Description of document:	Scoping Paper for a Comprehensive Review of the Nuclear Regulatory Commission's (NRC) Safeguards and Security Programs in Light of the Terrorist Attacks on September 11, 2001
Request date:	2014
Released date:	05-January-2015
Posted date:	21-September-2015
Source of document:	US Nuclear Regulatory Commission Mail Stop T-5 F09 Washington, DC 20555-0001 Fax: 301-415-5130 E-mail:FOIA.resource@nrc.gov

NRC FORM 464 Part I (10-2014) | U.S. NUCLEAR REGULATORY COMMISSION

RESPONSE TO FREEDOM OF INFORMATION ACT (FOIA) / PRIVACY ACT (PA) REQUEST

FOIA/PA	RESPONSE NUMBER
2013-0068	4

RESPONSE TYPE ☐ FINAL ☑ PARTIAL

REQUESTER

DATE JAN 05, 2015

PART I. -- INFORMATION RELEASED

☐ No additional agency records subject to the request have been located.

☐ Requested records are available through another public distribution program. See Comments section.

☐ GROUP ____ Agency records subject to the request that are identified in the specified group are already available in public ADAMS or on microfiche in the NRC Public Document Room.

☐ GROUP ____ Agency records subject to the request that are contained in the specified group are being made available in public ADAMS.

☑ GROUP ____ Agency records subject to the request are enclosed.

☐ Records subject to the request that contain information originated by or of interest to another Federal agency have been referred to that agency (see comments section) for a disclosure determination and direct response to you.

☑ We are continuing to process your request.

☐ See Comments.

PART I.A -- FEES

AMOUNT*
$ ____
* See comments for details

☐ You will be billed by NRC for the amount listed.

☐ You will receive a refund for the amount listed.

☐ None. Minimum fee threshold not met.

☐ Fees waived.

PART I.B -- INFORMATION NOT LOCATED OR WITHHELD FROM DISCLOSURE

☐ No agency records subject to the request have been located. For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

☑ Certain information in the requested records is being withheld from disclosure pursuant to the exemptions described in and for the reasons stated in Part II.

☑ This determination may be appealed within 30 days by writing to the FOIA/PA Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001. Clearly state on the envelope and in the letter that it is a "FOIA/PA Appeal."

PART I.C COMMENTS (Use attached Comments continuation page if required)

1. Group G: Secy-01-0215: "Scoping Paper for Comprehensive Review of the NRC's Safeguards and Security Programs in Light of the Terrorist Attacks on September 11, 2001"

2. This is Partial Response #4.

SIGNATURE - FREEDOM OF INFORMATION ACT AND PRIVACY ACT OFFICER

Roger Andoh

NRC FORM 464 Part II (08-2013)

U.S. NUCLEAR REGULATORY COMMISSION

RESPONSE TO FREEDOM OF INFORMATION ACT (FOIA) / PRIVACY ACT (PA) REQUEST

FOIA/PA 2013-0068

DATE JAN 05, 2015

PART II.A -- APPLICABLE EXEMPTIONS

GROUP G

Records subject to the request that are contained in the specified group are being withheld in their entirety or in part under the Exemption No.(s) of the PA and/or the FOIA as indicated below (5 U.S.C. 552a and/or 5 U.S.C. 552(b)).

- [x] Exemption 1: The withheld information is properly classified pursuant to Executive Order 12958.
- [ ] Exemption 2: The withheld information relates solely to the internal personnel rules and practices of NRC.
- [ ] Exemption 3: The withheld information is specifically exempted from public disclosure by statute indicated.
  - [ ] Sections 141-145 of the Atomic Energy Act, which prohibits the disclosure of Restricted Data or Formerly Restricted Data (42 U.S.C. 2161-2165).
  - [ ] Section 147 of the Atomic Energy Act, which prohibits the disclosure of Unclassified Safeguards Information (42 U.S.C. 2167).
  - [ ] 41 U.S.C., Section 4702(b), prohibits the disclosure of contractor proposals in the possession and control of an executive agency to any person under section 552 of Title 5, U.S.C. (the FOIA), except when incorporated into the contract between the agency and the submitter of the proposal.
- [ ] Exemption 4: The withheld information is a trade secret or commercial or financial information that is being withheld for the reason(s) indicated.
  - [ ] The information is considered to be confidential business (proprietary) information.
  - [ ] The information is considered to be proprietary because it concerns a licensee's or applicant's physical protection or material control and accounting program for special nuclear material pursuant to 10 CFR 2.390(d)(1).
  - [ ] The information was submitted by a foreign source and received in confidence pursuant to 10 CFR 2.390(d)(2).
  - [ ] Disclosure will harm an identifiable private or governmental interest.
- [ ] Exemption 5: The withheld information consists of interagency or intraagency records that are not available through discovery during litigation. Applicable privileges:
  - [ ] Deliberative process: Disclosure of predecisional information would tend to inhibit the open and frank exchange of ideas essential to the deliberative process. Where records are withheld in their entirety, the facts are inextricably intertwined with the predecisional information. There also are no reasonably segregable factual portions because the release of the facts would permit an indirect inquiry into the predecisional process of the agency.
  - [ ] Attorney work-product privilege. (Documents prepared by an attorney in contemplation of litigation)
  - [ ] Attorney-client privilege. (Confidential communications between an attorney and his/her client)
- [ ] Exemption 6: The withheld information is exempted from public disclosure because its disclosure would result in a clearly unwarranted invasion of personal privacy.
- [x] Exemption 7: The withheld information consists of records compiled for law enforcement purposes and is being withheld for the reason(s) indicated.
  - [ ] (A) Disclosure could reasonably be expected to interfere with an enforcement proceeding (e.g., it would reveal the scope, direction, and focus of enforcement efforts, and thus could possibly allow recipients to take action to shield potential wrong doing or a violation of NRC requirements from investigators).
  - [ ] (C) Disclosure could constitute an unwarranted invasion of personal privacy.
  - [ ] (D) The information consists of names of individuals and other information the disclosure of which could reasonably be expected to reveal identities of confidential sources.
  - [x] (E) Disclosure would reveal techniques and procedures for law enforcement investigations or prosecutions, or guidelines that could reasonably be expected to risk circumvention of the law.
  - [x] (F) Disclosure could reasonably be expected to endanger the life or physical safety of an individual.
- [ ] OTHER (Specify)

PART II.B -- DENYING OFFICIALS

Pursuant to 10 CFR 9.25(g), 9.25(h), and/or 9.65(b) of the U.S. Nuclear Regulatory Commission regulations, it has been determined that the information withheld is exempt from production or disclosure, and that its production or disclosure is contrary to the public interest. The person responsible for the denial are those officials identified below as denying officials and the FOIA/PA Officer for any denials that may be appealed to the Executive Director for Operations (EDO).

DENYING OFFICIAL	TITLE/OFFICE	RECORDS DENIED	APPELLATE OFFICIAL		
			EDO	SECY	IG
James T. Wiggins	Director, Office of Nuclear Security Incident Reporting	See Form 464, Part I.C	☑	☐	☐
			☐	☐	☐
			☐	☐	☐

Appeal must be made in writing within 30 days of receipt of this response. Appeals should be mailed to the FOIA/Privacy Act Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, for action by the appropriate appellate official(s). You should clearly state on the envelope and letter that it is a "FOIA/PA Appeal."

CONFIDENTIAL
OFFICIAL USE ONLY

November 28, 2001 SECY-01-0215

FOR: The Commissioners

FROM: William D. Travers
Executive Director for Operations

SUBJECT: SCOPING PAPER FOR A COMPREHENSIVE REVIEW OF THE NRC'S SAFEGUARDS AND SECURITY PROGRAMS IN LIGHT OF THE TERRORIST ATTACKS ON SEPTEMBER 11, 2001

PURPOSE

In response to the Chairman's memorandum dated September 28, 2001, the staff is providing to the Commission and requesting approval of a proposed course of action and proposed schedule for a comprehensive review of the NRC's safeguards and security programs. The staff is also seeking Commission guidance on preliminary issues associated with the comprehensive review. Finally, the staff is providing the Commission a classified, preliminary assessment of the current threat environment and requesting approval of an approach for establishing interim compensatory measures for categories of NRC licensees.

INTRODUCTION

As a result of the terrorist attacks on September 11, 2001, Chairman Meserve issued a memorandum to the Executive Director for Operations (EDO), dated September 28, 2001, [Attachment 1], in which he directed the staff to undertake a thorough review of the NRC's safeguards and security programs, with focus on identifying any necessary adjustments to the response capabilities of the NRC; licensees; and Federal, State, and local agencies.

CONTACTS: Vonna L. Ordaz, NRR/DIPM
(301) 415-2147
Jack R. Davis, NMSS/FCSS
(301) 415-7256

OFFICIAL USE ONLY
CONFIDENTIAL

Upon Removal of Attachment 10 this SECY Paper is UNCLASSIFIED

The Chairman's memorandum specifically required that the staff's review include a comprehensive examination of the basic assumptions underlying the NRC's current safeguards and security programs. In addition, the memorandum directed the staff to provide to the Commission a "scoping paper" containing a proposed course of action, proposed schedule, and any preliminary issues for which the staff seeks Commission guidance.

Subsequently, in a memorandum dated October 9, 2001, the EDO established the Response to Terrorist Acts (RTA) Task Force comprised of senior managers from selected offices and a deputy regional administrator to develop this scoping paper. A copy of the Task Force Charter is attached [Attachment 2]. In parallel with developing a charter, the Task force prepared the NRC request that the U.S. Office of Management and Budget (OMB) provide additional FY 2002 and 2003 funds in support of the NRC's response to the September 11 terrorist attack [Attachment 3]. The staff is conducting Program Review Committee meetings to identify programmatic and budget changes which may be necessary to provide resources for new safeguards and security activities.

The staff is also providing to the Commission a classified, preliminary assessment of the current threat environment [Attachment 10] facing NRC licensees. This assessment of the threat environment is focused on the overall scope and capability of potential adversaries rather than focusing on a specific design basis threat for which the licensee alone must protect. In addition, the staff is providing to the Commission and requesting approval of an approach to establish interim compensatory measures to enhance safeguards and security at licensee and certificate holder facilities, including proposed criteria for discriminating between licensees/certificate holders and Federal, State, and local responsibilities. The staff has included examples in Attachment 10 for nuclear power plants and uranium conversion facilities that were developed using this approach. The staff anticipates providing proposed interim compensatory measures to the Commission for approval by January 15, 2002 or sooner.

BACKGROUND

The NRC's response to the events of September 11, 2001, are summarized in Section A below, and the NRC's statutory bases for protection of nuclear facilities and nuclear material are summarized in Section B below.

A. NRC Actions in Response to the Terrorist Attacks of September 11, 2001

On September 11, 2001, terrorists simultaneously attacked commercial and government targets in New York, NY, and Washington, DC utilizing large commercial U.S. aircraft as weapons. Although there were no specific credible threats and no attacks against NRC-licensed facilities or activities,[1] the NRC took certain actions to ensure that the agency was able to monitor the

[1] A threat was received against the Three Mile Island power reactor on October 17, 2001. The NRC treated this threat as credible and the licensee, the State, and Federal

situation in a heightened threat environment, and advised licensees on measures they should take to respond to any events that might occur. Toward that end, the NRC activated its Incident Response Plan, analyzed available information, and provided safeguards advisories to selected licensees (i.e., power reactor licensees and Category I fuel facilities). These advisories described short-term and other actions to strengthen licensee's capabilities to deal with the potential spectrum of events that could be related to the September 11 attacks. The NRC also issued advisories to independent spent fuel storage installations, non-power reactors, large material licensees and Agreement States. The NRC continues to update and supplement these advisories when warranted. Further, NRC resident and specialist inspectors have reviewed licensee actions in response to these advisories. Additionally, Chairman Meserve has communicated with State governors on support for requests for additional security measures at power reactor and Category I fuel facility licensees.

