHS S&T	HHS, EPA, DoE, DoD, USDA
			13.1.3 Develop a CONOPS that includes strategies for maximizing existing clinical, environmental, and food laboratory capacity.	Planning	HHS	EPA, USDA

This page is intentionally blank.

APPENDIX B: ACRONYMS

Table B.1: *Acronyms*

Acronym	Meaning
AAFC	Agriculture Canada
AAR	After-Action Report
ACE	U.S. Army Corps of Engineers
ACS	Australian Customs Service
AcTIC	Arizona Counter-Terrorism Information Center
ADHS	Arizona Department of Health Services
AFP	Australian Federal Police
AGD	Attorney-General's Department (Australia)
AMS	Aerial Measuring System
ANSTO	Australian Nuclear Science and Technology Organisation
AOC	Agency Operations Center
ARC	American Red Cross
ARPANSA	Australian Radiation Protection and Nuclear Safety Agency
ARRA	Arizona Radiation Regulatory Agency
ASD-HD	Assistant Secretary of Defense for Homeland Defense
ASIO	Australian Security Intelligence Organisation
ASU	Arizona State University
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BOC	Business Operations Center
CAT	Crisis Action Team
CBSA	Canadian Border Services Agency
CDC	Centers for Disease Control and Prevention
CEWG	Control and Evaluation Working Group
CI/KR	Critical Infrastructure/Key Resources
CIC	Citizenship and Immigration (Canada)
CIR	Critical Information Requirement
CMHT	Consequence Management Home Team (DoE NNSA)
CMHT/OR	Consequence Management Home Team for the Oregon Incident
CMRT	Consequence Management Response Team (DoE NNSA)
CNSC	Canadian Nuclear Safety Commission
COGCON	Continuity of Government Readiness Conditions
CONPLAN	Concept of Operations Plan
COOP	Continuity of Operations
COP	Common Operating Picture

COSIN	Control Staff Instructions
CRCL	Civil Rights and Civil Liberties (DHS)
CSE	Communications Security Establishment
CSG	Counterterrorism Security Group
CSIS	Canadian Security Intelligence Service
CST	Civil Support Teams
CWG	Cyber Working Group
D	Detonation
D/As	Departments/Agencies
DEST	Domestic Emergency Support Team
DFAIT	Department of Foreign Affairs and International Trade (Canada)
DFAT	Department of Foreign Affairs and Trade (Australia)
DHS	Department of Homeland Security
DIAC	Department of Immigration and Citizenship (Canada)
DND	Department of National Defence (Canada)
DoC	Department of Commerce
DoD	Department of Defense
DoE	Department of Energy
DOHA	Department of Health and Ageing (Australia)
DoL	Department of Labor
DoS	Department of State
DoT	Department of Transportation
DRG	Domestic Readiness Group
DSAT	DHS Situational Awareness Team
EAWG	External Affairs Working Group
ECC	Emergency Command Center
EMA	Emergency Management Australia
EMG	Emergency Management Group
EMS	Emergency Medical Services
ENDEX	End of Exercise
EOC	Emergency Operations Center
EOD	Explosive Ordnance Disposal
EPA	Environmental Protection Agency
EPA NCERT	EPA National Counter Terrorism Evidence Response Teams
EPA RERT	EPA Radiological Emergency Response Team
ERT	Emergency Response Team (FEMA)
ESC	Executive Steering Committee
ESF	Emergency Support Function
EVALPLAN	Evaluation Plan

EXPLAN	Exercise Plan
FBI	Federal Bureau of Investigation
FCO	Federal Coordinating Official
FCO	Foreign & Commonwealth Office (United Kingdom)
FD	Fire Department
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
~~FOUO~~	~~For Official Use Only~~
FRMAC	Federal Radiological Monitoring and Assessment Center
FSE	Full-Scale Exercise
GFP	Guam Fire Department
GIS	Geographic Information System
GOC	Government Operations Centre (Canada)
GPD	Guam Police Department
HAZMAT	Hazardous Materials
HHS	Department of Health and Human Services
HMRT	HAZMAT Response Team (FBI)
HMRU	HAZMAT Response Unit (FBI)
HSAS	Homeland Security Advisory System
HSC	Homeland Security Council
HSEEP	Homeland Security Exercise and Evaluation Program
HSIN	Homeland Security Information Network
IAS	International Assistance System
IC (Canada)	Industry Canada
IC	Incident Command
IC	Intelligence Community
ICE	Immigration and Customs Enforcement (DHS)
ICLN	Integrated Consortium Laboratory Network
ICP	Incident Command Post
ICS	Incident Command System
IDETF	Inter-Departmental Emergency Task Force
IMAAC	Interagency Modeling and Atmospheric Assessment Center
IMPT	Incident Management Planning Team
IND	Improvised Nuclear Device
IOF	Interim Operating Facility
IP	Improvement Plan
IWG	Intelligence Working Group
JFO	Joint Field Office
JIC	Joint Information Center

JIS	Joint Information System
JOC	Joint Operations Center (FBI)
JTF-HD	Joint Task Force-Homeland Defense
LD/HD	Low Density/High Demand
LEO VCC	Law Enforcement Online Virtual Command Center
LNO	Liaison Officer
LRN	Laboratory Response Network
LTR	Long-Term Recovery
MSEL	Master Scenario Events List
NCC	National Crisis Committee (Australia)
NCR	National Capital Region
NED	National Exercise Division
NGO	Non-governmental Organization
NICC	National Infrastructure Coordinating Center
NICCL	National Incident Communications Conference Line
NIH	National Institutes of Health
NIMS	National Incident Management System
NJIC	National Joint Information Center
NNSA	National Nuclear Security Administration
NOAA	National Oceanic and Atmospheric Administration
NOC	National Operations Center
NORTHCOM	U.S. Northern Command
NPS	National Planning Scenario
NRAT	Nuclear/Radiological Advisory Team
NRCan	Natural Resources Canada
NRCC	National Response Coordination Center
NRF	National Response Framework
NRP	National Response Plan
NSC	National Security Committee of Cabinet (Australia)
NSC	National Security Council
NWS	National Weather Service
OCD-GHS	Office of Civil Defense – Guam Homeland Security
ODNI	Office of the Director of National Intelligence
OIP	Office of Infrastructure Protection (DHS)
OPA	Office of Public Affairs (DHS)
OSC	On-Scene Coordinator
OSHA	Occupational Safety and Health Administration
PACOM	U.S. Pacific Command
PFO	Principal Federal Official

PFR	Portland Fire and Rescue
PIO	Public Information Officer
PM&C	Department of Prime Minister and Cabinet (Australia)
POC	Point of Contact
POD	Partnership and Outreach Division
POEM	Portland Office of Emergency Management
PPB	Portland Police Bureau
PSC	Public Safety Canada
PSCC	Protective Security Coordination Centre (Australia)
PSO	Private Sector Office
PSWG	Private Sector Working Group
PWGSC	Public Works and Government Services Canada
RAP	Radiological Assistance Program (DoE)
RCMP	Royal Canadian Mounted Police
RDD	Radiological Dispersal Device
REAC/TS	Radiation Emergency Assistance Center/Training Site (DoE NNSA)
REOC	Regional Emergency Operations Center (EPA)
RFI	Request for Information
RISC	Regional Interagency Steering Committee
RPS	Radiation Protection Services (Oregon)
RRCC	Regional Response Coordination Center (FEMA)
SAC	Special Agent in Charge (FBI)
SBA	Small Business Administration
SC	Service Canada
SEO	Senior Energy Official
SEOC	State Emergency Operations Center
SFLEO	Senior Federal Law Enforcement Official
SIMCELL	Simulation Cell
SIOC	Strategic Information and Operations Center (FBI)
SITREP	Situation Report
SL	Senior Leadership
SLG	Senior Leadership Group
SME	Subject Matter Expert
SO	Senior Official
SOP	Standard Operating Procedure
STR	(b)(6) Recovery
STRATCOM	U.S. Strategic Command
SVTC	Secure Video Teleconference
SWAT	Special Weapons and Tactics

SWG	Scenario Working Group
T2	Top Officials 2
T3	Top Officials 3
T4	Top Officials 4
TC	Transport Canada
TCL	Target Capabilities List
TOPOFF	Top Officials
TPEP	Terrorism Prevention Exercise Program
TSA	Transportation Security Administration
TTP	Tactics, Techniques, and Procedures
TTX	Tabletop Exercise
UA	Universal Adversary
UC	Unified Command
USAR	Urban Search and Rescue
USCG	U.S. Coast Guard
USDA	U.S. Department of Agriculture
USG	United States Government
VA	Department of Veterans Affairs
VAMC	Veterinary Medicine Advisory Committee
VIPR	Visible Intermodal Protection and Response
VNN	Virtual News Network
VSIN	VA Network
VTC	Video Teleconference
WMD	Weapon of Mass Destruction

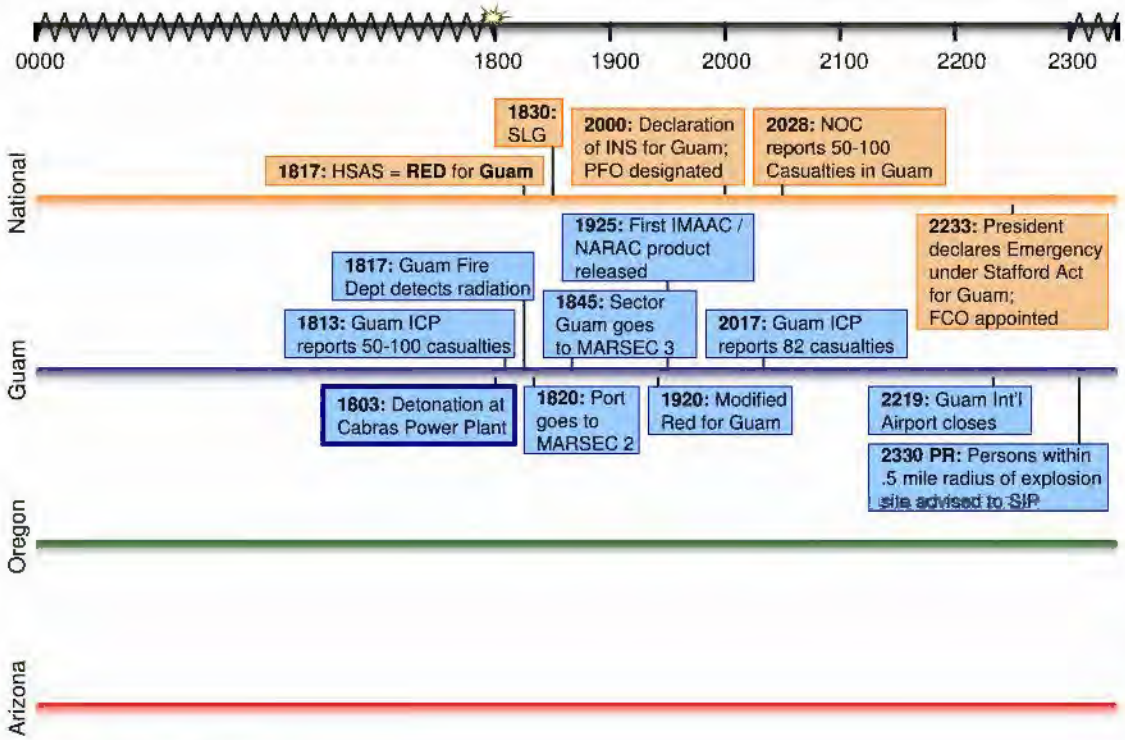
APPENDIX C: REFERENCE LIST

1. Department of Homeland Security Office of Infrastructure Protection AAR/IP
2. Department of Homeland Security, *DHS/OPS TOPOFF 4 Corrective Action Prioritization Tool*, December 2007.
3. Department of Homeland Security, Federal Emergency Management Agency (FEMA) National Response Coordination Center (NRCC) Standard Operating Procedure (SOP).
4. Department of Homeland Security, Federal Emergency Management Agency. *TOPOFF 4 Long-Term Recovery Tabletop Exercise Situation Manual (SitMan)*, December 2007.
5. Department of Homeland Security, Federal Emergency Management Agency. *TOPOFF 4 Long-Term Recovery Tabletop Exercise Reference Manual*, December 2007.
6. Department of Homeland Security, Federal Radiological Dispersal Device (RDD) Strategic Plan Summary.
7. Department of Homeland Security, Homeland Security Exercise and Evaluation Program (HSEEP): Volume III Exercise Evaluation and Improvement Planning, February 2007.
8. Department of Homeland Security, Homeland Security Information Network (HSIN): Concept of Operations Version 1.0, May 15, 2006.
9. Department of Homeland Security, Homeland Security Presidential Directives (HSPD) 5-8, December 2003.
10. Department of Homeland Security, Interagency Integrated Standard Operating Procedure (SOP): National Operations Center (NOC), September 2006.
11. Department of Homeland Security, National Incident Management System (NIMS), March 2004.
12. Department of Homeland Security, National Operations Center (NOC) Situational Awareness (SA) Common Operational Picture (COP): User Manual, April 27, 2007.
13. Department of Homeland Security, National Preparedness Goal, December 2005.
14. Department of Homeland Security, *National Response Plan*, December 2004.
15. Department of Homeland Security, *Notice of Change to the National Response Plan*, May 25, 2005.
16. Department of Homeland Security, Secretary DHS Crisis Action Team (CAT) Standard Operating Procedures (SOP), August 2007.
17. Department of Homeland Security, Standard Operating Procedure for the Interim Interagency Modeling and Atmospheric Assessment Center (IMAAC), December 8, 2006.
18. Department of Homeland Security, Target Capabilities List (TCL), September 2006.
19. Department of Homeland Security, TOPOFF 4 Full Scale Exercise Plan, May 2007.
20. Department of Homeland Security, Universal Task List (UTL): Version 2.1, May 23, 2005.
21. Department of State, *Consular Notification and Access*. January 2003
22. FM 3-11.22, Department of the Army Headquarters, JUNE 2003

23. *International Assistance System Concept of Operations*, September 4, 2007, developed by an interagency working group led by the Department of State and Department of Homeland Security.
24. National Nuclear Security Administration, FRMAC Operations Manual, December 2005. DOE/NV/11718—080-Rev. 2.
25. *Procedures for Foreign Cash Donations Offered in Response to a Disaster Affecting the United States*, June 22, 2007.
26. TOPOFF 2 After-Action Report
27. TOPOFF 3 After-Action Report
28. TOPOFF 4 Command Post Exercise After-Action Report
29. Lawrence Livermore National Laboratory. TOPOFF4 IMAAC After-Action Report. November 21, 2007.
30. U.S. Representative Brad Miller. *Radiological Response: Assessing Environmental and Clinical Laboratory*. U.S House of Representatives Committee on Science and Technology. October 25, 2007.
31. White House Homeland Security Council, *HSC TOPOFF 4 Lessons Learned*, November 9, 2007.
32. White House Homeland Security Council, *The Federal Response to Hurricane Katrina, Lessons Learned*. February 2006.