From September 11 to November 16, 2001, the NRC remained in the "Standby" mode continuously staffing the headquarters' operations center and regional incident response centers (IRCs); provided an NRC representative to the Strategic Information and Operations Center (SIOC) established by the Federal Bureau of Investigation (FBI); and, when needed, provided an NRC representative to the Emergency Support Team of the Office of Homeland Security. On November 16, the headquarters' operations center shifted to a "Modified Standby" mode and the regional IRCs shifted to an "on call" posture. The NRC also enhanced its communications and interfaces with members of the intelligence community [including the U.S. Departments of Defense (DOD), Justice (DOJ), and Energy (DOE)], States, and other entities. NRC regional administrators held extensive discussions with senior executives for reactor licensees in their respective regions, and NRC management and staff continue to meet regularly with industry representatives to discuss and evaluate heightened security measures. In addition, the NRC briefed members of Congress and oversight committees upon request, and the Chairman and the Secretary of Energy have met with the Director General of the International Atomic Energy Agency (IAEA) to discuss international cooperation in safeguarding nuclear programs and combating terrorism.

With respect to the NRC's internal physical security program, the agency has increased the level of security at the headquarters complex and at each of the NRC's regional offices. With respect to the NRC's information security programs, the NRC shut down its external web site to review its contents for sensitive information that might be of use to a potential adversary. The staff subsequently returned a small portion of the web site to service and is returning non-sensitive documents to public access in accordance with a redesigned web-site format.

---

agencies took appropriate protection measures. However, subsequent information indicated that the threat was not credible.

B. Statutory Bases for Safeguards and Security

The NRC's mission under the Atomic Energy Act of 1954 (AEA), as amended, is to ensure adequate protection of the health and safety of the public and the environment and to protect the common defense and security with regard to the operation of nuclear facilities and use of nuclear materials. This statutory mandate includes the responsibility to ensure adequate safeguards of nuclear materials, including special nuclear material (SNM), and physical security of nuclear facilities. This broad responsibility, initially established by the AEA [see, generally, Sections 2 and 3 of the AEA], and upon enactment of the Energy Reorganization Act of 1974 (ERA), became the NRC's primary mission [see ERA, Title II]. The ERA also required the NRC to review the safety and safeguards of all facilities and materials licensed under the AEA. This broad mandate encompasses monitoring, testing, and recommending necessary upgrading of internal systems to account for SNM. It also encompasses developing contingency plans to deal with threats, thefts, and sabotage related to SNM, high-level radioactive waste, and nuclear facilities, in all activities licensed under the AEA [see ERA § 204(b)].

The Commission's general regulatory authority in Sections 161b, 161i, and 161o of the AEA is extremely broad and specifically includes authority which encompasses safeguards and security of facilities and materials. In particular, Section 161b authorizes the Commission to "establish, by rule, regulations, or order, such standards and instructions to govern the possession and use of special nuclear material, source material, and byproduct material as the Commission may deem necessary or desirable to promote the common defense and security or to protect health or to minimize danger to life or property...."

Section 161i provides, in relevant part, that the Commission is authorized to prescribe such regulations or orders as it may deem necessary "(2) to guard against the loss or diversion of any special nuclear material ... to prevent any use or disposition thereof which the Commission may determine to be inimical to the common defense and security, ... and (3) to govern any activity authorized pursuant to this Act, including standards and restrictions governing the design, location, and operation of facilities ... in order to protect health and to minimize danger to life or property."

The NRC's current safeguards requirements implementing this authority are contained in 10 CFR Parts 20 and 73. They include the NRC's design basis threats for sabotage and theft, and represent the results of ongoing discussion over civilian use of nuclear materials and the level of physical protection that should be required for nuclear facilities, material, and activities.

In addition to being statutorily responsible for protection of facilities, materials, and activities, the NRC is also responsible for ensuring protection of certain kinds of information about these facilities and activities and, at the same time, making available a large amount of information. Some of the statutes aimed at these potentially conflicting responsibilities are Government-wide, and others are specific to nuclear matters. The Government-wide National Security Act of 1947 requires that NRC protect "national security information" (NSI), which is

commonly known as "classified" information. The criteria for classifying information are set forth in Executive Order 12958. At the same time, the Government-wide Freedom of Information Act (FOIA), the Government in the Sunshine Act (GISA), and the Federal Advisory Committee Act (FACA) prescribe a high degree of public access to Government information, with certain well-known exceptions (in particular the exception for information classified under Executive Order 12958).

To these general requirements for protection of NSI and for openness under FOIA, GISA, and FACA, sections 141 and 147 of the AEA add specific requirements regarding two kinds of information about nuclear facilities, materials and activities — "Restricted Data" (RD), which is essentially a form of classified information, and "Safeguards Information" (SGI), which is sensitive unclassified information that is subject to restricted dissemination because it "specifically identifies a licensee's or applicant's detailed [material] control and accounting measures and security measures." Although the AEA protects both RD and SGI, it also sets high thresholds for calling information either RD or SGI and explicitly does not authorize the agency "to prohibit the public disclosure of information pertaining to the routes and quantities of shipments of source material, by-product material, high level nuclear waste, or irradiated nuclear reactor fuel."

DISCUSSION

The staff has developed and is requesting Commission approval of a proposed course of action to conduct a comprehensive review of the safeguards and security programs for NRC-licensed facilities/activities, the NRC security infrastructure, the Incident Response Program, the means of intergovernmental coordination, and the process for engaging NRC stakeholders. The proposed course of action is described in Section A below. In order to appropriately schedule activities, the staff developed a methodology to prioritize the various reviews of NRC-licensed facilities/activities. The methodology includes both consequence- and vulnerability-informed insights, among other criteria and is discussed in Task B below. Additionally, the staff has summarized the boundary conditions and assumptions that it used in developing the proposed course of action and associated major milestones.

In developing the proposed course of action, the staff identified four policy issues for which the staff is seeking Commission guidance (Section B below). Commission guidance on these policy issues is fundamental to assessing options and the establishment of any final recommendations from a comprehensive review of the NRC's safeguards and security programs. While the Commission considers these policy issues the staff intends to conduct near term activities using the series of interim measures such as those discussed in Section C and listed in Attachment 8.

As discussed in Section D below, the staff has identified areas in the NRC's strategic plan that should likely be reviewed during this proposed course of action. In Section E the staff has provided information on proposed changes to the agency's organizational structure, staffing,

and training in security and safeguards. Recent actions taken by foreign governments and the NRC's international coordination efforts since the terrorist attacks of September 11 are provided in Section F.

A. Proposed Course of Action in Response to Terrorist Acts

The staff has developed a proposed course of action for review of the NRC's safeguards and security programs that contains three major interdependent components (tasks), as follows:

Task A – Intergovernmental Coordination and Stakeholder Communications
Task B – Comprehensive Review and Implementation of Safeguards and Security Revisions for NRC-Licensed Facilities/Activities
Task C – Review of the NRC's Infrastructure and Incident Response Program

These tasks identify specific work activities that provide for a comprehensive and timely examination of the current safeguards and security programs, including their fundamental assumptions. Attachment 4 provides a flowchart for each of the three major tasks, and are summarized below. The staff has also determined the required level of effort, resources, and associated schedules with various sub-tasks needed to accomplish each main task.

The staff has also provided as Attachment 5, a schedule with major milestones for the proposed course of action for each task. These milestones are divided into three areas: Immediate or Current Activities, Comprehensive-Review Phase, and Implementation Phase. The first area reviews the activities that have already been completed or will be completed in the very near term. The Comprehensive-Review Phase compiles the tasks that are directly related to the review of safeguards and security of NRC licensees, the agency infrastructure, and the Incident Response Program. The last area is the Implementation Phase, which provides the options for regulatory actions, including rulemaking, needed subsequent to the comprehensive review, and the activities to revise regulatory guidance, training, inspection programs, performance-based testing, and emergency planning exercises affected by rulemaking. Finally, in Attachment 6 the staff has provided a detailed comparison (i.e., a "crosswalk") between the Chairman's September 28 memorandum, the supplemental funding request of October 19, 2001, and the tasks and sub-tasks in the proposed course of action.

Review of Intergovernmental Coordination and Stakeholder Communication — Task A

Task A describes an integrated approach for coordinating and communicating with both internal and external stakeholders. The purpose of this task is to refine intergovernmental communications between Federal, State, local, and Tribal governments and the NRC by determining appropriate levels of communication; establishing communications protocols and expectations; and establishing intergovernmental alignment. Once these actions are achieved, a long-term stakeholder communication and participation plan would be developed to include Federal, State, local, and Tribal governments; licensees; certificate holders; industry groups;

public interest groups; the media; and members of the public. Some activities under this task are currently underway. For example, since September 11 the NRC has enhanced its communications and interfaces with elements of the national intelligence community, States, and other stakeholders. Communications between NRC Regional Administrators and senior executives for reactor licensees, in their respective regions, is still ongoing. In addition, NRC management and staff have met regularly with licensees and industry representatives to discuss the implementation of heightened security measures at licensee facilities/activities. Senior agency managers have briefed Members of Congress and the oversight Committees on the actions taken by the NRC, and the staff has responded to numerous Congressional inquiries. As an additional interim measure, a near-term communications plan with stakeholders would be developed if the Commission determines that the proposed course of action should be provided to the public.

Comprehensive Review and Implementation of Safeguards and Security Revisions for NRC-Licensed Facilities/Activities — Task B

Task B describes a comprehensive methodology for reviewing the safeguards and security of NRC-licensed facilities/activities which begins with an evaluation and assessment of the national threat characteristics and the threat to NRC-licensees, and culminates with revisions to existing regulations, guidance, and supporting inspection programs. For each class of facility/activity, the staff intends to evaluate the need for, and put in place, interim compensatory measures based upon a preliminary assessment of the threat environment. In the longer term, the staff would reexamine threat characteristics for each class of facility/activity and determine any significant safeguards vulnerabilities [both physical protection and material control and accounting (MC&A) measures]. Using that data, the staff intends to reevaluate the physical protection, MC&A, and access authorization requirements, as needed, for each class of licensee. The staff intends to compare the results of that information with the feasibility and practicality of a licensee implementing the identified physical protection measures. For threats beyond the capability and practicality of a licensee to implement, the staff intends to evaluate the need for augmentation of the licensee's physical protection measures. This augmentation may be provided by local, State, and Federal entities, which may require coordination with other Federal departments and agencies. In addition, the staff intends to evaluate the impacts on radiological emergency preparedness and the integration of security and emergency planning against the new threat environment and assumptions. The staff intends to coordinate this evaluation with the security and radiological emergency preparedness communities.

The staff has prioritized these activities according to the ranking of the facility/activity, as discussed below, to accomplish the course of action as expeditiously as possible by permitting concurrent activities. For example, while the staff is refining its analysis of the threat, the staff would also be examining vulnerabilities of licensed facilities/activities through structural studies and safeguards assessments. This process will expedite projects, although program offices must consider the degree that resource constraints impact the ability to conduct activities in parallel. During the evaluation and assessment, the staff intends to collect data needed to

reexamine existing regulations and guidance. Tasks which are not dependent upon completion of other tasks are expected to start immediately; some of them are currently underway.

Once the evaluation and assessment have been completed, the results would be incorporated by rulemaking or other regulatory means; by revision of regulatory guidance; and by revision of inspection programs, as appropriate. The staff will perform a backfit analysis that addresses the requirements of 10 CFR 50.109, 70.76, 72.62, 76.76 and related provisions, and will include an evaluation of whether the proposed changes are necessary to ensure the facility provides adequate protection of public health and safety and is in accord with common defense and security.

Prioritization of NRC-Licensed Facilities/Activities

The staff recognizes that all of the tasks in the proposed course of action cannot be accomplished simultaneously. In order to address this issue, the staff has categorized NRC-licensed facilities/activities into nine classes for prioritization purposes: power reactors, decommissioning facilities, non-power reactors, independent spent fuel storage installations (ISFSIs), fuel cycle facilities (Categories I and III), gaseous diffusion and uranium conversion facilities, byproduct facilities, industrial and medical licensees, and transportation of radioactive material. The prioritization of NRC facilities/activities into classes is reflected on pages 5 and 6 of Attachment 5, in the sequencing of activities and sub-tasks.

(b)(7)(F)

Review of the NRC's Infrastructure and Incident Response Program — Task C

Task C provides a proposed course of action for reviewing the NRC's infrastructure, including: the NRC's Incident Response Program, the NRC's internal physical security program, the NRC's web sites, and the NRC's secure communications capabilities. The NRC's internal physical security program may be upgraded, including physical upgrades of NRC buildings and evaluation of alternate response centers for Continuity of Operations/Continuity of Government (COOP/COG). These processes are currently underway. The staff also is currently evaluating

the NRC's public web site and the cyber security of the NRC's information technology infrastructure in the areas of enhanced security detection and monitoring, increased technical support, and threat analysis. The staff plans to analyze the capability of the NRC's public web site to provide a sustained capability to disseminate critical health and safety information to the public and stakeholders under surge conditions of significant demand. The staff will inform the Commission of any significant necessary changes.

Another large portion of this review involves the area of secure communications, both internally and externally. The staff is in the process of evaluating the NRC's information security program for control of classified or sensitive unclassified information; how that program supports the headquarter's Operations Center and Regional Incident Response Centers; and how that program impacts communications with Federal, State, local, Tribal, governments and licensees. In addition, the staff is evaluating methods and equipment to enhance transmittal of classified and sensitive unclassified information, within the agency, to NRC licensees, and to others. Some activities in this task are currently underway.

Lastly, the staff is re-evaluating the agency's incident response plans, policies, procedures, and emergency preparedness regulations. The staff is also prepared to respond to initiatives established by sources external to the NRC (e.g., the Office of Homeland Security). The staff will identify any necessary changes and they will be made in concert with the appropriate NRC offices.

Internal Communication and Monitoring of the Proposed Course of Action

The staff's ongoing work on the proposed course of action will be updated and tracked in order to provide the Commission and NRC managers with timely information on the overall progress of the proposed course of action, the status of key milestones, and timely identification of any emergent policy issues. This tracking system will be maintained such that it can be used to facilitate timely communication of the agency's actions to key external stakeholders.

To facilitate timely completion of these milestones and individual tasks, the staff working on these projects will remain cognizant of prior task results, any interdependencies between tasks accomplished by different program offices, the current status of tasks, and the resources planned for upcoming tasks, versus those actually used.

Assumptions and Boundary Conditions

In developing this paper, the staff's proposed course of action and schedule were predicated upon (1) receipt of adequate funding from the OMB, as requested in Attachment 3, (2) receipt of Commission guidance on the specific policy issues discussed in Section B below, (3) reprogramming of any necessary resources under the planning, budgeting, and performance management (PBPM) "add/shed" process; and (4) receipt of any necessary external input (e.g., from the Office of Homeland Security). Additionally, the staff used standard

planning assumptions in developing the proposed course of action and major milestones, and assumed that stakeholder interactions would occur according to existing agency processes. Furthermore, the supplemental funding request included all activities described in the proposed course of action, but did not include RTA impacts on future licensing of a mixed-oxide (MOX) fuel fabrication facility or new power reactors. Finally, the staff recognizes that additional policy issues may be identified, as the course of action progresses. The staff iwill seek Commission guidance on any emergent policy issues, as they are identified.

The task force's course of action does not presume any fundamental flaws in the NRC's rules or internal operations. Rather, this paper outlines the policies, topics, and regulatory areas that require analysis as a result of the September 11, 2001, terrorist attacks. Notwithstanding this presumption, the staff has already identified several potential improvements to security programs which are currently under consideration. However, the full nature of any potential changes requires an in-depth evaluation of the feasibility and costs. Furthermore, the staff recognizes that modifications to the proposed course of action may be required, subsequent to the submission of this paper, based on external influences. Consequently, the staff recognizes that flexibility may be needed in implementing the proposed course of action.

B. Policy Issues for Which the Staff is Seeking Commission Guidance

Associated with Tasks A, B, and C of the proposed course of action, the staff has preliminarily identified four policy issues for which the staff is seeking Commission guidance [Attachment 7]. These policy issues are summarized below and include:

Issue 1 – The Boundary Between Private/government Security Responsibility
Issue 2 – The Nrc's Role and Interface in the National Infrastructure
Issue 3 – Balancing National Security Interests with Public Information Needs
Issue 4 – Protecting the Public from Release of Hazardous Chemicals at NRC-licensed Facilities.

In Attachment 7, the staff has provided detailed information for each policy issue, discussed the context of each issue, and identified aspects requiring Commission guidance. In Section C below the staff has provided interim actions relating to the preliminary policy issues [Attachment 8].

Boundary Between Private/Government Security Responsibility — Issue 1

This policy issue questions how responsibility should be allocated among licensee, Federal State, and local entities to respond to a spectrum of threats, including threats that exceed the design basis threats (DBTs)[2], to best protect public health and safety and the common defense

[2] The NRC currently has two DBTs — one for theft and diversion of SNM and the second for radiological sabotage at power reactors.

and security. In order to address this issue, the existing threat environment must be reassessed and possibly be modified in coordination with other Federal agencies, including the DOE and the DOD. The objective of this threat reassessment and modification is to clearly and completely identify threat characteristics against which licensees and/or State, local or Federal entities must protect. The sum of these efforts may also require the Commission, the Federal community, and stakeholders to revisit the larger issue of what constitutes an acceptable level of risk to the public, as well as reassessing the roles and responsibilities of Federal agencies in addressing the threat environment.

The staff will provide any further detailed information associated with the following issues, if requested by the Commission. The Commission is requested to provide guidance as to (1) whether the staff should implement the modified threat assessment approach (as described in Attachment 7) to clearly identify which characteristics of the threat are within licensee's capabilities, and which are not; (2) whether the staff should revisit the NRC's 1976 decision on Federalization of NRC-licensed power reactor security forces; and (3) whether 10 CFR 50.13 should be modified or reinterpreted to reflect a clear delineation of responsibilities for those characteristics beyond the capabilities of a licensee to protect. Whether similar regulations should be written to delineate division of responsibilities for other NRC-licensed facilities.

NRC's Role and Interface in National Infrastructure — Issue 2

This policy issue questions whether NRC should pursue protection of licensed facilities/activities as part of the Nation's critical infrastructure. It also questions the role that the NRC should play in defining and protecting critical national infrastructure. In addition, this policy issue summarizes the NRC's past activities in this area, the best information available as to the current definition of "critical national infrastructure," a discussion of the licensed nuclear industry as a part of the Nation's critical national infrastructure, and a discussion of the NRC's potential leadership role in policy development and implementation in this area.

The Commission is requested to provide guidance as to (1) the degree to which the NRC should play a more direct and substantial role in shaping national policy regarding protection of NRC licensees and Agreement State activities as critical national infrastructure, (2) whether the staff should proceed in developing the bases for including additional NRC-licensed facilities/activities as elements of the critical national infrastructure, and (3) whether the staff should reassess the agency's position on whether the NRC's internal infrastructure is critical.

Balancing National Security Interests with Public Information Needs — Issue 3

This policy issue relates to redefining what information the NRC should routinely release to the public, as well as to what extent and under what processes NRC stakeholders should be involved in the Agency's decision-making process. Also, this issue addresses how the agency should limit or prohibit public access to "sensitive" information by classification as national security information or control as safeguards information (i.e., exempt from disclosure under

UNCLASSIFIED
OFFICIAL USE ONLY

FOIA). The degree of meaningful public participation and involvement in NRC regulatory programs is a function of the public's ability to readily access information.

This issue also discusses the potential for significant internal and external impacts arising from an increased quantity of classified information. Internal impacts would involve staff (increased resources to respond to FOIA requests and questions from stakeholders), facilities (increased need for secure work space and classified material storage areas, (b)(7)(F) (b)(7)(F) telecommunications (increased numbers of secure telephones), and staff training and oversight to handle, store, process, and communicate a significantly increased volume of classified material. For an increased quantity of SGI information, similar internal impacts would occur. For classified information, external impacts would involve increased processing of security clearances for licensee facilities and personnel.

The Commission is requested to provide guidance as to (1) whether the staff should undertake a review of MD 3.4 and related regulations and redefine what types of information should be routinely released to the public; (2) whether the staff should seek to limit [restrict] public access to sensitive information or to prohibit public access to sensitive information (i.e., the material would meet one of the FOIA exemptions); (3) whether the staff should propose changes to the NRC's Strategic Plan associated with the public confidence strategy in recognition of the new terrorist threat and the NRC's increased need to restrict access to sensitive information; (4) whether the staff should undertake a review of our openness policy and determine whether alternate means to obtain meaningful public participation in the NRC's regulatory process are sufficient.

Protecting the Public from Releases of Hazardous Chemicals at NRC-Licensed Facilities — Issue 4

This issue questions the need for NRC to pursue regulatory authority for protection of hazardous chemicals against sabotage at licensed facilities. The NRC, U.S. Environmental Protection Agency (EPA), and U.S. Occupational Safety and Health Administration (OSHA) currently do not have specific requirements in this area. By contrast, the NRC's statutory authority extends to licensed radioactive materials and their associated byproducts. Any authority to regulate chemicals is, at best, implicit, and is likely limited to chemicals used to process licensed materials or chemicals that could directly affect licensed materials and increase radiation risk. Such authority does not extend to protection of bulk chemical storage areas located in a licensee's site.

(b)(7)(F)

OFFICIAL USE ONLY
UNCLASSIFIED

The Commission is requested to provide guidance as to (1) whether the agency should pursue resolution of long-standing jurisdictional issues between the NRC, EPA and OSHA regarding responsibility for protecting chemical components or activities against acts of terrorism and sabotage on NRC licensed sites or involving NRC licensed materials; and (2) whether the staff should increase its participation and visibility on interagency committees and working groups related to chemical issues to assure that NRC positions are well represented during the developmental stages of policy development as opposed to after the fact.

C. Interim Actions Relating to the Policy Issues

In Attachment 8, the staff has provided the Commission a summary of the interim measures both taken and proposed by the NRC until decisions on the policy issues described in Section B are made. This information is intended to provide a starting point for Commission deliberations on the proposed course of action and the policy issues.

D. NRC Strategic Goals and Performance Measures

As a consequence of the proposed course of action, the staff believes that the NRC must revisit its Strategic Plan (NUREG-1614, Vol 2, Parts 1 and 2) to address several issues. These issues include (1) updating specific strategies against theft and diversion, as well as radiological sabotage, in the Nuclear Reactor Safety, Nuclear Materials Safety, Nuclear Waste Safety, and International Nuclear Safety Support arenas; (2) developing new strategies for the protection of sensitive information; (3) updating the public confidence strategies in light of the new strategies for the protection of sensitive information; (4) developing new measures in the Nuclear Material Safety and Nuclear Waste Safety arenas relating to the loss of control of licensed material and attempted malevolent use of this material; and (5) developing new measures on reporting requirements for malevolent use of nuclear material. Additionally, the NRC may need to take a broader or more in-depth review of its strategic goals and performance measures.