APPENDIX D: TIMELINE OF KEY EXERCISE EVENTS

Figure D.1: *Key Events (October 15, EDT)*



PR = Press Release

Figure D.2: *Key Events (October 16, 0001 – 1600 EDT)*

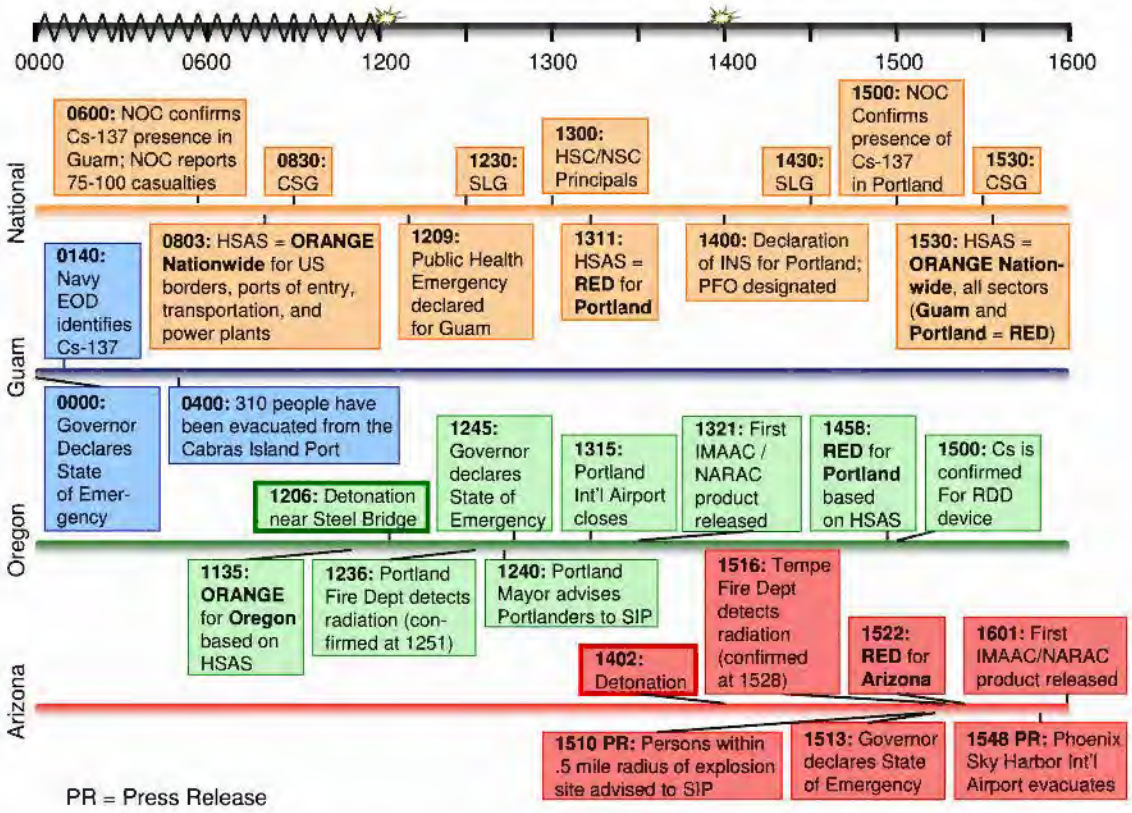


Figure D.3: *Key Events (October 16, 1600 – 2400 EDT)*

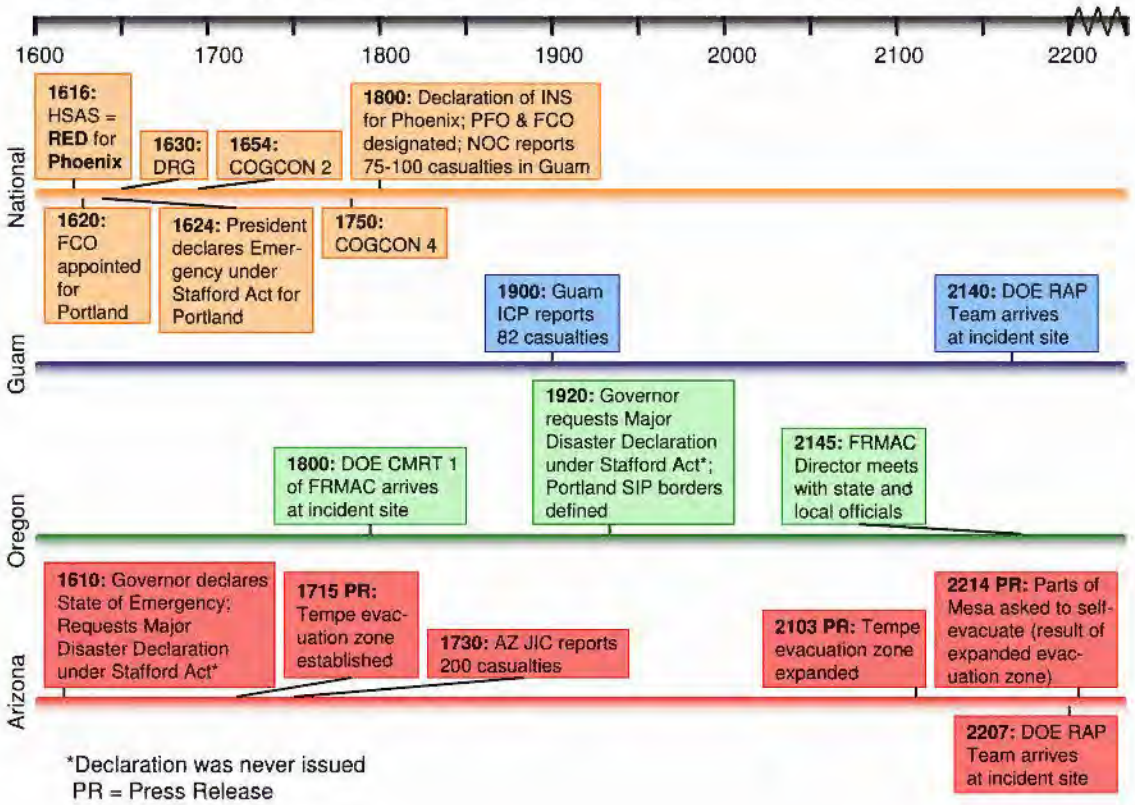


Figure D.4: *Key Events (October 17, EDT)*

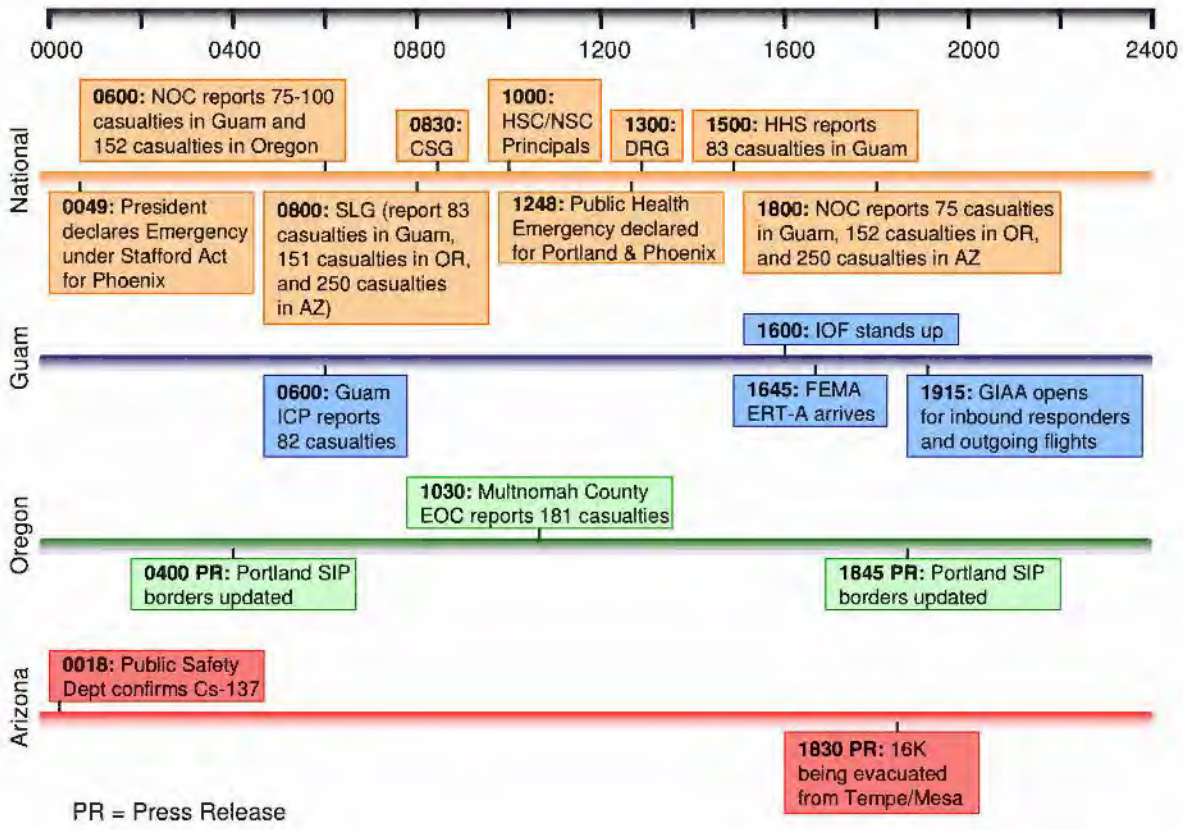
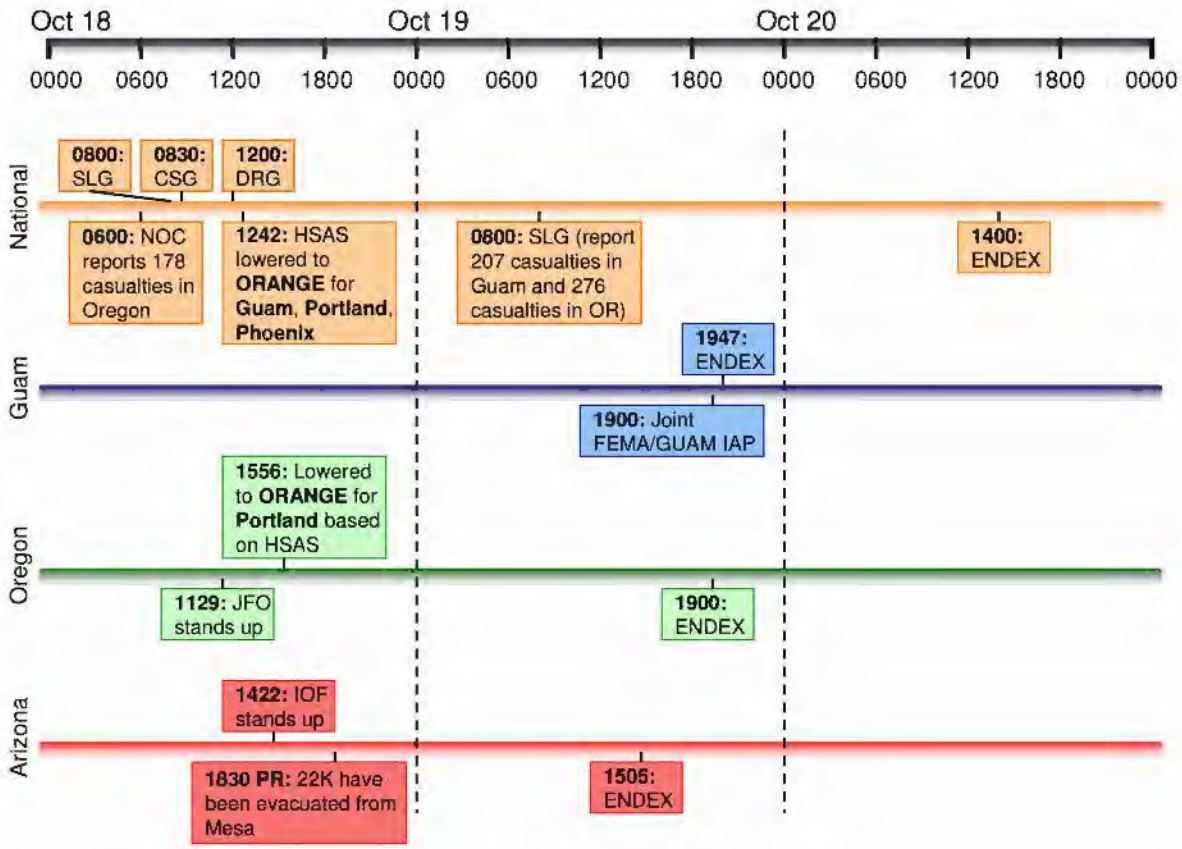


Figure D.5: *Key Events (October 18 – 20 EDT)*



This page is intentionally blank.

ANNEX 1: EXERCISE DESIGN AND DEVELOPMENT

This Annex is provided to summarize key issues and observations noted during the portion of the AAC focused on the design and development process of the T4 exercise. Under the guidance of the T4 ESC, working groups were formed at the national level to support the design and development process with the support of participating D/As within the NCR. These working groups were replicated at each venue to provide key planners the required insight and background for exercise development at the regional, state, territorial, and local levels.

The overall T4 exercise design and development process consisted of identifying capabilities, tasks, and objectives; designing the scenario; developing documentation; coordinating external affairs events and logistics; planning exercise conduct; and selecting an evaluation and improvement methodology. A summary of the key observations (strengths and areas for improvement) noted by each of the working groups and venue sponsors during and following the AAC are provided in the paragraphs below.

Prevention Component

Strengths:

- The significant level of commitment and play by state and local law enforcement participants to the expanded prevention element added a new and necessary element to the TOPOFF exercise package. State and local law enforcement, along with in-venue federal entities (most notably, FBI field offices in Guam, Phoenix, and Portland) devoted time and resources to exercise planning and conduct.
- The structure and duration of the prevention component allowed for immediate "return on investment" to the participating agencies. The areas for improvement identified during the prevention element allowed players to attempt to resolve issues and improve capabilities during the response portion that followed.

Areas for Improvement:

- Some elements of prevention play were limited by the need to constrain the scenario and roll into the response phase. Although discrete prevention successes were developed that did not interfere with the response scenario, some constraints required by the follow-on response exercise prohibited full realistic and comprehensive prevention play.
- Fiscal constraints kept some agencies from providing optimum commitment to the prevention scenario. Some elements of the scenario were overly focused at the state and local law enforcement level due to the inability of federal agencies in the NCR to commit to full play. Attempts to simulate federal play were not always adequate to generate a realistic environment for participating law enforcement agencies at the state, territorial, and local level.
- The prevention component needs to be more effectively coordinated with the IWG. Better coordination will allow prevention play to incorporate more D/As that would

support real-world prevention activities. Better integration of the intelligence effort would also support the requirement for improved coordination/ visibility across unclassified and classified information systems. During exercise execution, better integration of prevention and intelligence MSELs would provide more effective training for participating agencies.

- Future prevention exercises should consider what other entities (e.g., the private sector, public safety professionals, etc.) would be impacted by the information and intelligence that is gathered and shared during the lead up to the response element. These additional factors should be accounted for in the integrated MSEL development of the prevention exercise.

Scenario Working Group

Strengths:

- In NPS-11, "*...the Universal Adversary (UA) purchases stolen cesium chloride to make a radiological dispersal device (RDD), or 'dirty bomb.' The explosive and the shielded cesium 137 (137Cs) sources are smuggled into the U.S. Detonator cord is stolen from a mining operation, and all other materials are obtained legally in the United States. Devices are detonated in three separate, but regionally close, moderate-to-large cities.*" With this substantive scenario as its foundation, the SWG was able to adapt the overarching T4 objectives into a plausible and effective exercise scenario. The NPS provided an appropriate level of technical and operational specificity, yet adequately accommodated the unique directions provided by the T4 ESC to allow the SWG to tailor the story to specific requirements provided by the federal, state, territorial, and local participants.

Areas for Improvement:

- The ESC directed the SWG to lock the scenario on July 2, 2007. Despite this, several organizations made changes or additions to the scenario to support their organizational objectives without informing the SWG. While most of these changes were eventually accommodated, changes made after the designated locking of the scenario resulted in extensive re-work.
- Elements of the Ground Truth relating to technical or physical aspects of the simulated source material acquisition, transportation, and weapon construction required subject matter expertise and consultation. While help from several key federal D/As and national laboratories was provided, it was offered on an ad-hoc, voluntary basis. Responsibility for this expertise was never officially assigned or accepted. The lack of accountability resulted in an ill-defined level of technical expertise and support.
- Designated D/As with recognized subject matter expertise should be ultimately responsible for developing of the Ground Truth technical details required to support the scenario. Ground Truth details should include technical details about weapons systems and effects, characteristics of UA individuals and organizations, and detailed information essential to law enforcement investigation. A dedicated group focused on the Ground Truth should be set up to augment the work of the SWG to ensure the integration, de-confliction, and validation of required information.

Intelligence Working Group

Strengths:

- Controllers, evaluators, and observers noted the very good cooperation at all levels within IWG. During exercise execution, communication among controllers within the ICC was free flowing and could be an example of how intelligence agencies, defense, and law enforcement could work together in a centralized fusion center.
- The Scripting Conferences facilitated by the IWG provided a forum where all participating representatives could provide input and comment on key intelligence-related aspects of the scenario that could not be discussed at SWG meetings due to their classification. Because the overall script at the national level generally remained unchanged, there were few disconnects due to scripting and writing of ad-hoc events.
- Access to SVTCs conducted during the exercise by the CSG was invaluable for the ICC. This insight allowed ICC controllers to monitor player action and response to intelligence implementers in real time.

Areas for Improvement:

- A chairperson for the IWG should be designated who would be responsible for defining the intended level of effort of each member organization, including instructions, roles, responsibilities, and milestones. Additionally, the IWG chairperson and staff should identify the intelligence community controller and evaluator staffing requirements early in the exercise design process to help planning continuity.
- There was an inadequate level of realistic "white noise" in the intelligence database system to plausibly replicate a real-world threat stream. Incorporating additional information not critical to the scenario's main threat stream would provide players and analysts with a more challenging and complex intelligence picture. This information should be incorporated more effeetively into the UA database.
- A DHS exercise portal and web-based content management system similar to the Extranet Secure Portal (ESP) should be created based upon other more commonly used Homeland Security classified and unclassified networks (e.g., HSIN, HSDN, and C-LAN/JWICS). These systems should provide role-based access to appropriate intelligence, defense, and law enforcement users by exercise.
- A law enforcement working group should be considered in order to encourage better integration of the intelligence and law enforcement communities.
- Further development and funding of the UA database would provide a more realistic threat stream for intelligence exercise support. Ideally this database would be housed within a national-level SIMCELL.
- Coordination of international partners' integration into intelligence planning early in the exercise planning process is integral to the realistic representation of information sharing. Early miscommunication among U.S. and partner nation planners resulted in an unrealistically restricted information sharing process.