E. NRC Organizational Structure

In Attachment 1, the Chairman also directed the staff to evaluate "the agency's organizational structure, staffing, and training in the security and safeguards areas." The staff will address this task in developing the agency's workforce restructuring plan, as mandated by the OMB, and will provide the plan to the Commission in June 2002, as indicated in the appendices to the FY 2003 Budget Estimates and Performance Plan (Blue Book), which the staff provided to OMB on October 30, 2001.

F. Foreign Government Responses and Coordination with International Organizations

The international community responded immediately following the terrorist attacks on September 11, 2001. Countries with nuclear and radiological programs implemented additional measures to improve the security posture at their nuclear facilities and associated activities. The staff has provided a summary of specific actions taken by various foreign governments in Attachment 9. The staff obtained this information from a variety of sources, but generally not through official government-to-government channels. Additionally, the staff was provided a description of actions proposed by the IAEA to strengthen its programs and assist Member States in improving their material control and accounting and physical protection regimes.

Separately, Chairman Meserve met with Secretary of Energy Spencer Abraham and IAEA Director General Dr. Mohamad ElBaradei to discuss international cooperation to further strengthen nuclear programs and controls and combat terrorism. The NRC staff has also provided periodic updates to the IAEA staff concerning the NRC's actions since September 11.

CONCLUSIONS

The staff believes that the proposed course of action for conducting a comprehensive review of the NRC's safeguards and security programs, as discussed above, accomplishes the tasking directed by the Chairman's September 28 memorandum to (1) set forth the staff's proposed course of action, (2) set forth a proposed schedule (including identification of major milestones) to implement the course of action, and 3) identify any preliminary issues for which the staff is seeking Commission guidance.

While this course of action is underway, the staff intends to identify appropriate interim compensatory measures, in addition to the immediate measures that have already been taken, to ensure public health and safety. The staff is confident that this approach will provide adequate protection in the current threat environment and allow for a longer-term, methodical and comprehensive safeguards review to be completed. The staff intends to propose adjustments or additional measures to react to a significant change in the national threat environment, if warranted. The staff believes that the proposed course of action and the interim compensatory measures represent a comprehensive and appropriate response strategy to the events of September 11.

In implementing this course of action, the staff plans to continue its coordination and communication efforts with the national intelligence community, the Homeland Security Council, other key Federal agencies, and Congress. Further, the NRC will continue to engage its stakeholders as appropriate, in accordance with established policies, in the development of any regulatory or guidance changes.

RESOURCES

Not all of the resources to conduct the activities described in the proposed course of action are included in the NRC's FY 2002 appropriation. In Attachment 3, the Commission requested that OMB provide additional supplemental funds for FY 2002. The FY 2003 budget request to OMB, as also modified by Attachment 3, includes resources for these activities. The OMB decision on the NRC's FY 2002 emergency supplemental funding request and the FY 2003 budget request will be included in the FY 2003 budget passback that is expected in the near term.

The staff's proposed recommendations are predicated upon the receipt of adequate funding from the OMB for FY 2002 and FY 2003. If that does not occur, the staff intends to examine to what extent reprogramming of available resources under the PBPM "add/shed" process will be needed to maintain the scope and duration of the proposed course of action.

COORDINATION

The Office of the General Counsel has participated in the development of this paper as part of the RTA Task Force. The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objections.

RECOMMENDATIONS

That the Commission:

1. Approve the staff's proposed course of action and proposed schedules as discussed in Attachments 4 and 5.

2. Approve the staff's approach to the development of proposed interim compensatory measures for nuclear power reactors and the uranium conversion facility, as provided in Attachment 10, and the plan to proceed with an assessment of need for interim compensatory measures for other categories of licensees/certificate holders.

3. Provide guidance to the staff on the policy issues discussed in Attachment 7.

4. Note:

   a. The appropriate Congressional committees, members of Congress who expressed specific interest in the NRC's actions, and the Office of Homeland Security, will be informed of the agency's progress to date and anticipated approaches contained in the proposed course of action.

   b. Several elements of the staff's proposed course of action are already underway.

c. The staff will submit additional policy and/or rulemaking papers to the Commission, consistent with the milestones described in Attachment 5.

William D. Travers
Executive Director for Operations

Attachments:
1. Memo to EDO from Chairman Meserve, dated September 28, 2001 (U)
2. Task Force Charter on Response to Terrorist Acts (U)
3. Supplemental Funding Request to OMB (Letter from Chairman Meserve, dated October 19, 2001) (U)
4. Proposed Course of Action for the Comprehensive Evaluation of Safeguards and Security (U)
5. Major Milestones for the Proposed Course of Action (U)
6. Comparison Between the Chairman's Memo to the EDO, the Supplemental Funding Request, and the Proposed Course of Action (U)
7. Details of the Policy Issues (U)
8. Interim Actions Relating to the Policy Issues (U)
9. Foreign Government Responses and International Coordination (U)
10. Approach for Developing Interim Compensatory Measures Considering the Current Threat Environment (C)

Commissioners' completed vote sheets/comments should be provided directly to SECY by **c.o.b. Thursday, December 13, 2001.**

Commission staff office comments, if any, should be submitted to the Commissioners **NLT December 6, 2001,** with an information copy to SECY. If the paper is of such a nature that it requires additional review and comment, the Commissioners and the Secretariat should be apprised of when comments may be expected.

DISTRIBUTION:
Commissioners
OGC
OIP
OCA
CFO
EDO
REGIONS
SECY

ATTACHMENT 1

Memo to the EDO from Chairman Meserve, dated September 28, 2001 (U)

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

CHAIRMAN

SENSITIVE INFORMATION - NOT FOR PUBLIC RELEASE

UNCLASSIFIED

September 28, 2001

OFFICIAL USE ONLY

MEMORANDUM TO: William Travers
Executive Director for Operations

FROM: Richard A. Meserve

SUBJECT: Response to Terrorist Acts

In the aftermath of the terrorist attacks of September 11, 2001, and the continuing uncertainty about future terrorist intentions, the NRC must undertake a thorough review of its safeguards and physical security program. I believe that the NRC has responded to these unsettling events in an appropriate, expeditious, and thoughtful manner, and that the NRC's current security and safeguards programs provide for a very high level of security. However, the nature and scope of the attacks have made clear that special and focused attention must be given to any necessary adjustments in NRC, licensee, and Federal, State, and local response capabilities. Moreover, the nature of the terrorist attacks requires that the NRC's review include a comprehensive examination of the basic assumptions underlying the current safeguards and physical security program.

This effort should include, but should not necessarily be limited to, an evaluation of the following items:

- the agency's safeguards and security regulatory requirements, as well as policies and guidance to licensees. This should include evaluation of NRC inspection and assessment activities;
- the scope of licensee obligations and those of governmental entities in the event of attacks that exceed NRC's Design Basis Threat (DBT);
- the vulnerability of NRC-licensed facilities to attacks that exceed the DBT;
- the policies and procedures relating to the protection of critical NRC infrastructure, including both headquarters and regional offices. This should include an evaluation of the adequacy of contingency plans to maintain continuity of operations during events that result in the unavailability of the Headquarters Emergency Response Center or the Region IV Incident Response Center;
- the capability for handling and processing classified information in the Emergency Response Center and the Region Incident Response Centers. Recommendations should be provided for improving these capabilities and for making physical modifications to allow classified briefings in or near the Emergency Operations Center or backup facilities;

OFFICIAL USE ONLY

SENSITIVE INFORMATION - NOT FOR PUBLIC RELEASE

UNCLASSIFIED

- the capability to transmit classified information in a timely fashion to appropriate State officials and licensee facilities with the need to know;

- the agency's organizational structure, staffing, and training in the security and safeguards area;

- the policies, procedures, and regulations related to the control of the availability and access to information having safeguards and security implications regarding licensed activities;

- the agency's emergency response planning, staffing and training for handling protracted events;

- coordination and communication with other Federal agencies, State and local governments, and licensees. This should include consideration of the need for contacts at a variety of levels at other Federal agencies, including contacts at a decision/policy-making level; and

- communication with the press, public, and interested parties as appropriate.

Because there will no doubt be widespread examination of the implications of the recent terrorist attacks by the Executive Branch and the Congress, the NRC effort will have to be integrated in some respects with a broader national strategy.

Therefore I, with the full support of the Commission, direct you to establish a special task force to conduct a comprehensive review of the safeguards and security program. The task force should include representatives from the Office of General Counsel, the Regions, and the program offices. An early product should be a paper for Commission review that sets out the staff's proposed course of action, the proposed schedule, and any preliminary issues on which the staff seeks guidance.[1]

Additional resources, beyond those provided in the budget, should be requested from OMB in support of this effort. The initial paper scoping the effort should be provided to the Commission within the next 60 days.

SECY please track.

cc: See next page

---

[1] Due to the many significant and interrelated activities already underway in the reactor safeguards area that may be impacted by the recommendations of the task force, the staff should immediately identify the papers now pending Commission review that should be withdrawn, supplemented, or revised.

cc: Commissioner Dicus
Commissioner McGaffigan
Commissioner Merrifield
OCA
OGC
CFO
SECY

ATTACHMENT 2

Task Force Charter on Response to Terrorist Acts (U)

RESPONSE TO TERRORIST ACTS (RTA) TASK FORCE FINAL CHARTER

1. BACKGROUND

On September 28, 2001, Chairman Meserve tasked the Executive Director for Operations (EDO) with initiating a thorough review of NRC's safeguards and physical security programs as a result of the September 11, 2001, terrorist attacks on the United States. With full support of the Commission, the EDO was directed to establish a special task force composed of representatives from the Office of General Counsel, the Regions, and the program offices to conduct this review.