International Working Group

Strengths:

- The International Working Group was a successful forum for coordinating international partner participation with U.S. government D/As. This coordination was further facilitated by scheduling International Working Group meetings to coincide with DHS National Planning Seminars and T4 planning conferences.
- International participation in National Seminars and planning conferences allowed key partner nation representatives to learn more about U.S. emergency response policies and procedures. Additionally, their participation provided U.S. federal, state, and local representatives with valuable insight into the international dimension of domestic incidents, and fostered bilateral working relationships that are key to response and recovery activities.
- The early establishment of international and DoS objectives facilitated focused exercise planning and participation, and supported the deployment of a DoS representative and international consular officials to Portland. Exercising the consular affairs aspect of emergency response was new to TOPOFF and added realism to live play.
- The creation of the Quadrilateral Public Affairs Agreement among the four participating nations during exercise planning facilitated information sharing among key U.S. and partner nation players.

Areas for Improvement:

- Unlike T3, when international partners conducted domestic exercises, there were no terrorist events in the partner nations during T4. International planners agreed that events in partner nations related to the U.S. domestic incident would drive more realistic play for international players, vs. only reacting to a U.S. domestic event.
- Given the wide disparity in time zones, the lack of consistent 24/7 exercise play in all venues hindered the full integration of international play and response efforts. Additionally, levels of play among partner nations and U.S. role players varied widely, impacting exercise realism.
- Federal identification of international partner nations and international observer nations earlier in the planning process would facilitate exercise and observer program activities.
- Procedures for sharing ~~"For Official Use Only" (FOUO)~~ documents with international partners were established on a delayed basis. Planners should have these procedures in place early, in the event that future international partners go beyond Australia, Canada, and the United Kingdom.
- No more than three international partner nations should be considered for future NLEs because of finite USG resources and ability to incorporate international participation in domestic play.

Private Sector Working Group

Strengths:

- The defined schedule of meetings helped participants to follow the progression of exercise design. The support and materials provided by the DHS team allowed private sector entities to continue the development of key issues and to integrate the efforts of the other exercise working groups.
- The T4 experience gave exercise planners an appreciation for the breadth and depth of private sector capabilities to recover from a crisis. Awareness was raised in key areas including supply chain issues, operational shortfalls, and public-private sector incident management system relationships. The different levels of participation, (e.g., TTX, Looking Glass, or SIMCELL) provided organizations with choices.
- The exercise provided participating agencies with opportunities to learn about and expand existing methods of integrating national-level policies (e.g., NIMS) into private sector processes. The exercise illustrated the need for additional clarity on information sharing materials and processes required in emergency situations.

Areas for Improvement:

- Private sector integration and engagement needs to be continually expanded and developed. In order to integrate the objectives of private sector entities, NGOs, and special needs organizations, input should be sought much earlier in the planning process. There should be careful planning about when and where participation should be included. This integration would support scripting of MSEL injects to ensure both realism and relevance to real-world situations.
- The term "private sector" lacks a clear definition. There should be clear distinction between the level of participation of CI/KR entities and their representative organizations (Partnership for Critical Infrastructure Security/PCIS), individual large corporate partners (e.g., Wal-Mart, Boeing, Cisco Systems, etc.), NGOs and voluntary organizations, and state and local business partners. Each of these distinct representatives of private sector interests would have different objectives and requirements for participation in national-level exercise events.
- Although great progress was made to include large private sector entities, there was inadequate participation by NGOs and local service organizations. This resulted in a significant gap in human services delivery during response and recovery. Local NGOs and voluntary organizations are most familiar with the types of support needed to maintain the population's physical and mental well-being. Local organizations are the foundation for long-term recovery and should be encouraged to participate early in the planning process.
- Security and handling of official documents used by the private sector should be established early in the process to be fully understood, appreciated, and implemented by all participants. Policies should address requirements for and restrictions on document sharing and disclosure limitations for sensitive information. A designated team with specific disclosure control responsibilities would be most effective.

- Many exercise terms (e.g., "planner", "controller") may not be familiar to private sector entities, NGOs, or special needs exercise participants. An "Exercise 101" course should be made available to support their involvement in the exercise process.

Control and Evaluation Working Group

Strengths:

- The expanded attention to MSEL development by a broader cross section of D/As led to the creation of a more complex and realistic exercise in many targeted areas of interest. Several organizations at the federal level that had not previously participated in TOPOFF took the opportunity to develop MSEL events that stressed defined training objectives. MSEL injects supporting special needs populations, international consular affairs issues, and CI areas were noteworthy.
- Increased access to federal operations centers – especially the placement of evaluators in the NOC – led to more insightful evaluation and analysis. Evaluators were able to observe the multi-tasking done by the IMPT and the NOC CAT. Enhanced access to the NOC and other key operations centers allowed the evaluation team to better assess processes across the spectrum of federal, state, and local participating agencies.
- Due to the exceptional efforts of the FBI Tactical Response Unit, access to classified communications systems was available for the first time in a TOPOFF exercise at the same location as the MCC. The portable systems installed by the FBI allowed the exercise directors and their key leadership teams to communicate in real time with the ICC and numerous DoD and law enforcement elements of the exercise control structure.

Areas for Improvement:

- Attendance at the NCR Working Group meetings and training sessions was limited. Exercise planning teams need to redefine the objectives of the CEWG and lay out specific milestones and timelines during the planning process. A defined schedule would contribute to an effective control and evaluation architecture that could begin with a small focused group that grew in attendance and responsibilities as exercise execution approached.
- HSEEP guidance should be reviewed to ensure that it effectively addresses and supports the unique requirements and level of participation expected in a Tier 1 NLE. Current guidance does not adequately address the full spectrum of interagency participation at the highest federal level.
- The current process of planning, developing, executing, and evaluating TOPOFF is not linked to a common training program that would teach knowledge, skills, and abilities to the "top official" target audience. Training standards are established and administered for operational and tactical participants by their own agency or governmental authority, but strategic decision makers at all levels of government receive information and knowledge on an ad-hoc basis. A training program linked to the NLE would significantly enhance the participation and success of "top officials" in the NEP.

- The continued development of a standing DHS exercise control cell facility with classified and unclassified IT connectivity is essential to exercise quality and continuity. The current need to build the control architecture, (i.e., computers, video projection, telephones, etc.) just prior to exercise execution intensifies the demanding work of supporting an NLE. An adaptable MCC that could be expanded or contracted as exercise requirements dictate would provide a greatly improved capability to support interagency federal, state, and local training and exercise objectives.
- Additional emphasis must be put on synchronizing the MSEL, particularly events that affect multiple agencies. These synchronization efforts should be incorporated into the planning during CEWG meetings at both the national and venue level.
- The training plan for controllers and evaluators should he expanded. The complexity of the Tier 1 exercise program requires more extensive training tailored to the specific requirements of each exercise venue. If controllers and evaluators could be identified earlier in the exercise planning process, a control and evaluation training schedule could be integrated into the venue visit and interagency group meeting schedules.
- The development of a more extensive SIMCELL within the MCC and VCCs would enhance the realism for many participating agencies needing to interact with specific departments, agencies, or organizations that are not scheduled to participate (e.g., adjacent jurisdictions, NGOs and special needs agencies). Additional coordination with key planners would help to identify organizations that should be represented and ensure that training objectives can be more effectively met.
- Experienced senior-level controllers should be carefully selected to support deputies and principals meetings and ensure that high-level exercise objectives are being met. They could prompt or re-direct players towards decisions that had been scripted for exercise purposes. For example, no formal decision was reached to deploy the DEST after the October 16, 2007 senior leadership morning meetings. However, the requirement to deploy the DEST had been previously planned to support numerous other training objectives. An experienced and qualified controller could have stepped in during the meeting and reviewed the situation with the participants to illustrate that the specific decision to deploy the DEST to Oregon would achieve exercise objectives.

Cyber Working Group

Strengths:

- The CWG promoted good coordination and information-sharing among the various federal D/As, as well as private sector participants.
- The CWG created various exercise documents that promoted a realistic approach to cyber play for participants in the FSE.
- The coordination and management of exercise injects with federal D/As was coordinated well.

Areas for Improvement:

- There was inadequate coordination and information-sharing between the CWG and other T4 working groups during the planning phase, especially the IWG. This less-

than-optimal integration hindered the training opportunity and critical information that was disseminated among interagency D/As and other key stakeholders during the FSE.

- There was inadequate intra- and inter-jurisdictional coordination at the federal and state levels of cyber- and communications-related information resulting in unnecessary challenges for integration of injects into the FSE.

External Affairs Working Group

Strengths:

- The early participation of a wide cross-section of federal public affairs representatives enhanced the public affairs level of play throughout the exercise. The designation of ESF-15 leads and interagency participation (e.g., FEMA, FBI, ATF, ACE, USCG) supported an effective networking opportunity for problem solving and planning. Venue visits by federal representatives from DHS OPA, FEMA, USCG, and the FBI enhanced the interaction between federal and regional or venue counterparts and supported the development of public affairs-focused tabletop and conference call exercises in the weeks preceding the FSE. In total, approximately 450 public affairs representatives participated "inside" the FSE.
- National Seminar 2 was completed dedicated to the external affairs function. Public affairs representatives from all three venues, international partners, and most federal agencies participated. Well-received presentations on public health, special populations, law enforcement, ESF-15 and risk communications provided a basis for outstanding information exchange, training, and exercise planning. The seminar was replicated in all three venues to provide regional, state, territorial, and local public affairs representatives with similar opportunities for information exchange and training.
- The VIP/Observer program designed by the EAWG provided an opportunity for over 400 domestic and international observers (representing 17 nations) to witness response efforts, share information, and collaborate on future preparedness and training efforts. By developing daily themes during exercise play, the program was designed so that observers could view different parts of the response effort as events unfolded. Among the elements of the program were information exchange opportunities and tours at incident sites, healthcare facilities, non-governmental agency support locations, and federal, state, territorial, and local EOCs.
- Allowing international VIPs and observers to be fully integrated with the DHS observer program gave them a unique perspective on the exercise and U.S. domestic incident response activities, and should be included in future NLEs.
- The real-world media program involved the coordination of daily media activities in each venue to manage media inquiries about the exercise. The program allowed media to observe various parts of the exercise while maintaining exercise integrity. More than 170 members of the media covered the FSE. Media coverage raised the visibility of the program and DHS. The exercise was covered by all local print and broadcast sources and several national news sources including CNN, MSNBC, the Associated Press, and *The Washington Post*.

Areas for Improvement:

- The wide range of duties and demands on the public affairs teams to support the external aspects of the exercise limits their ability to actually participate "inside" the exercise. During T4, the DHS OPA had responsibility for coordinating public affairs play within the exercise as well as the VIP/Observer program. DHS/FEMA public affairs had responsibility for real-world media coordination. These important demands outside the exercise limited public affairs representatives' ability to respond to the demands of VNN and notional media requirements and to meet the public affairs training objectives presented by the exercise itself.
- There could be an even more effective public messaging campaign during the planning phase of the exercise to explain the NEP and the tiered concept of exercise events, particularly the comprehensive nature of the Tier 1 TOPOFF series. This program could include press releases surrounding the national seminars and planning conferences and other milestone planning events.
- Thirty-seven countries and international organizations were invited to send two representatives each to the observer program, but several countries sent more than two. To effectively manage invitations, the number of countries and international organizations for future NLEs should not exceed this number. The number of reserved spaces for each observer country should he increased to three. Invitations should still request only two, but by reserving a larger number, a hidden margin would be built in to allow countries to send more representatives.

Virtual News Network (VNN)

Strengths:

- The VNN team provided 195 live segments of broadcast during the FSE. These events included coverage of events, press conferences, interviews, and on-scene updates from all three venues and the NCR (across 14 time zones). VNN adds realism to the exercise, holds decision makers accountable, and provides a valuable way to provide timely injects that move the scenario forward.
- VNN footage can be used in the future to support numerous DHS/FEMA tabletop or functional exercise requirements.

Areas for Improvement:

- The VNN Live broadcast hours (12:00 Noon – 8:00 p.m. Eastern Time) were designed to best support all three venues, given funding considerations. The lack of 24-hour coverage did weaken the intensity of play when the broadcast was not on the air.
- There was no posting of fact sheets or press releases on VNN.com throughout the night (Eastern Time).
- The positive contribution to the exercise provided by VNN is demonstrated by the demand among participants and players for an expanded simulated media product (e.g., competing networks, blogs, web pages, etc.).

Venue Observations and Recommendations

The participation of thousands of planners, controllers, evaluators, and exercise participants at the three T4 venues was a critical element of success for the entire training audience. During the AAC, T4 venue representatives were asked to provide summary observations of the exercise design and development process from a venue perspective for the interagency participants. The paragraphs below provide an overview of the most noteworthy discussion points and recommendations for consideration by future venue planners and those teams responsible for support in the venues. More extensive discussion and documentation of venue exercise design issues has been conducted with venue leaders and planners for use in future exercise planning efforts.

Arizona

Discussion Points and Recommendations:

- **Level of Play:** Determine the level of play of participating communities and agencies as early as possible, and recommend that similar size communities support similar levels of play.
- **Benchmarks:** Venue planners should set guidelines and benchmarks for levels of participation to ensure that there is an adequate cost/benefit to support. Even when a community or organization commits to only a short period of participation, there is still considerable effort required to ensure that a training benefit is achieved. Personnel requirements for the agreed-upon level of support should be established early in the plauning process.
- **Mentor Program:** Establish and maintain the TOPOFF mentor program among previous participating venue representatives. The expertise provided by these venue counterparts provides a unique insight into important exercise planning elements and more importantly, supports real-world best practices development.
- **Venue Visit Schedules:** Consideration should be given to modifying the duration of visits by venue support teams to optimize the use of their time. Especially when there are travel requirements within the venue (e.g., Phoeuix to Tucson), consideration should be given to extending visits to best accommodate planning efforts.
- **Workshops:** Schedule a designated training objective workshop for participants early in the planuing process and hold agencies and communities accountable for defiuing their participation level based upon those objectives.
- **Local Federal Representatives:** Institutionalize a program to eugage local and regioual federal representatives from early planniug through ENDEX. The participation of these regionally-based federal resources provides a critical link to their respective NCR-based D/As and facilitates important relationship building that will continue well after exercise completion.

Guam

Discussion Points and Recommendations:

- **Mentor Program:** The vital benefit provided by the mentor program to the TOPOFF planning process was never fully utilized during T4 planning. Learning from a former state or territorial planner about his or her experiences when preparing for and executing TOPOFF would have provided a unique advantage to the planning process and would have enhanced the exercise. DHS should present the mentor program to the venues and clearly define which specific opportunities each venue can take advantage of during the TOPOFF planning process. The mentor program should be open to any former TOPOFF planners, not only those from the most recent TOPOFF exercise.
- **Venue Seminars and Conferences:** Seminars and planning conferences are vital elements of the exercise planning process. During the T4 planning cycle, the venue conferences and seminars were intended to follow the format and topics of the preceding national conference and seminars. Although the format and topics of the national events were closely followed in each of the venues, many federal presentations were not conducted by the most appropriate speakers. Many times, venue planners had to present federal presentations due to the lack of federal representation. This circumstance proved to be a disadvantage to those venue-based planners who had not had the opportunity to attend the national conferences and seminars. In order to provide additional exposure and integration among the venues, consideration should be given to holding the national conferences and seminars at venue locations, similar to the events conducted during the T3 planning process. This will also give the federal presenters and participants the opportunity to visit the venues and meet with the local and regional federal planners.

Oregon

Discussion Points and Recommendations:

- **Level of Play:** During the exercise design and development hot wash, several agencies commented that their level of play depended on other agencies' level of play. The consequence of this "wait-and-see" decision model was that agencies arrived at level of play commitments that were not always aligned with exercise budget decisions that had been made several months (or years) earlier. Additionally, some agencies made level of play decisions that were dependent on the commitment of other non-affiliated agencies. These agencies were not always prepared to meet the demands of the exercise. Since many agencies did not commit to their level of play until very late in the planning process, these interdependencies were not always identified in time. One reason behind some agencies failing to establish a firm level of play was the late development of the national-level federal agency objectives. This caused the regional federal agencies to delay making commitments and thus affected the work of the other local planners. Establishing an agency's exercise level of play, determining their exercise objectives, and developing an exercise budget were all identified as critical planning elements. Each of these elements has a direct effect on the others. All of

these items need to be decided at the earliest point possible during the exercise planning process.

- **Real-World Media and VIP Visits During Exercise Play:** During the exercise, real-world media opportunities were planned that competed for time with the participation of several top official players. During the peak of exercise play, several key players were at the exercise site addressing the media. While this was an effective forum for presenting the exercise to the media, it had some negative consequences for exercise play. (For example, the governor was unable to sign a disaster declaration in timely manner; the PFO was not in Bothell or Salem to meet with players, etc.) Several observers and members of the media toured various exercise EOCs. The visit of one VIP pulled the City of Portland EOC manager away from exercise play and caused the POEM EOC to miss an early critical planning conference call with the state and county EOCs. One VIP visit to the Rapid Screening Point was cited as an example of a visit with a direct negative impact because it distracted the exercise training audience from their focus on exercise objectives. The visit halted the two-hour exercise play for 30 minutes causing the players to fall well short of their throughput goals. While all planners agreed that it was important for local elected officials to take time to deliver positive messages to the public about the exercise, due consideration should be given to the impact that removing the officials from play could have on the exercise. There were various suggestions about how this could be approached in the future to minimize the effect on the exercise. One suggestion was for elected officials to pre-brief the media prior to the STARTEX and then remain totally inside the exercise for the remainder of the event. Another suggestion was that elected officials could appoint a spokesperson to update the media throughout the exercise. A third suggestion was to take all media events to a segregated area near but separate from the exercise site. For example, the media area at the PIR site worked well and provided the media with a good backdrop while not interfering with the exercise. This was in contrast to the Rapid Screening Point and some EOCs where the observers, media, and press events were allowed to mix with the exercise players. This mixing often resulted in significant interference with the exercise. Thorough planning of VIP/Observer and real-world media events is essential to ensure that these important elements of the exercise do not have an undue or unanticipated impact on the actual "inside the exercise" training opportunity.

ANNEX 2: CUSTOMS AND BORDER PATROL AARS

Office of Intelligence and Operations Coordination
Operations Coordination Division

U.S. Customs and Border Protection

AAR for T4 National Emergency Preparedness Exercise

Background: T4 is a congressionally-mandated national emergency preparedness and response exercise conducted every two years, involving every federal agency and a variety of state and local authorities. The T4 scenario presented for this year's exercise involved the terrorist detonation of radiological material (Cesium-137) in three separate venues (Guam; Phoenix, Arizona; and Portland, Oregon). The exercise was heavily weighted on response and recovery issues.

Exercise Scenario: Due to the geographic location of each attack and CBP's current operations, its participation was primarily limited to the Office of Field Operations, Directors of Field Operations (DFO) in San Francisco, California and Tucson, Arizona; and the subordinate Port Directors in the events venues. Each DFO and Port Director assigned specific individuals to actively participate in each exercise activity as a representative of CBP.

Objectives: Headquarters (HQs) and Field

- Use of established common response communication language to ensure that information dissemination is timely, clear, acknowledged, and understood by all receivers.
- Demonstrate the ability to issue, manage, and update emergency notification systems under all conditions to ensure that all employees are accounted for.
- Demonstrate the ability to activate their COOP plans, redeploy officers to alternate locations, account for overtime, assume post-event business resumption protocols, and deploy under ESF-13, if activated.
- Demonstrate the ability to activate the proper channels of communication to include reporting to the Commissioner's Situation Room or as requested by HQ, reporting to DFO, Port Management, and Lead Field Coordinators (LFCs) in respective regions.
- Demonstrate the ability to coordinate with other agencies and appropriate emergency management contacts according to agreements/policies to facilitate information sharing and solve issues while remaining in accordance with NIMS/NRP.

All of the objectives were met to varying degrees and timelines. The following observations and recommendations will address the objectives:

Observations and Recommendations:

Observation: It was noted in all three venues that there was an overabundance of acronyms and technical terms in use that often required definition.

Recommendation: Use common language. The ICS principals clearly identify the requirement to use common language and terms.

Observation: There was a lack of training and connectivity during the initial report of the incident. While local authorities attempted to engage officials of various organizations, there was no uniform notification system available to alert federal, state, and others to the emergency event. CBP largely depended on the media for notification.

Recommendation: It is recommended that (nationally) CBP managers in all facilities develop and foster relationships and a means of communicating first responder alerts or notifications of any event within their area of responsibility. This recommendation could be as simple as creation of basic telephone contact trees to high-tech internet protocol-linked radio frequencies accessible by all authorities within an affected geographical area.

Observation: CBP field participants were not provided with an official notification of changes in the HSAS threat level from Yellow to Orange and Red. The changes were provided via the media and local officials.

Recommendation: For future exercises, as in real-world reporting of emergencies, an HQ SIMCELL should be created to provide top-down communications of official policy changes with the appropriate guidance. Staffing issues curtailed this activity and it was only addressed in a notional sense.

Observation: There appeared to be too many EOC facilities engaged in this exercise. It was not practical to co-locate CBP personnel in every EOC. (State EOC, City EOC, Airport/Seaport EOC, plus the JIC, JOC, and JFO.)

Recommendation: A single centralized facility under a unified command structure would have streamlined the information flow, connectivity process, and communications. CBP should focus on the JOC first and than EOCs with a direct CBP nexus.

Observation: CBP officers were unable to access the JOC. The JOC is operated by the FBI and serves as the location and activity responsible for conducting a criminal investigation of the event. Access to the JOC requires a secret clearance at a minimum, and the security clearance must be on file with the FBI at HQs. The FBI SAC of the JOC arranged for limited access for several CBP officers, out of recognition of the need for information related to the border crossing and international travel of the terrorists.

Recommendation: LFCs should pre-identify JOC/ EOC personnel who possess appropriate clearances.

Final Observation: A recurring theme discerned from all exercise venues identified the fact that CBP appears to operate in a vacuum. Operational activities, capabilities, authorities, and responsibilities are relatively unknown to many within the law enforcement or civil government

communities. Anecdotal reports from various sources throughout the exercise indicated a pleasant surprise and welcome once CBP assets arrived to assist in an activity. Issues as simple as the ability to detect the presence of radiation or assist with traffic control and security measures were resolved once CBP officers became engaged in the emergency.

Recommendation: A greater emphasis on "CBP 101" outreach programs to the public, private sector entities, and community governments.

Office of Intelligence and Operations Coordination
Operations Coordination Division

U.S. Customs and Border Protection

AAR of CBP T4 "Preventative Play" Radiation Protocol Field Testing Exercise

Background:
In January 2007, DHS announced the T4 National Preparedness Exercise. The premise of this exercise is based on terrorist-detonated RDD attacks in three geographically separate locations. The venues were identified as Guam; Portland, Oregon; and Phoenix, Arizona. Of particular interest to CBP is the exercise scenario, which scripted the smuggling of 5,000 curies of the radioactive isotope Cesium-137 across the southwest border from Mexico into the United States by the members of a terrorist organization.