2. OBJECTIVES

- To provide a comprehensive examination of the basic assumptions underlying the current NRC safeguards and physical security programs as a result of the implications associated with the September 11th terrorist attacks.
- To develop a proposed course of action based on assessment of the adequacy of current policies, programs, and requirements; develop a proposed schedule, and; identify preliminary issues in which the staff seeks Commission guidance
- To provide special and focused attention to any necessary adjustments in NRC, licensee, and Federal, State, and local response capabilities
- To evaluate the scope of licensee obligations and those of governmental entities in the event of attacks that exceeded NRC's Design Basis Threat
- To integrate the Emergency Funding Request and any additional supplemental funding into the proposed course of action associated with the comprehensive review of the NRC safeguards and physical security programs

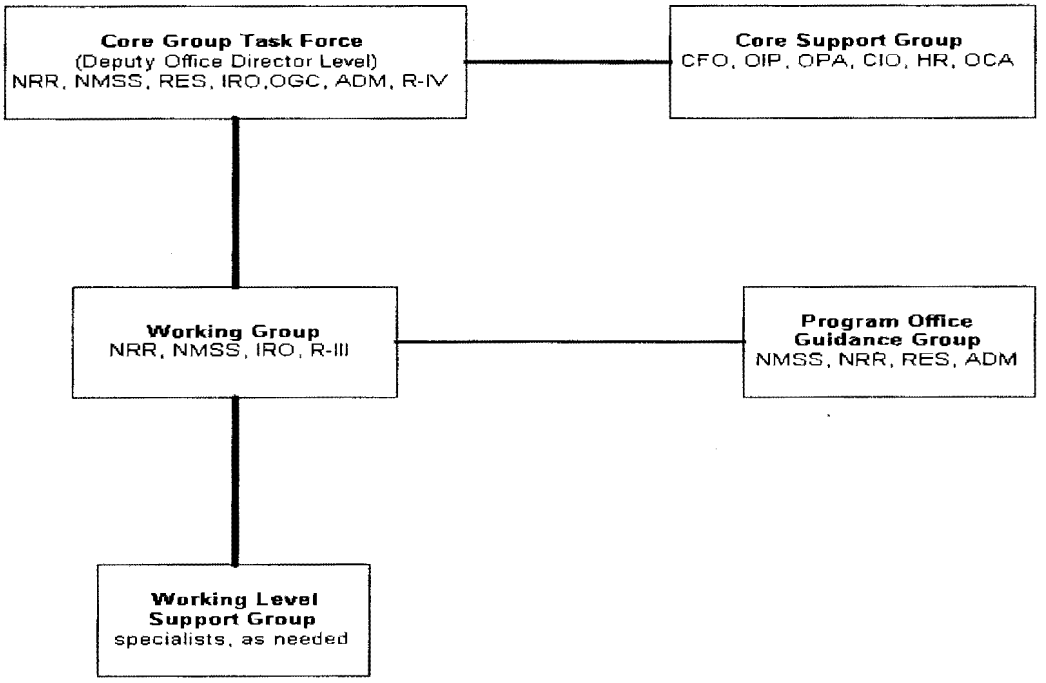
3. DELIVERABLES

- Initial Emergency Funding Request for Supplemental Appropriations Act
  Due: October 5, 2001 to CFO (Complete)
- Final Emergency Funding Request information to support 10/18/01OMB Briefing
  Due: October 16, 2001 to EDO (Complete)
- EDO Memo on Recommendation for Withdrawal of Commission Papers
  Due: October 19, 2001 to EDO (Complete)

- Identification of Near-term, high-profile activities since 9/11
  Due: October 26, 2001 to EDO (Complete)

- Initial scoping Commission paper
  Due: November 21, 2001 to EDO; November 28, 2001 to Commission

5. ORGANIZATION



6. ROLES/RESPONSIBILITIES

Core Group Task Force - responsibilities include coordination and integration of intra-office issues, strategic guidance/direction, and external agency interface

Core Support Group - responsibilities include interface and support (e.g., budget, resources, congressional interfaces, public/stakeholder interactions, information technology support, international-related issues, and others, as needed)

Program Office Guidance Group - responsibilities include program office alignment and program level interfaces with external stakeholders

Working Group - responsibilities include synthesis of major program technical issues and products as directed by the core group;

Working Level Support Group - specialized technical support from line organization, as needed (e.g., emergency preparedness specialists, threat analysts, physical security specialists, legal specialists, etc.) and as directed by the Working Group

7. MEMBERSHIP

Core Group Task Force - M. Federline, NMSS (Task Force Chairperson) J. Johnson, NRR; R. Zimmerman, RES; S. Burns, OGC; P. Gwynn, Region IV; J. Holonich, IRO; and M. Springer, ADM

Core Support Group - R. Rough, CFO; B. Keeling, OCA; R. Hauber, OIP; E. Hayden, OPA; J. McDermott, HR; J. Schaeffer, CIO

Program Office Guidance Group - G. Tracy, NRR; C. Haney, M. Weber, NMSS, D. Dorman, RES; T. Martin, ADM

Working Group - Vonna Ordaz (co-lead), Jack Davis (co-lead)

Full-time Support - B. Schnetzler (task lead), R. Albert, H. Bailey, B. Baxter, P. Brochman, J. Creed, S. Crockett, E. Fox, J. Goldberg, E. Jacob-Baynard, A. Ramey-Smith, M. Warren

As-needed Support - R. Carmon, C. Cox, B. Dam, W. Davis, K. Fitch, K. Gibson, C. Harbaugh, B. Manili, D. Negrin, E. Perch, L. Silvious, C. Stone, E. Weinstein

8. COMMUNICATIONS/INTERFACES

Core Group Task Force - meets twice weekly; interfaces with Core Support Group, as necessary; interfaces with EDO on a weekly basis; interfaces with the Commission and external stakeholders, as necessary

Working Group - meets daily; interfaces with Core Group Task Force biweekly; supports Core Group Task Force meetings; interfaces with Working Level Support Group daily; interfaces with Program Office Guidance Group biweekly

NRR/NMSS Leadership Teams - informational briefings mid-course and prior to final draft deliverables, if possible

Program Office Guidance Group - obtains input from internal stakeholders with regards to the Enemy of the State objective and engages in external communications to address it

9. ATTACHMENTS

EDO's Memo entitled "Response to Terrorist Acts," dated October 9, 2001

EDO R/F

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

October 9, 2001

MEMORANDUM TO: Martin J. Virgilio, Director, Office of Nuclear Material Safety and Safeguards
Samuel J. Collins, Director, Office of Nuclear Reactor Regulation
Ashok C. Thadani, Director, Office of Nuclear Regulatory Research
Karen D. Cyr, General Counsel
Michael L. Springer, Director, Office of Administration
Ellis W. Merschoff, Regional Administrator, Region IV
Richard H. Wessman, Director, Incident Response Operations
William M. Beecher, Director, Office of Public Affairs
Stuart Reiter, Chief Information Officer
Janice Dunn Lee, Director, Office of International Programs
Jesse L. Funches, Chief Financial Officer
Paul E. Bird, Director, Office of Human Resources

FROM: William D. Travers
Executive Director for Operations

SUBJECT: RESPONSE TO TERRORIST ACTS

The Chairman's September 28, 2001 memorandum, "Response to Terrorist Acts," Attachment 1, discussed the need for a comprehensive examination of the basic assumptions underlying our current safeguards and physical security programs. In order to conduct this examination in an integrated and effective manner, a Task Force is being formed to develop a proposed course of action, target schedules and milestones, and identify preliminary issues. The Task Force's early product will be a SECY paper which is an initial scoping effort, and is scheduled to be completed within 60 days.

The Task Force will be composed of a Core Group and a Support Group (Attachment 2). The Core Group will include the following representatives: M. Federline (NMSS), Chairperson; M. Springer (ADM); J. Johnson (NRR); S. Burns (OGC); R. Zimmerman (RES); and P. Gwynn (RIV). The Core Group has already been tasked to develop a charter which will discuss roles and responsibilities, and identify senior managers who will be members of the Support Group. Support Group participation may be expanded as new activities or needs are identified during the review.

Additionally, the Deputy Executive Directors for Operations will provide senior level review and coordination support for the Task Force as it undertakes this important review.

Attachments: As stated

cc: W. Kane, OEDO
C. Paperiello, OEDO
P. Norry, OEDO
H. Miller, RI
B. Mallett, RII
J. Dyer, RIII

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

CHAIRMAN

SENSITIVE INFORMATION - NOT FOR PUBLIC RELEASE

September 28, 2001

MEMORANDUM TO: William Travers
Executive Director for Operations

FROM: Richard A. Meserve

SUBJECT: Response to Terrorist Acts

In the aftermath of the terrorist attacks of September 11, 2001, and the continuing uncertainty about future terrorist intentions, the NRC must undertake a thorough review of its safeguards and physical security program. I believe that the NRC has responded to these unsettling events in an appropriate, expeditious, and thoughtful manner, and that the NRC's current security and safeguards programs provide for a very high level of security. However, the nature and scope of the attacks have made clear that special and focused attention must be given to any necessary adjustments in NRC, licensee, and Federal, State, and local response capabilities. Moreover, the nature of the terrorist attacks requires that the NRC's review include a comprehensive examination of the basic assumptions underlying the current safeguards and physical security program.

This effort should include, but should not necessarily be limited to, an evaluation of the following items:

- the agency's safeguards and security regulatory requirements, as well as policies and guidance to licensees. This should include evaluation of NRC inspection and assessment activities;
- the scope of licensee obligations and those of governmental entities in the event of attacks that exceed NRC's Design Basis Threat (DBT);
- the vulnerability of NRC-licensed facilities to attacks that exceed the DBT;
- the policies and procedures relating to the protection of critical NRC infrastructure, including both headquarters and regional offices. This should include an evaluation of the adequacy of contingency plans to maintain continuity of operations during events that result in the unavailability of the Headquarters Emergency Response Center or the Region IV Incident Response Center;
- the capability for handling and processing classified information in the Emergency Response Center and the Region Incident Response Centers. Recommendations should be provided for improving these capabilities and for making physical modifications to allow classified briefings in or near the Emergency Operations Center or backup facilities;

SENSITIVE INFORMATION - NOT FOR PUBLIC RELEASE

- the capability to transmit classified information in a timely fashion to appropriate State officials and licensee facilities with the need to know;
- the agency's organizational structure, staffing, and training in the security and safeguards area;
- the policies, procedures, and regulations related to the control of the availability and access to information having safeguards and security implications regarding licensed activities;
- the agency's emergency response planning, staffing and training for handling protracted events;
- coordination and communication with other Federal agencies, State and local governments, and licensees. This should include consideration of the need for contacts at a variety of levels at other Federal agencies, including contacts at a decision/policy-making level; and
- communication with the press, public, and interested parties as appropriate.

Because there will no doubt be widespread examination of the implications of the recent terrorist attacks by the Executive Branch and the Congress, the NRC effort will have to be integrated in some respects with a broader national strategy.

Therefore I, with the full support of the Commission, direct you to establish a special task force to conduct a comprehensive review of the safeguards and security program. The task force should include representatives from the Office of General Counsel, the Regions, and the program offices. An early product should be a paper for Commission review that sets out the staff's proposed course of action, the proposed schedule, and any preliminary issues on which the staff seeks guidance.[1]

Additional resources, beyond those provided in the budget, should be requested from OMB in support of this effort. The initial paper scoping the effort should be provided to the Commission within the next 60 days.

SECY please track.

cc: See next page

---

[1] Due to the many significant and interrelated activities already underway in the reactor safeguards area that may be impacted by the recommendations of the task force, the staff should immediately identify the papers now pending Commission review that should be withdrawn, supplemented, or revised.

cc: Commissioner Dicus
Commissioner McGaffigan
Commissioner Merrifield
OCA
OGC
CFO
SECY

Attachment 2

TASK FORCE MEMBERSHIP

Core Group

Office of Nuclear Materials Safety and Safeguards
Office of Nuclear Reactor Regulation
Office of Nuclear Regulatory Research
Office of the General Counsel
Office of Administration
Region IV (representing all four regions)

Support Group

Office of Incident Response Operations
Office of the Chief Financial Officer
Office of International Programs
Office of Public Affairs
Office of the Chief Information Officer
Office of Human Resources

ATTACHMENT 3

Supplemental Funding Request to OMB (Letter from Chairman Meserve, dated October 19, 2001) (U)

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

CHAIRMAN

October 19, 2001

UNCLASSIFIED
OFFICIAL USE ONLY

The Honorable Mitchell E. Daniels, Jr.
Director
Office of Management and Budget
Eisenhower Executive Office Building
Washington, D.C. 20503

Dear Mr. Daniels:

I am writing on behalf of the Nuclear Regulatory Commission (NRC) in response to your September 14, 2001 memorandum concerning emergency funding to respond to the terrorist attacks that occurred on September 11, 2001. We appreciate the Administration's commitment to reimburse all costs directly related to these terrorist attacks, including preparedness and mitigation of potential threats.

In response to the September 11, 2001, terrorist attacks, the Commission has taken a number of responsive actions to ensure adequate protection of civilian nuclear power plants and nuclear fuel facilities, including activation and staffing the NRC Operations Center 24 hours a day. In addition, the Commission has close coordination with the Federal Bureau of Investigation, other intelligence and law enforcement agencies, NRC licensees, and military, state, and local authorities. We continue to monitor the situation, and are prepared to make any adjustments to security measures as may be deemed appropriate.