This scripting of a perceived failure by CBP was designed to permit the simulated detonation of the RDDs within CONUS, requiring a subsequent emergency response by various assets of the federal, state, and local authorities.

Within CBP, the Offices of Anti-Terrorism, Internal Affairs, Human Resources, and Border Patrol coordinated to develop a "no notice" field activity, where designated role players attempted to pass through a U.S. Border Patrol (BP) checkpoint outside of Nogales, Arizona with a small quantity of Cesium-137.

Primary Goal of Testing:
The primary goal of this exercise was to test CBP's radiation detection policy and procedures, as well as to assess the ability and the willingness of the BP agents involved to detect, detain, and process a radiation-based terrorist threat. CBP leadership decided to leverage the T4 scenario and the supporting simulated intelligence to conduct an internal CBP exercise, which focused on testing CBP's ability to respond to specific border-threat-related intelligence and to assess CBP radiation detection policies and procedures. Ultimately, DHS leadership agreed to include CBP's internal exercise as an annex to the actual T4 exercise.

Field Test Development

Radioactive Field Test Material: 0.075 Mil-Rems of Cesium-137

Training and Coordination:
The participating role players received formal radiation safety training and certification from the Office of Occupational Safety and Health. In addition, a specific use permit was issued by DoT for movement and use of the radioactive material based on the Nuclear Regulatory Commission (NRC) license maintained by CBP Radiation Safety Officer (b)(6) The Office of Internal Affairs (b)(6) supported the exercise by helping to coordinate the transport of the material via FEDEX (Dangerous Goods) and provide safety equipment for secure handling of the material.

Concealment:
The Cesium-137 was contained inside a standard metal shipping "pig" case with the top removed and secured inside a cardboard box in a side pocket of a canvas backpack. The "pig" was positioned in the backpack with the unshielded beam facing the driver's side door in the middle row of a Dodge mini-van. All other sides of the "pig" were provided with a lead apron covering to effectively shield the driver and other passengers participating in the exercise. A personal radiation detector (PRD) screening of the vehicle's driver's side exterior indicated a numerical reading fluctuating between a 6 and 8.

Exercise Role Players:
(b)(6)
(b)(6)
(b)(6)

Role Players Script:
The role playing team posed as employees of "Care International," which is a Northern Virginia-based charitable organization with suspected ties to terrorist money laundering activities. The role players claimed that they were returning from a short vacation in Puerto Penasco (Rocky Point), Mexico, and were en-route to Tucson International Airport. Prior to the exercise, role players divested themselves of any and all identification and material links to government employment. The role players carried only some cash and local Virginia/ Maryland driver's licenses.

Actual Field Test Results:
The field-testing exercise commenced at 1115 hrs (PDT), with the role players driving north approximately 12 miles out of Nogales on Arizona Highway 82, where a BP tactical checkpoint was encountered. The role-playing team was stopped by a BP agent who, while attempting to determine the citizenship of the team, recognized the audible alert and visual indicators of his PRD. Upon receiving this audible alert, the BP agent escorted the team to a secondary inspection area where additional BP agents were located.

BP agents interviewed the role players briefly while in the vehicle, discussing the citizenship and travel of the team. The role players were requested to exit the vehicle and asked to provide identification while the questioning continued. The role players observed the BP agents communicate with each other and use additional PRD(s) and a Radioactive Isotope Identification Device (RIID) along the exterior of the vehicle.

The role players were questioned as a group by the BP agents, who asked why radiation was detected and if they had any knowledge that radioactive material was in their possession. The role players denied having knowledge of any radioactive material and agreed to the BP agent's request to search the vehicle. However, they declined a request to search personal baggage contained in the vehicle.

During the questioning, the role players were individually searched for weapons to ensure the safety of the BP agents. For additional safety considerations, the role players were required to wear radiation dosimeter badges at about chest-level for later testing and evaluation. BP agents did discover similar dosimeter badges on each role player during the search for weapons. The dosimeters found on the role players by the BP agents were not marked and there was no indication as to their purpose or function. Each role player individually declined to comment as to the purpose of the dosimeters when asked about them by the BP agents.

The role players were then separated and escorted to individual BP vehicles for secure detention purposes. At this point, the BP agents began:

- Contacting the Nogales Station to describe and identify the dosimeters
- Researching the role players' identification for criminal history
- Researching the crossing data on the vehicle
- Researching the employer organization "Care International"

The "hot" baggage was identified and isolated. The RIID identified the material as Cesium-137. The BP checkpoint Field Operations Supervisor (FOS) initiated contact with the Nogales Station and Laboratory Scientific Services (LSS) in preparation to transmit the isotope spectral signature to LSS for analysis (LSS management had been previously advised of the field testing team's covert activities and was awaiting the call).

Exercise Conclusion:
The field testing team leader (b)(6) identified himself and members of the role playing team to the senior agent on duty and requested that the he contact the exercise "trusted agent", Assistant Patrol Agent in-Charge (APAIC) Dolph Hunt from the Nogales BP Station. APAIC Hunt responded shortly afterwards and member identification was validated and the exercise was concluded. A de-briefing and hot wash was then conducted with the entire checkpoint group.

Observations and Recommendations:
As stated previously, the primary purpose of this exercise was to highlight and demonstrate the capabilities of the BP to detect, detain, and process a radiation-based terrorist threat as linked to the T4 National Preparedness Exercise scenario. While deemed a successful interdiction of the terrorist event, several "gaps" were identified during the hot wash with tbe BP agents:

1. **Education:** Although agents effectively managed this field test, they were unsure of specific legal authorities and radiation properties. Basic courses should be reviewed and edited to ensure that they address radiation sources, tbe identification of types of radiation, specific hazards, and their legitimate uses. agents should be aware of the legal requirements to possess and transport radioactive material (i.e., licenses, permits, etc.) and also possess the capability to validate the licenses or permits. In addition, knowledge of the civil or criminal penalties for illegal possession of radioactive materials as well as an understanding of when other authorities are required to be notified should also be addressed.

- Office of Intelligence and Operation Coordination (OIOC)/ IMOC will coordinate with the Office of Training and Development to discuss these issues.

2. **Technical connectivity:** Although this specific checkpoint was not considered permanent, all checkpoints should have the technical means necessary to transmit the data required by LSS without having to secure and move vehicles and suspects to a station.

    - OIOC/ IMOC will discuss the technical issues and coordinate with the Office of Information Technology and Office of Border Patrol regarding this issue.

This page is intentionally blank.

TOPOFF 4 Evaluator Handbook

October 2007

Homeland Security

Dear TOPOFF 4 Evaluator,

Congratulations and thank you for your participation in the Top Officials 4 (T4) Exercise. Your efforts are greatly appreciated and very important to our collective goal of securing the homeland. This document provides important information regarding individual requirements and directions, pre-assembly, and preliminary logistics information. Please take time to thoroughly read all of the contents of this document.

It is vital to exercise play that you arrive at your designated assembly area on time with the essential materials. Please allow sufficient time to compensate for traffic, inclement weather, and processing through exercise security and check-in procedures.

Safety is paramount throughout exercise preparation and conduct. You will be provided one or more safety briefings to ensure that you are aware of hazards or safety concerns at your venue site. Your individual assistance in recognizing and identifying emergent hazards is equally important. As a T4 Exercise Evaluator, you are also a key member of its safety team. Please help us to keep T4 accident-free.

Again, we thank you very much for participating in the T4 exercise. We look forward to your important contribution to a hugely successful training event for our key players and Top Officials.

Evaluator Checklist

The following evaluation checklist describes the evaluator's responsibilities before, during, and after the exercise.

Before the exercise:

- ❑ Review the EXPLAN, scenario, MSEL, EVALPLAN, and COSIN, with special emphasis on the objectives, capabilities, and key issues identified to facilitate data collection.
- ❑ Complete evaluator training requirements.
- ❑ Familiarize yourself with the missions, plans, policies, procedures, and processes applicable to your assigned location.
- ❑ Identify and review the forms you must fill out (see table at the end of this checklist).
- ❑ Attend the Controller/Evaluator (C/E) briefing at your assigned location.

Upon arrival at start of shift:

- ❑ Check in with the Lead Controller at your site.
- ❑ Receive a turnover (shift change) brief from the outgoing evaluator.

During the exercise:

- ❑ Observe the exercise and record your observations in the Evaluator Log as described in Part 2 of this handbook.
- ❑ Interview participants to clarify events and gain insight into decisions and actions.
- ❑ Collect supplementary data, including the following:
  - Situation Reports, Spot Reports, briefings
  - Logs (e.g., communications log, daily log)
  - Requests for Information (RFI) and RFI logs
  - Press releases, fact sheets, FAQ documents
  - Technical data products (e.g., GIS products, maps, plume model results)
  - Incident Action Plans and other planning documents.

  Be sure to note the date and time along with your location
- ❑ Ensure players copy emails to t4data@cna.org [during the FSE only].
- ❑ Collect participant feedback forms for those personnel whose extent of play is over.
- ❑ During downtime, after your shift, or after ENDEX:
  - Complete the applicable EEGs (see table below)
  - Complete the Common Operational Picture (COP) Form.

At the end of shift:

- ❑ Conduct a turn-over brief with your replacement.

- ❑ Contact the lead controller or evaluator at your site, Master Control Cell (MCC), or Venue Control Cell (VCC) if your replacement does not arrive.

After FSE ENDEX:

- ❑ Attend and document the site/player hot wash.
- ❑ Participate in the C/E debrief in your venue.
- ❑ Collect any remaining participant feedback forms that are submitted ~~in~~ hardcopy.

Within 72 hours after FSE ENDEX:

- ❑ Transcribe all forms into electronic versions (observation log, EE~~Gs~~, and supplementary forms).
- ❑ Email your forms to t4data@cna.org (please enter "evaluator forms" ~~in the~~ subject header). Turn in hard copies to the venue Evaluation Lead or mail to:

(b)(6)

The CNA Corporation
4825 Mark Center Drive
Alexandria, VA 22311-1850

Be sure to note the date and time along with your location on all materials.

The table below shows what forms are required for each type of location.

Venue Law Enforcement Nodes	Yes	All: • Information Sharing and Dissemination • Recognition of Indicators and Warnings • Law Enforcement Investigation and Ops	Yes
Venue Fusion Centers	Yes	All: • Information Sharing and Dissemination • Intelligence Analysis and Production • Recognition of Indicators and Warnings	Yes
Venue ICP/UCPs	Yes	All: • On Site Incident Management	Yes
Emergency Operations Center (local, state, territorial, federal, or multi-agency)	Yes	All: • Emergency Ops Center Management If EOC engages in intelligence sharing: • Intel / Info Sharing and Dissemination If EOC includes a public affairs component: • Emergency Public Info and Warning If EOC includes a recovery component: • Economic and Community Recovery	Yes
Joint Information Centers (JICs) or other public affairs entities	Yes	All: • Emergency Public Info and Warning	Yes
Other (e.g., Top Official or agency offices)	Yes	N/A	N/A

TABLE OF CONTENTS

LIST OF TABLES

Part 1

I. General Information

A. Document Purpose and Organization

The TOPOFF 4 (T4) Evaluator Handbook provides the essential information and materials that evaluators need to carry out their roles and responsibilities. The T4 Evaluator Handbook is a standalone document that provides the instructions necessary for evaluators to collect the data necessary to support the evaluation methodology. The handbook provides background information on T4 – including the Prevention Component and the Full Scale Exercise (FSE), data collection and reporting procedures, and guidance and forms necessary to make relevant exercise observations. Further details on the evaluation methodology and TOPOFF 4 can be found in the Evaluation Plan (EVALPLAN) and T4 FSE Exercise Plan (EXPLAN).

The T4 Evaluator Handbook is organized in two sections. Part 1 includes general information, evaluator roles and responsibilities, and safety and reporting procedures. Part 2 includes the data collection instructions and forms that evaluators are required to complete.

B. Selected Definitions

Players. Players are department and agency (D/A) personnel who actively respond to emergencies. During T4, they will carry out their normal roles and functions in response to scenario events.

Controllers. Controllers plan and manage exercise conduct, direct and monitor the pace and intensity of exercise play, and ensure safety and security. They monitor exercise events and provide information and instructions to players.

Evaluators. Evaluators record observations of player actions and manage data collection at each exercise venue. Evaluators are familiar with the roles and responsibilities of the players they observe, and the data they collect will support the post-exercise reconstruction and analysis. Evaluators include members of the exercise support team and personnel from participating departments and agencies.

Simulators. Simulators are control staff personnel who simulate player actions of all non-participating agencies and individuals.

Master Scenario Events List (MSEL). The MSEL is a detailed listing of scheduled events and anticipated player actions that will take place during the exercise.

National Master Scenario Events List (NxMSEL). NxMSEL is an automated system for MSEL management. During exercise execution, NxMSEL provides tools for tracking progress and for reviewing, modifying, and releasing injects to the training audience.

Virtual News Network (VNN). VNN is the mock news media for the T4 FSE. VNN Live is a satellite feed that will broadcast breaking news and interviews as the T4 FSE scenario unfolds. VNN.com is an online news source that will provide the media's perspective on events. Players will receive public media injects through VNN as would be expected during an actual terrorist event.

Extranet Secure Portal (ESP). Available online, ESP is a secure online collaboration tool that consists of an instant messenger, document library, and chat room. Controllers and evaluators will use the ESP chat room to coordinate real-time information on events and activities across exercise venues and sites.

Homeland Security Information System (HSIN). HSIN is a computer-based counterterrorism communications system connecting all 50 states, five territories, Washington, DC, and 50 major urban areas. HSIN allows all states and major urban areas to collect and disseminate information between federal, state, and local agencies involved in combating terrorism. Evaluators working in the Master Control Cell (MCC) or Venue Control Cells (VCCs) will have access to HSIN to monitor exercise play.

Common Operational Picture (COP). The COP is an application available through HSIN that allows critical decision makers to define and prioritize the information required for their operational activities and then to display that data in ways that facilitate their mission.

C. T4 FSE Venues

The T4 FSE will take place in the following venues:

- **Interagency:** The federal departments and agencies (e.g., Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), Department of Energy (DoE)) will participate from their national emergency operations centers (EOCs). Most are located in the Washington, DC area.
- **State Venues:** Local, territorial, state, and federal departments and agencies will participate from emergency operations centers and field sites located in Arizona, Guam, and Oregon.
- **International:** Australia, Canada, and the United Kingdom will also participate from both U.S. and overseas locations.

For more information on exercise play at each venue, refer to the individual venue EXPLANs, which complement the overall EXPLAN.

II. Evaluation Overview

The TOPOFF 4 evaluation methodology is based on the Homeland Security Exercise and Evaluation Program (HSEEP) doctrine and designed to support the national goals for T4. HSEEP provides common evaluation standards and is supported by tools to assist organizations in conducting their own evaluations.

The overall T4 evaluation focuses on high-level (e.g., top official, interagency) coordination, support plans, policies, and procedures. The evaluation does not focus on individuals or organizations, but rather on how departments and agencies interact to share information and coordinate activities. Organizations are encouraged to conduct their own internal evaluations based on their specific missions, objectives, tasks, and procedures.

The evaluation of T4 will identify both strengths and areas for improvement, and is designed to support the improvement planning process that will follow the exercise. In the improvement planning process, recommendations from the evaluation After-Action Report (AAR) are used to develop a formal plan that lays out concrete steps for implementing corrective action and assigns responsibility for each step.

A. Capabilities Being Evaluated

Table 1 shows the target capabilities that will be the focus of the evaluation.

Table 1: Target Capabilities

Prevention	Information Gathering and Recognition	Law Enforcement nodes, Intel sharing nodes
	Intelligence Analysis and Production	Law Enforcement nodes, Intel sharing nodes
	Intelligence/Information Sharing and Dissemination	EOCs, Law Enforcement nodes, Intel sharing nodes
	Law Enforcement Investigation and Operations	Law Enforcement nodes
FSE	Intelligence/Information Sharing and Dissemination	EOCs, Law Enforcement nodes, Intel sharing nodes
	On Site Incident Management	Venue ICP/UCPs
	Emergency Operations Center Management	EOCs
	Emergency Public Information and Warning	JICs
	Economic and Community Recovery	EOCs

B. The T4 FSE Evaluation Process

The T4 evaluation consists of the following three-step process:

1. **Observation and data collection**. Evaluators make observations and collect data at their assigned venues. Evaluators are responsible for recording their observations in an Evaluator Log, collecting supporting data, and providing an initial analysis of the capabilities using Exercise Evaluation Guides (EEGs).
2. **Reconstruction**. The evaluation team will use the data collected by the evaluators to build a fact-based, de-conflicted account of what happened during the exercise and why. This ensures that issues and recommendations are supported by the data.
3. **Analysis**. The evaluation team will use the reconstruction to determine what happened during the exercise and why, identify issues that arose during the exercise and their root causes, and document these findings in the After-Action Report (AAR). This analysis will support the development of actionable recommendations.

III. Communications, Safety and Reporting Procedures

The EXPLAN contains detailed instructions for control staff, including the control organization and safety procedures.

A. Safety

Safety during the T4 FSE is paramount. All exercise players, controllers, and evaluators share the responsibility of observing safety procedures and halting play if a safety problem exists or if an actual accident or emergency occurs.

In the case of an actual emergency, render first aid, call emergency medical services (911), and maintain control of the scene. The impacted venue or site controller will call a "STOP PLAY" and notify the T4 MCC or VCC of the location, situation, and on-scene requirements. Play resumption is a coordinated decision between the T4 FSE MCC/VCC, the on-scene controller, and the respective D/A safety and security personnel. Greater detail on the safety protocols for T4 can be found in the EXPLAN, Annex G: Safety and Security.

B. Communicating with the MCC and VCCs

The Control Staff Instruction (COSIN), Annex A of the EXPLAN, contains the unclassified phone numbers for the control cells. Although unclassified, the COSIN must be properly maintained and used by exercise control staff.

Evaluator shifts are scheduled to align with the level of play at each location. In cases where sites are operating 24/7, evaluators will be assigned to 13-hour shifts that include a 30-minute turnover period at the start and end of each shift. Evaluators at field sites should check in with the lead controller or evaluator at their assigned location at the start of each shift. Outgoing evaluators should brief incoming evaluators on key player actions that occurred during the shift, the status of key events scheduled in the MSEL, and any issues observed.

During shifts, evaluators should notify the MCC (for interagency locations) or VCC (for venue locations) evaluator of the following:

- Any unexpected player actions that might impact play at other locations
- If the incoming evaluator has not reported for his/her shift.

C. Maintaining the Exercise Log on the Extranet Secure Portal (ESP)

Controller and evaluator teams located in operations centers and other indoor sites during the FSE should have access to at least one workstation with Internet connectivity. This will allow them access to the following collaboration tools available through ESP:

- A library of exercise documentation, including the EXPLAN and MSEL
- Secure messaging
- Situational Awareness Log (chat room).

The purpose of the Situational Awareness Log is to record key player actions for the exercise reconstruction and provide situational awareness of player activities throughout all venues. Controllers and evaluators should report key player actions at their locations, including decisions, events, and the receipt of information such as:

- Changes in security levels (e.g., Homeland Security Advisory System)
- Emergency declarations and waivers
- Requests for support
- Resource allocations and deployments
- Requests for Information (RFIs)
- Arrival of resources and assets

- Status of emergency response activities
- Key issues.

The controller and evaluator team at each site should designate one of its members to monitor the Exercise Log and make entries for that location. Entries to the Exercise Log must include:

- **Who:** Who made the decision? Who took the action? Who received the information?
- **What:** What was the decision? What was the action? What was the information?
- **When:** When was the decision reported? When was the information received?
- **How**: How is the action being carried out? How was the information sent?

The log will automatically record the time of the entry and the site reporting it. Examples of properly entered log entries are shown in Table 2.

Table 2: Sample Situational Awareness Log Entries

IA NOC Rep 1 (10/16 9:25AM) CAT is fully activated
GU EOC Rep 2 (10/16 9:35AM) Announcement: GU Governor has requested a Disaster Declaration
OR EOC Rep 1 (10/16 9:36AM) VNN reports an explosion. EOC personnel working to confirm report.
IA NRCC Rep 3 (10/16 9:40 AM) NRCC Director requests Ops develop recommendations for pushing resources to GU.

D. Supporting the Hot Wash and C/E Debrief

Evaluators should attend and document the hot wash conducted at their assigned location. If requested, evaluators can assist in facilitating this hot wash. Guidelines for facilitation are included in the EVALPLAN.

In addition, the C/E team at each site should nominate at least one staff member to attend the C/E de-brief. A briefing template will be provided to the site teams for use assembling out-briefings on the key issues identified at their locations.

E. Administrative Information

What to wear: Evaluators assigned to outdoor environments, such as the incident site, should dress appropriately for the weather in comfortable clothing. Field evaluators should note that cool light-colored clothing is highly recommended. Because there will be rubble, dirt, and uneven footing, safety shoes or rugged leather footwear is required for evaluators assigned to the incident site.

Evaluators working indoors should dress comfortably according to ~~the standards of their venue~~. Those working in sites with the press or with government officials should make a point to dress in business or business casual attire for all day shifts.

Meals and water: Please refer to the meal plan for your assigned venue for information on the availability of food and water at your location. Evaluators should also bring their own water and snacks.

Part 2

I. Introduction

This section of the handbook contains the data collection forms that evaluators are required to use and instructions on how to use them. There are three types of forms that evaluators will use:

1. The Evaluator Log
2. Exercise Evaluation Guides
3. Common Operational Picture (COP) Form

Electronic copies of all the forms will be posted to the administrative page of VNN.com (available on llis.gov) and to the ESP library. They will also be made available by email. The Evaluator Log is also provided in bard copy at the end of this handbook.

II. Instructions and Examples

A. Evaluator Log

The Evaluator Log is the primary data collection form and is critical to building an accurate exercise reconstruction. The evaluator log is used to document key events for the exercise reconstruction.

Evaluators should record observations of key injects, events, and player actions. Record the time that an event occurred in the box labeled "Time" and check the "Inject" column if you are aware that you are observing an inject. In the description box, provide details on the event. Sentences should be clear and use the active tense whenever possible. Please use a "subject + verb + object + qualifications" structure in the description for clarity where possible. (Example: Incident commander [subject] contacted [verb] State EOC [object] to report explosion using cell phone [qualification].) An example is shown in table 3.

The Evaluator Log is provided in both hard copy and electronic formats. Evaluators may use whichever format they prefer during the exercise. Evaluators are required to transcribe their log into the electronic version after the exercise and then submit it according to the instructions provided on the Evaluator Checklist.