The Commission believes that we have responded to these unsettling events in an appropriate, expeditious, and thoughtful manner, and that the current security and safeguards programs provide for a very high level of security at our licensed facilities. However, in the aftermath of the terrorist attacks and the continuing uncertainty about future terrorist intentions, we have commenced a thorough review of our safeguards and physical security programs, including a comprehensive examination of the programs' basic underlying assumptions. The nature and scope of the attacks have made clear the urgency for giving special and focused attention to any necessary adjustments in NRC, licensee, and Federal, State, and local response capabilities.

To meet these urgent needs to prevent and mitigate the potential impact of terrorist attacks on commercial nuclear facilities, and the transportation, storage and use of commercial nuclear materials, resources in addition to those previously planned and budgeted are needed. We currently estimate that our activities will require an additional $36 million in FY 2002 and $29 million in FY 2003. I request that funds for FY 2002 be provided from those made available by the Emergency Supplemental Appropriations Act of 2001. Our FY 2003 estimate can be considered an addition to our September 14, 2001 budget request for FY 2003. Since these

additional activities are needed to properly respond to the recent terrorist attacks and buttress government-wide efforts to protect the national interests and safeguard the national infrastructure, we strongly believe that these funds should come from the General Fund and not from fees charged to NRC licensees. Many of these additional activities will assist the Office of Homeland Defense in developing strategies to defend NRC-licensed facilities against beyond design basis threat enemy-of-the-state terrorist attacks.

As explained in more detail in the enclosure, NRC's additional activities and resource needs are focused on the following:

- Re-analyzing its threat assessment framework and its design basis threats which are used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material.

- Re-analyzing the vulnerabilities and physical protection requirements for NRC-licensed facilities and for radioactive materials in transit.

- Re-analyzing the processes used to authorize access to NRC-licensed facilities.

- Strengthening NRC's emergency preparedness and response capabilities and better integrating its security and emergency preparedness planning.

- Strengthening NRC's infrastructure and communications capabilities.

We are committed to continuing to ensure the protection of public health and safety in the wake of these tragic events. I would be pleased to meet with you and your staff to discuss our emergency funding needs.

Sincerely,

Richard A. Meserve

Enclosure: As stated

cc: J. Pfeiffer, OMB

NUCLEAR REGULATORY COMMISSION'S EMERGENCY FUNDING REQUIREMENTS TO RESPOND TO THE SEPTEMBER 11, 2001 TERRORIST ATTACKS

In response to the September 11, 2001 terrorist attacks, the Nuclear Regulatory Commission (NRC) has been working around the clock to ensure adequate protection of nuclear power plants and nuclear fuel facilities. This has involved close coordination with the Federal Bureau of Investigation, other intelligence and law enforcement agencies, NRC licensees, and military, State, and local authorities. The agency continues to monitor the situation, and is prepared to make any adjustments to security measures as may be deemed appropriate.

The NRC has responded to these unsettling events in an appropriate, expeditious, and thoughtful manner, and the current security and safeguards programs provide for a very high level of security at NRC-licensed facilities. However, in the aftermath of the terrorist attacks and the continuing uncertainty about future terrorist intentions, the NRC must undertake a thorough review of its safeguards and physical security programs, including a comprehensive examination of the programs basic underlying assumptions. The results of this review not only aid NRC in its efforts but will also assist the Office of Homeland Defense in developing strategies to defend NRC-licensed facilities against beyond design basis threat enemy-of-the-state terrorist attacks. The nature and scope of the attacks have made clear the urgency for giving special and focused attention to any necessary adjustments in NRC, licensee, and Federal, State, and local response capabilities. In doing so, the NRC is focusing its efforts on:

1. Re-analyzing its threat assessment framework and its design basis threats which are used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material.

2. Re-analyzing the vulnerabilities and physical protection requirements for NRC licensed facilities and for the transportation of radioactive materials.

3. Re-analyzing the processes used to authorize access to NRC-licensed facilities.

4. Strengthening NRC's emergency preparedness and response capabilities and better integrating its security and emergency preparedness planning.

5. Strengthening NRC's infrastructure and communications capabilities.

The table below summarizes NRC's Salaries and Expenses Appropriations resource requirements for the 5 activities listed above:

Activity Number	FY 2002	FY 2003
1	$2.7	$1.7
2	18.2	13.3
3	4.4	3.3
4	5.4	4.3
5	5.4	6.7
TOTAL	$36.1M	$29.3M

The following provides a more detailed explanation of these activities.

1. RE-ANALYZE NRC'S THREAT ASSESSMENT FRAMEWORK AND ITS DESIGN BASIS THREATS.

	FY2002	FY2003
Request:	$ 2.7M	$ 1.7M

Explanation/Justification:

The design basis threats (DBTs), as delineated in the NRC's regulations, are used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material. The DBT varies with the category of licensee, depending on whether the threat includes theft and sabotage (at fuel cycle facilities) or only sabotage (at nuclear power reactors). With the additional funding, the NRC intends to:

- Re-evaluate the NRC's threat assessment methods and approach used to define the DBT and consider the need for an expansion of the DBT and application of a DBT to other NRC-licensed activities.
- Re-evaluate the NRC's adversary characteristics document (ACD) that provides additional detail on the weapons and tactics associated with the DBT.
- Re-evaluate 10 CFR 50.13, "Attacks and destructive acts by enemies of the United States; and defense activities."
- Re-analyze how the DBT is applied to performance-based exercises at NRC licensed facilities; the extent of insider assistance/information available to the adversaries; and the extent, predictability, and sophistication of the threat scenarios.

- Increase the NRC's interactions with other Federal agencies to ensure coordination of national infrastructure decisions which may impact activities/decisions in this area.

- Evaluate the potential impact of cyber-terrorism on NRC-licensed facilities.

In addition, the quantity of intelligence information received has increased significantly and is expected to increase even more as the U.S. undertakes action to fight terrorism worldwide. This increase has resulted in the following increased resource requirements:

- Analysis and disposition of the increased intelligence information.

- Extended support to the NRC Incident Response Center.

- Reconfigure and expand the Two White Flint North SCIF.

- Procure additional stand-alone classified workstations for the NRC's threat analysis.

2. RE-ANALYZE THE VULNERABILITIES AND PHYSICAL PROTECTION REQUIREMENTS.

	FY2002	FY2003
Request:	$18.2M	$13.3M

Explanation/Justification:

The terrorist events of September 11, 2001 necessitate a re-evaluation of the existing requirements for the physical protection of radioactive materials used or possessed at fixed facilities (e.g., power reactors, nonpower reactors, decommissioning reactors, fuel cycle facilities, by-product material licensees, and spent fuel storage installations). Additionally, physical protection requirements must also be re-evaluated for the transportation of special nuclear material (SNM), spent fuel, high level waste, and byproduct material. With the additional funding, the NRC intends to use a risk-informed process to:

- Re-examine the NRC's statutory and regulatory requirements, and guidance on physical protection for facilities and transportation of materials.

- Evaluate the need for physical protection requirements at NRC-licensed facilities currently not covered by existing physical protection regulations.

- Examine the need for physical protection against chemical/industrial sabotage at NRC-licensed facilities.

- Re-examine the NRC's physical protection requirements with regard to the security impacts on the national infrastructure from the loss of such facilities.

- Develop and analyze representative nuclear power reactor structures under various attack loading conditions and conduct an integrated assessment of the effects of various attack scenarios, including cyber attacks.

- Develop and analyze spent fuel storage casks and radioactive material transportation packages under various attack loading conditions and conduct an integrated assessment of the effects of various attack scenarios.

- Evaluate other types of facilities (as described above) and analyze various attack conditions and conduct an integrated assessment of the effects of various attack scenarios.

3. RE-ANALYZE ACCESS AUTHORIZATION PROCESSES AT NRC LICENSED FACILITIES.

	FY2002	FY2003
Request:	$ 4.4M	$ 3.3M

Explanation/Justification:

Licensees will continue to be charged with processing access authorization requests; however, in light of the September 11, 2001 terrorist attacks, the NRC intends to implement near-term access authorization process improvements that includes:

- Expediting improvements to the existing access authorization process at NRC reactor sites for individuals with temporary unescorted access, including the processing of fingerprints through electronic means.

Longer term access authorization process initiatives involve:

- Evaluating the adequacy and robustness of the existing access authorization process at NRC-licensed facilities.

- Evaluating the need for access authorization processes at other NRC-licensed facilities (e.g., by-product materials, non-power reactors, category II and III facilities).

- Determining the feasibility of integrating a national security check program into existing processes at NRC-licensed facilities.

- Determining the feasibility of obtaining overseas criminal history checks.

4. STRENGTHEN NRC'S EMERGENCY PREPAREDNESS AND RESPONSE TO TERRORIST ACTS.

	FY 2002	FY 2003
Request:	$ 5.4M	$ 4.3M

Explanation\Justification:

As a result of the September 11, 2001 terrorist attack, the NRC must evaluate and upgrade, as necessary, emergency preparedness and response programs for terrorist attacks using conventional, chemical and/or biological weapons. This includes reexamining the processes, staffing, and authority of the NRC Incident Response Center (IRC) with respect to the new level of threat demonstrated by the terrorists. With the additional funding, the NRC intends to:

- Evaluate the NRC's capability to respond to multiple, coordinated terrorist attacks on commercial nuclear facilities throughout the United States.
- Evaluate and upgrade, as necessary, regulatory requirements and guidance for emergency preparedness programs at NRC-licensed facilities.
- Increase the NRC's staff resources to support additional counter terrorism and related emergency preparedness activities, to mobilize and respond to a national threat.
- Increase the NRC's coordination with stakeholders, including industry, public, other Federal government agencies, State and Tribal governments, and international counterparts relating to terrorist attacks and emergency preparedness and response.
- Reexamine the NRC's processes to support continuity of operations/continuity of government (COOP/COG), consistent with PDD-67.
- Evaluate adequacy of emergency action level (EAL) requirements and guidance in consideration of terrorist activities.
- Evaluate the adequacy of policy, programs, and guidance for public protective actions.
- Evaluate adequacy of protection equipment for licensee emergency response personnel against the revised spectrum of threats.
- Develop inspection guidance on licensees' integration of security and emergency plans to assess the capability of licensees to respond to terrorist attacks.

- Reassess NRC's capabilities for first response, independent assessment and oversight of incidents at licensee facilities (e.g., analytical tools, mobile labs)
- Accelerate the upgrade of the NRC's IRC Information Management System.
- Establish additional secure areas in NRC Region IV, Region IV IRC (as backup to Headquarters IRC), and establish off hour utilities for NRC Region II.
- (b)(7)(E)
- Enhance intelligence communications outlet (secure email and 4 additional STEs) in TWFN (b)(7)(F) and install additional secure communications in NRC HQ.
- Investigate the capability to transmit classified information in a timely fashion to appropriate State officials and licensee facilities (without resident inspector offices) that have a need-to-know.
- Identify and implement multiple levels of NRC official contacts/liaison with other Federal agencies including decision/policy-making level contacts.

5. STRENGTHEN NRC'S INFRASTRUCTURE AND COMMUNICATIONS CAPABILITIES.

	FY2002	FY2003
Request:	$ 5.4M	$ 6.7M

Explanation/Justification:

In light of the September 11, 2001 terrorist attacks, significant improvements are needed in NRC physical facilities and information technology infrastructures, and communications.

To provide adequate protection of NRC facilities, the NRC intends to:

(b)(7)(E)

To improve communications the NRC intends to:

- Review and revise the NRC's communication protocols with the press, public, members of Congress, and other interested stakeholders, as necessary, in order to balance public information needs with control of the availability and access to information having safeguards/security implications.

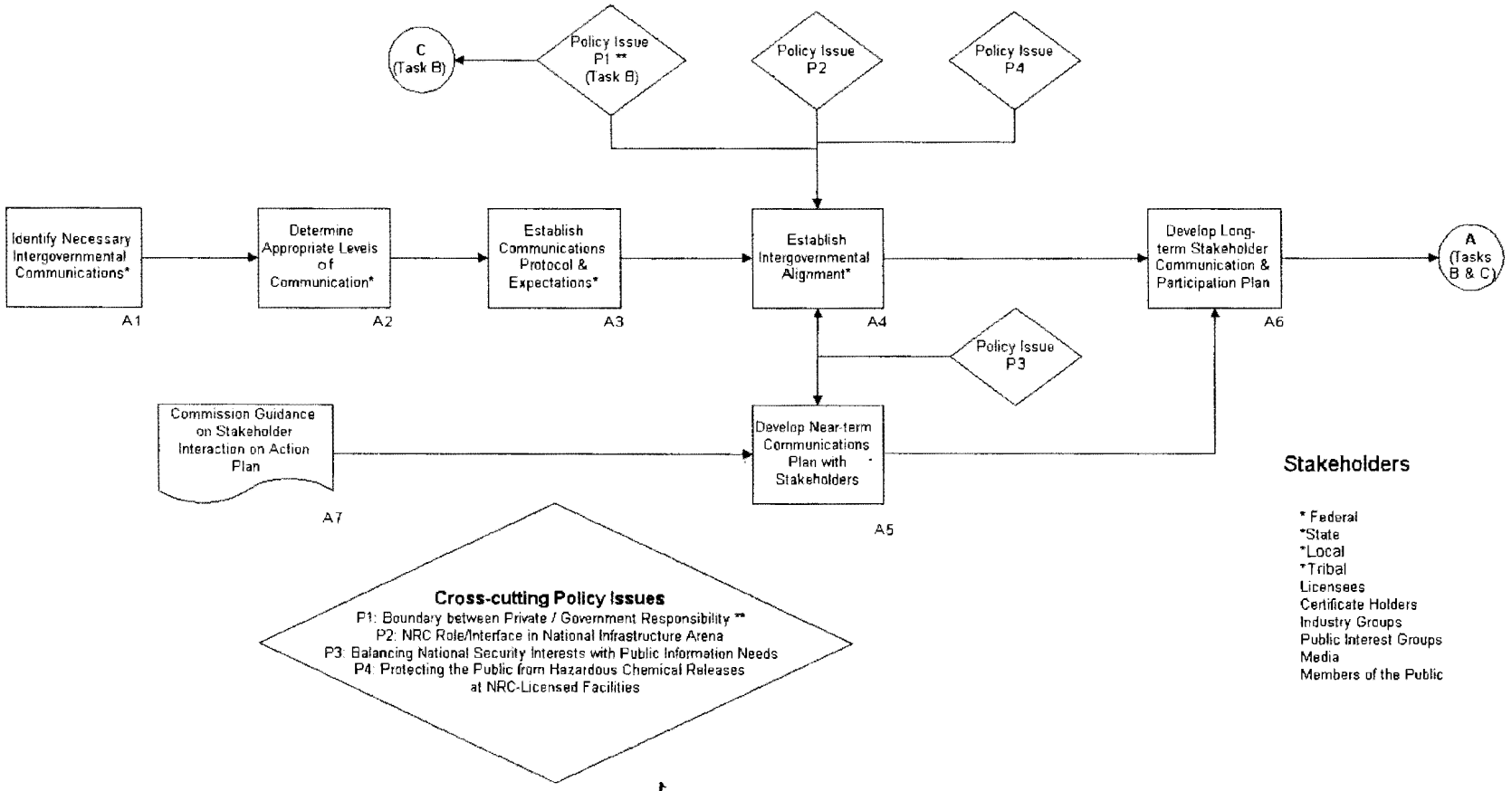
To improve the protection of NRC Information Technology Infrastructure and capabilities, the NRC intends to evaluate the need to:

- Expand staff to provide continuous technical support for the agency's information infrastructure
- Enhance security detection and monitoring capability for internal network/infrastructure security
- Conduct cyber threat analysis of the agency network security and Internet access to validate cyber security processes, procedures, and capabilities
- Expand external Web server capability to handle surge requirements from events

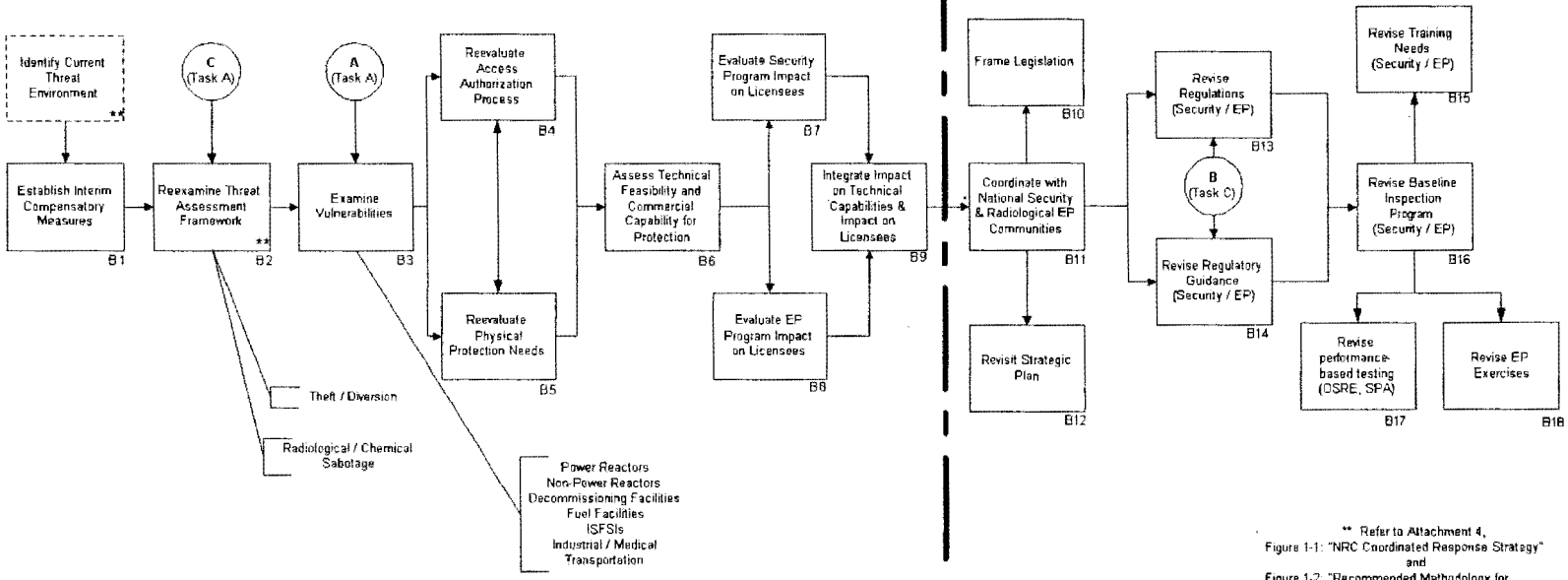
ATTACHMENT 4

Proposed Course of Action for the Comprehensive Evaluation of Safeguards and Security (U)

Task A: Intergovernmental Coordination and Stakeholder Communications

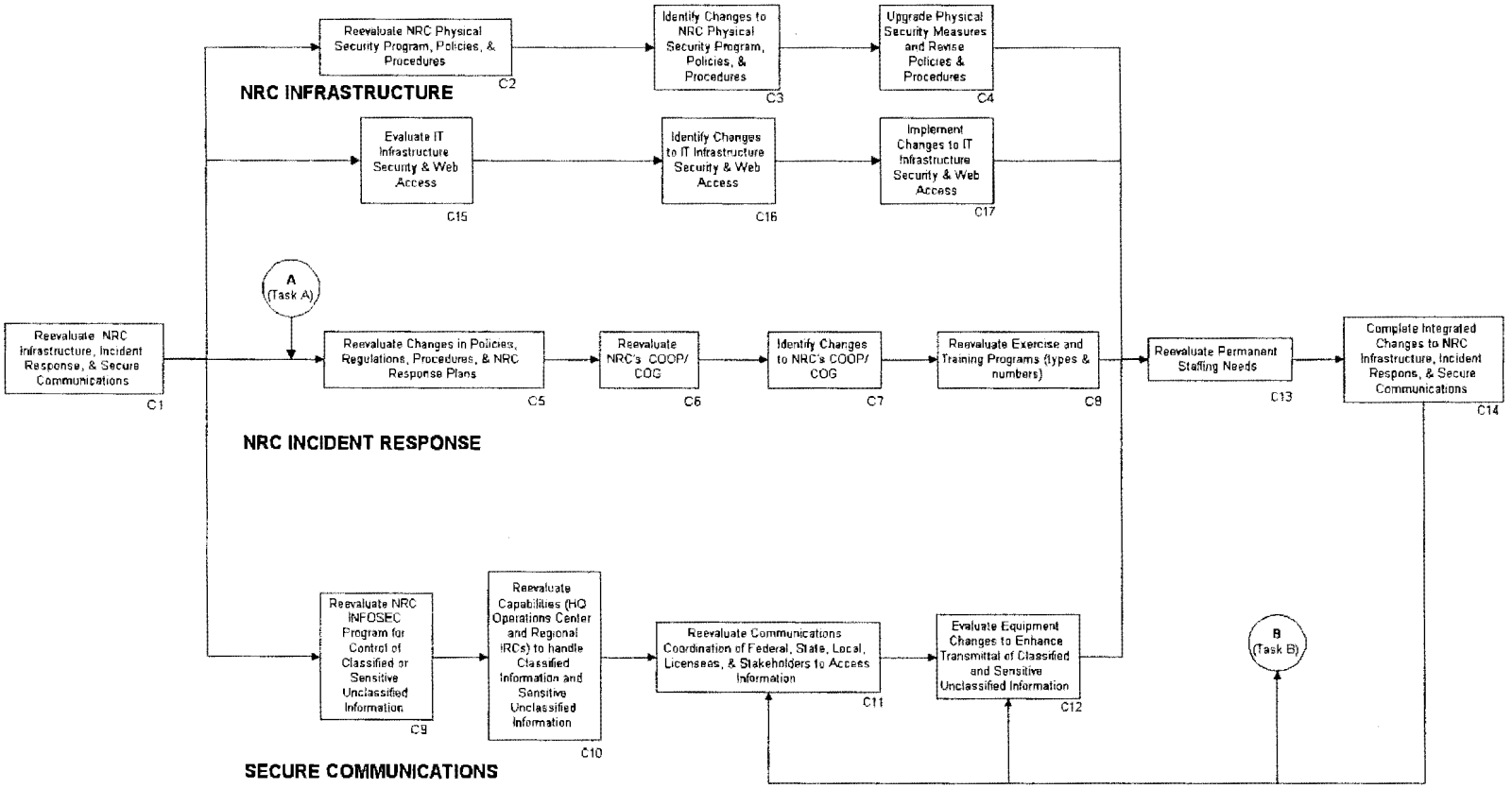


Task B: Comprehensive Review and Implementation of Safeguards and Security Revisions for NRC-Licensed Facilities / Activities