Table 3: Sample Evaluator Log

Time	Description	INJ
0800	EOC control injects to EOC that an explosion has occurred at a local shopping center at 0755. Control passes INJ to EOC operations director.	X
0803	EOC operations director notifies the emergency management director (EMD). EMD is departing for EOC, immediately. Expected time of arrival is 0825.	
0810	EOC fire representative receives a call that fire units have arrived at the scene and the northeast corner of shopping center is ablaze. Additional fire units are requested. EOC fire rep notifies the EOC operations director	

Time	Description	INJ
0815	Dispatch reports that EMS is on scene. Many walking injured exiting the shopping center	
0820	VNN com video shows shopping center on fire and people exiting through the doors. Some injured are being carried out. Reporter interviews witnesses who said they heard a large explosion at the other end of the shopping center and then were knocked down by a blast.	
0830	EMD arrives at the EOC. EOC operations director briefs EMS on current status of incident: • Explosion occurred at shopping center located at Main St. and 10th Ave. • After talking to witnesses, police on the scene suspect it was an improvised explosive device (IED) that went off near the food court	
---	• Current casualty figures are 10 dead and 100 injured • Fire are on scene and working to extinguish the fire • The fire chief has requested additional help from neighboring counties • EMS are caring for the injured but have insufficient ambulances to transport the injured	
0850	EMD telephones St. Mary's Hospital to stand by for mass casualties. Should expect 100 casualties based on estimates provided by EOC operations director in status brief.	

B. Exercise Evaluation Guides

Exercise Evaluation Guides (EEGs) assist exercise evaluators by providing them with consistent standards and guidelines for observation, data collection, and analysis. The EEGs were developed for T4 using the Target Capabilities List and are linked to each capability's activities, tasks, and performance measures. Refer to the checklist at the beginning of this document to find the EEGs that are used at each type of exercise location.

Evaluators should review the EEGs that apply to their assigned location prior to the exercise. During downtime or after the exercise, evaluators should complete the EEGs using the information documented in their Evaluator Log and then submit them according to the instructions provided on the Evaluator Checklist. The completed EEGs will be used by the evaluation team for the development of the Quick Look and After-Action Reports. Example excerpts from an EEG are shown on the next page.

TOPOFF 4 (T4) Full Scale Exercise

Emergency Operations Center Management

Exercise Evaluation Guide

Capability Description:

Emergency Operations Center (EOC) management is the capability to provide multi-agency coordination (MAC) for incident management by activating and operating an EOC for a pre-planned or no-notice event. EOC management includes: EOC activation, notification, staffing, and deactivation; management, direction, control, and coordination of response and recovery activities; coordination of efforts among neighboring governments at each level and among local, regional, State and Federal EOCs; coordination of public information and warning; and maintenance of the information and communication necessary for coordinating response and recovery activities. Similar entities may include the National (or Regional) Response Coordination Center (NRCC or RRCC), Joint Field Offices (JFO), National Operating Center (NOC), Joint Operations Center (JOC), Multi-agency Coordination Center (MACC), Initial Operating Facility (IOF), etc.

Capability Outcome:

The event is effectively managed through multi-agency coordination for a pre-planned or no-notice event.

Jurisdiction or Organization: DHS	**Name of Exercise: TOPOFF 4 Full Scale Exercise**
Location: National Operations Center (NOC) / Crisis Action Team (CAT)	**Date: October 22, 2007**
Evaluator: (b)(6)	**Evaluator Contact Info:** (b)(6) **@cna.org /** (b)(6)
Note: This guide is based on the HSEEP Exercise Evaluation Guides (EEGs), but is modified to support the overall T4 evaluation. Please fill out the observation keys and include additional comments and clarifications as necessary. Note any deviations from policies, plans, and procedures.	

Activity 1: Gather and Provide Information

Activity Description: Upon establishing EOC/MACC/IOF operations, gather, organize, and document incident situation and resource information from all sources to maintain situational awareness within the EOC/MACC/IOF, and horizontally and vertically within the National Incident Management System (NIMS).

Tasks Observed (check those that were observed and provide the date and time of observation, if applicable)

Note: Asterisks (*) denote Performance Measures and Performance Indicators associated with a task. Please record the observed indicator for each measure.

Tasks / Observation Keys	***Comments***
1.1 Coordinate emergency management efforts among local, county, regional, State, and Federal EOC/MACC/IOF. – *Identify mechanisms used at the EOC/MACC/IOF to communicate and receive/disseminate information from/to other State/local EOCs/MACCs/IOFs.* ☐ Phone calls ☒ Emails ☒ Receipt of Spot Reports and Situation Reports	Describe communication and coordination processes at the EOC/MACC/IOF. What entities did it communicate and coordinate with at the State and Federal levels? Was there a set schedule of briefings and updates established? The CAT received information through several email accounts, HSIN, and the COP portal. The IMOs reviewed incoming information and forwarded / posted it per the CAT SOP. This information came primarily from Federal agencies and entities such as LNOs, the NRCC, and the JFO. The NOC did not communicate directly with State/local entities.

Evaluator Observations

Record your key observations using the structure provided below. Please try to provide a minimum of three observations for each section. There is no maximum (three templates are provided for each section; reproduce these as necessary for additional observations). Use these sections to discuss strengths and any areas requiring improvement. Please provide as much detail as possible, including references to specific Activities and/or Tasks. Document your observations with reference to plans, procedures, exercise logs, and other resources. Describe and analyze what you observed and, if applicable, make specific recommendations. Please be thorough, clear, and comprehensive, as these sections will feed directly into the drafting of the After-Action Report (AAR). Complete electronically if possible, or on separate pages if necessary.

Strengths

1. Title: CAT had defined the tasks it was responsible for and developed SOPs for carrying out these tasks

Related Activity:

Record for Lesson Learned? (Check the box that applies) Yes [X] No [ ]

a) Analysis: (Include a **discussion** of what happened. When? Where? How? Who was involved? Also describe the **root cause** of the observation, including contributing factors and what led to the strength. Finally, if applicable, describe the positive **consequences** of the actions observed.)

Based on lessons learned from Hurricane Katrina, other events, and previous exercises, the CAT had defined the mission essential tasks (METs) for its mission as described in the NRP. The CAT SOP detailed the procedures for carrying out these tasks and the CAT staff attended training on these procedures prior to the exercise. For many CAT members, this was the first event or exercise they participated in and they arrived prepared to carry out their roles and responsibilities.

b) Recommendation: (Even though you have identified this issue as a strength, please identify any recommendations you may have for enhancing performance further, or for how this strength may be institutionalized or shared with others.)

The CAT SOP could serve as a model for other agency emergency response teams to develop their own METs and SOPs for carrying out those tasks.

Areas for Improvement

1. Title: Information management

Related Activity:

Record for Lesson Learned? (Check the box that applies) Yes [ ] No [X]

a) Analysis: (Include a **discussion** of what happened. When? Where? How? Who was involved? Also describe the **root cause** of the observation, including contributing factors and what led to the problem. Finally, if applicable, describe the negative **consequences** of the actions observed.)

CAT IMOs could not keep up with the volume of emails that came into the various inboxes that they monitored. Many emails were duplicates that came from multiple sources and some of them contained information that was duplicated on HSIN and the COP. The volume of email was too large for the staff and at times some of it was not reviewed and processed per the SOP. This issue is larger than CAT internal SOPs and is related on the heavy use of email, as opposed to sites like HSIN and the COP for interagency information sharing.

b) Recommendation: (Write a recommendation to address the root cause. Relate your recommendations to needed changes in plans, procedures, equipment, training, mutual aid support, management and leadership support.)

Establish an interagency working group to address information sharing and develop business rules for sharing information that minimize the use of email where possible.

C. Common Operational Picture (COP) Form

One of the goals of the evaluation is to assess whether departments, agencies, and organizations achieved a shared situational awareness during the FSE component of the exercise. Through HSIN, DHS has a COP tool designed to promote shared situational awareness. The purpose of the COP Form is to support this assessment.

The COP Form lists the essential elements of information as currently defined in the COP tool. Evaluators should record the value of each of these elements (if known) at the following times:

Table 5: COP Reporting Times

	Time (EDT)	Arizona	Oregon	Guam
Oct. 15	1900		1600	0900, Oct. 16
Oct. 16	0100		2200, Oct. 15	1500
	0700		0400	2100
	1100		0800	0100, Oct. 17
	1500	1200	1200	0500, Oct. 17
	1900	1600	1600	0900, Oct. 17
Oct. 17	0100	2200, Oct. 16	2200, Oct. 16	1500
	0700	0400	0400	2100
	1300	1000	1000	0300, Oct. 18
	1900	1600	1600	0900, Oct. 18
Oct. 18	0700	0400	0400	2100
	1900	1600	1600	0900, Oct. 19
Oct. 19	0700	0400	0400	2100
	1900		1600	0900, Oct. 20

Evaluators should record the value of each essential element known to the data collection location at the reporting times indicated. If exercise play at your location starts later than 0700, record the essential elements at the start of play (note the time on the form) and then continue with the other reporting times. Likewise, if exercise play at your location ends play prior to 1900, record the essential elements at the end of play (and make a note of the time). If no information is known about an essential element, enter "N/A". In the source row, note the source of the information (e.g., SITREP, conference call, briefing, press release, observation log, etc.). Provide hard copies or electronic copies of all source documents for reference. The next page shows an example.

Table 6: Sample COP Form

Essential Element	June 19 1900	June 20 1900	June 21 0700	June 21 1100	June 21 1500	June 21 1900	June 22 0700
Incident Type	COGCON Level 3 set	Order to go to COGCON 2 given	Order to go to COGCON 1 given	Operating from COOP site as of 0900	Explosion	IND explosion	IND explosion
Source							
Incident Location	N/A	N/A	N/A	N/A	Landport	Landport	Landport
Source							
Time of Incident	N/A	N/A	N/A	N/A	12:00 p.m. June 21	12:00 p.m. June 21	12:00 p.m. June 21
Source							
Threat/causal factors	N/A	N/A	N/A	N/A	Unknown	Terrorism suspected	Terrorism confirmed
Source							

Name:_____ Date:_____

Email / Phone:_____ Location:_____

Evaluator Log

Time	Description	INJ

Name:_____ Date:_____ Name

Email / Phone:_____ Location:_____

Time	Description	INJ

Name:_____ Date:_____ Natu

Email / Phone:_____ Location:_____

Time	Description	INJ

Name:_____ Date:_____

Email / Phone:_____ Location:_____

Time	Description	INJ

Name:_____ Date:_____

Email / Phone:_____ Location:_____

Time	Description	INJ

Name:_____ Date:_____ Name

Email / Phone:_____ Location:_____

Time	Description	INJ

Name:_____ Date:_____ Nam

Email / Phone:_____ Location:_____

Time	Description	INJ

Name:_____ Date:_____

Email / Phone:_____ Location:_____

Time	Description	INJ

Name:_____ Date:_____

Email / Phone:_____ Location:_____

Time	Description	INJ

Name:_____ Date:_____

Email / Phone:_____ Location:_____

Time	Description	INJ

Name:_____ Date:_____

Email / Phone:_____ Location:_____

Time	Description	INJ

Name:_____ Date:_____

Email / Phone:_____ Location:_____

Time	Description	INJ

Name:_____ Date:_____

Email / Phone:_____ Location:_____

Time	Description	INJ

Name:_____ Date:_____ Name

Email / Phone:_____ Location:_____

Time	Description	INJ