** Refer to Attachment 4,
Figure 1-1: "NRC Coordinated Response Strategy"
and
Figure 1-2: "Recommended Methodology for Resolving Government / Private Responsibility"

Task C: Review of NRC Infrastructure and Incident Response Program



ATTACHMENT 5

Major Milestones for the Proposed Course of Action (U)

Task A: Intergovernmental Coordination and Stakeholder Communications	Due Date
Policy Issue 1- Boundary Between Private/Government Responsibility (requesting feedback from Commission by due date)	1/15/02
Established presence at FBI Special Incident Operations Center.	9/11/01C
Conducted selected Security Audits- Fuel Facilities/Cat-2.	11/16/01C
Established initial contact with the Office of Homeland Security and the Department of Energy regarding design basis threat revision.	Ongoing
Provided onsite representative to the Office of Homeland Security	10/01C
Selected Security Audits-Fuel Facilities/Cat-1	12/6/01
Selected Security Reviews-Power Reactors	1/1/02
Staff Proposed Interim Compensatory Measures: (in order of priority as discussed in paper) - Decommissioning Reactors - Power Reactors - Fuel Facilities - Conv - Fuel Facilities - GDP - Transportation - Non Power Reactors - ISFSI - Indust/Med - Fuel Facilities - Cat-1 - Fuel Facilities - Cat-3	 12/21/01 11/28/01 11/28/01 12/15/01 1/15/02 1/11/02 1/15/02 1/15/02 12/15/01 12/21/01

Task A: Intergovernmental Coordination and Stakeholder Communications	Due Date
Policy Issue 2- NRC Role/Interface in National Infrastructure Arena (requesting feedback from Commission by due date)	1/15/02
Establish Lines of Contact - Intergovernmental Communications w/Federal, State, Local and Tribes	2/14/02
Determine Appropriate Levels of Communication	3/15/02
Establish Communications Protocol & Expectations	5/18/02
Policy Issue 3- Balancing National Security Interests with Public Information Needs (requesting feedback from Commission by due date)	1/15/02
Shutdown NRC's external web site, scrubbed it, and restored portions of the web site	10/17/01C
Submitted COMSECY-01-0030, "Guidance to the Staff on Release of Information to the Public," to the Commission, which contained criteria for discretionary release of information to the public.	10/29/01C
Develop Near-Term Communications Plan with Stakeholders	1/25/02
Develop Long-Term Stakeholder Communication & Participation Plan	3/18/02
Continue restoring portions of the web site as reviews are completed	ongoing
Policy Issue 4- NRC Responsibility regarding Chemical Sabotage (requesting feedback from Commission by due date)	1/15/02
Establish interim compensatory measures for uranium conversion facilities	11/28/01
Establish interim compensatory measures for GDP's	12/15/01

Other Intermediate/Concurrent Activities	Due Date
Enhanced security at NRC facilities.	9/11/01C
Advised Joint Chiefs of Staff on the limitations of nuclear facility security forces.	9/19/01C
Advised government agencies on possible nuclear plant vulnerabilities.	9/23/01C
Issued letters to Governors concerning the use of state resources in the protection of nuclear facilities.	9/26/01C
Initiated State-licensee dialogs for consideration of additional facility security measures.	9/26/01C
Coordinated with FAA for flight advisories and restrictions over nuclear facilities.	9/01C
Conducted Audit Instructions at Power Reactors and Decommissioning Reactors	11/16/01C
Purchased and installed software to expedite Electronic Fingerprinting Process for Access Authorization.	9/01C
Reviewed FBI watch lists against NRC employee records and forwarded them to licensees for check against licensee records.	10/25/01C
Issued Confirmatory Action Letters to decommissioning reactor licensees.	10/15/01C 10/19/01C 10/26/01C
Issued threat advisories to licensees (21 issued as of 11/9/01).	11/9/01
Suspended mail handling at NRC HQ and tested for anthrax; resumed mail upon negative results	10/31/01C

TASK B: Comprehensive Review and Implementation of Safeguards and Security Revisions for NRC-License Facilities									
Task B: Comprehensive Review Phase	**Decomm**	**Power Reactors**	**Fuel Fac Conv/ GDP**	**Trans-portation**	**Non-Power Reactors**	**Fuel Fac Cat-3**	**ISFSI**	**Indust/ Med**	**Fuel Fac Cat-1**
Liaison Threat w/Intell. & Fed. Law Enforcement ; New Threat Completed	3/02								
Modify Threat Assessment Program	6/02								
Develop Threat Assessment Rulemaking Package	8/02								
Determine feasibility of integrating Nat. Sec. check/overseas crim. His. Check into existing processes	5/30/02	5/30/02							5/30/02
SAFEGUARDS REVIEW - The dates noted below are the dates individual tasks are scheduled to be completed. The tasks are scheduled according to the four prioritization factors established for this review (See Section B of the Secy Paper), but also taking into consideration the workload/office assigned to each task. It is assumed that while working on one task, the responsible office would be collecting data and information to complete the next task, and so on. It should be noted that many of the individual tasks under Task B are not dependent upon completion of other tasks or prior tasks and are expected to start immediately, or are already in progress.									
Reevaluate Access Authorization Prog.	8/02	11/02	1/03	1/03	7/03	5/03	5/03	9/03	9/03

TASK B: Comprehensive Review and Implementation of Safeguards and Security Revisions for NRC-License Facilities

Task B: Comprehensive Review Phase	Decomm	Power Reactors	Fuel Fac Conv/ CDP	Trans-portation	Non-Power Reactors	Fuel Fac Cat-3	ISFSI	Indust/ Med	Fuel Fac Cat-1
Determine Structural Vulnerabilities	9/02	Phase 1 1/02 Phase 2 6/02 Phase 3 9/03	8/02	12/02	Part 1 6/02 Part 2/3 12/03	8/02	Part 1 6/02 Part 2/3 12/03	9/03	8/02
Determine Safeguards Vulnerabilities	9/02	5/03	3/03	8/03	8/03	9/03	8/03	12/03	12/03
Determine MC&A Vulnerabilities	9/02	5/03	3/03	8/03	8/03	9/03	8/03	12/03	12/03
Reevaluate Licensee Physical Protection Needs	11/02	7/03	5/03	10/03	10/03	11/03	10/03	2/04	2/04
Assess Technical Feasibility and Commercial Capability for Protection	12/02	8/03	6/03	11/03	11/03	12/03	11/03	3/04	3/04
Evaluate Security Program Impact on Licensees	12/02	8/03	6/03	11/03	11/03	12/03	11/03	3/04	3/04
Evaluate EP Program Impact on Licensees	12/02	8/03	6/03	11/03	11/03	12/03	11/03	3/04	3/04
Integrate Impact on Technical Capabilities & Impact on Licensees	1/03	9/03	7/03	12/03	12/03	1/04	12/03	4/04	4/04

TASK B: Comprehensive Review and Implementation of Safeguards and Security Revisions for NRC-License Facilities									
Task B: Implementation Phase	**Decomm. Power Reactors**	**Power Reactors**	**Fuel Fac. Conv/ GDP**	**Trans-portation**	**Non-Power Reactors**	**Fuel Fac. Cat-3**	**ISFSI**	**Indust/ Med**	**Fuel Fac. Cat-1**
Revisit Strategic Plan	9/03								
Frame Legislation, if needed	TBD								
Coordinate with national security and radiological emergency planning communities	4/03	12/03	10/03	3/04	3/04	4/04	3/04	7/04	7/04
Revise Requirements : Safeguards, Access Authorization, and Emergency Planning[1]									
Option 1: Issue Immediately Effective Order (non-confirmatory)	5/03	1/04	11/03	4/04	4/04	5/04	4/04	8/04	8/04
Consideration: Would require licensee to take action based on NRC directive; may involve hearing but after implementation.									
Option 2: Issue Immediately Effective Confirmatory Order	5/03	1/04	11/03	4/04	4/04	5/04	4/04	8/04	8/04

[1]Interim compensatory measures will be established for all licensees as needed, based on preliminary assessment of the threat, vulnerabilities, and consequences. Once a more thorough review is performed, based on more thorough analysis of the threat, vulnerabilities and consequences, the Commission can direct the staff to take any of a number of options for implementation based upon the outcome of this review. This range of options (none of which is mutually exclusive) each has a variety of implementation times and considerations.

TASK B: Comprehensive Review and Implementation of Safeguards and Security Revisions for NRC-License Facilities

Task B: Implementation Phase	Decomm	Power Reactors	Fuel Fac. Conv/ GDP	Trans-portation	Non-Power Reactors	Fuel Fac. Cat-3	ISFSI	Indust/ Med	Fuel Fac. Cat-1
Consideration: 1) follows an agreed upon action by the licensee but in the form of an order 2) licensee can waive right to hearing may involve hearing, but unlikely - public could request if claims injury									
Option 3: Confirmatory Action Letter (CAL)	5/03	1/04	11/03	4/04	4/04	5/04	4/04	8/04	8/04
Consideration: follows an agreed upon action by the licensee but **not** in the form of an order									
Option 4: Interim or Temporary Rule	1/04	8/04	6/04	12/04	12/04	1/05	12/04	4/05	4/05
Consideration: A regulatory document that is effective for a definable period of time. An interim or temporary rule has the same effect as a normal or final rule and provides an effective date for each amendment. The NRC may request public comment and consider adjustments to the regulation before adopting it in final form.									
Option 5: Immediate Effective Rule	immediate; effective usually 45 days after publication. Commission may omit notices and comment when, for good cause, it finds "notice and public procedure thereon are unpractical, unnecessary, or contrary to the public interest." Final rule is effective 30 days following publication unless the Commission finds "good cause" for a shorter period.								
Consideration: 1) can be made while normal rulemaking proceeds in parallel 2) Would have no stakeholder comment or restricted period of comments prior to rule implementation. 3) Rarely done by NRC									

TASK B: Comprehensive Review and Implementation of Safeguards and Security Revisions for NRC License Facilities									
Task B: Implementation Phase	**Decomm**	**Power Reactors**	**Fuel Fac: Conv/ GDP**	**Trans-portation**	**Non-Power Reactors**	**Fuel Fac: Cat-3**	**ISFSI**	**Indust/ Med**	**Fuel Fac: Cat-1**
Option 6: Final Rulemaking	10/04	6/05	4/05	9/05	9/05	10/05	9/05	12/05	12/05
Consideration: Full Public and stakeholder participation in the process; 1) time to complete can be lengthy, unless expedited (these dates are based on 18 months) 2) process could be pursued concurrently with other options - see overarching consideration below[2]									
Revise Regulatory Guidance: Safeguards, Access Authorization, and Emergency Planning	Guidance would be developed in parallel with the rulemaking option chosen from above.								
Revise NRC training needs: Safeguards, Access Authorization, and Emergency Planning	Completion would be approximately 2 ½ months subsequent to the rulemaking option chosen from above.								

[2]**Overarching considerations:** The following points should also be considered in the selection of an option for implementation.
1) Involving each facility stakeholder in process from the outset (including possible ACRS Committee) would have Immediate benefit- (time must be factored in to obtaining consensus)
2) Could be done concurrently with Interim or Temporary Rule, preceded by CAL, or if ineffective, supported by Immediately Effective Order.
3) Would have stakeholder buy-in during each phase of the review, making implementation easier.

TASK B: Comprehensive Review and Implementation of Safeguards and Security Revisions for NRC-License Facilities									
Task B: Implementation Phase	**Decomm**	**Power Reactors**	**Fuel Fac. Conv/ GDP**	**Trans-portation**	**Non-Power Reactors**	**Fuel Fac. Cat-3**	**ISFSI**	**Indust/ Med**	**Fuel Fac. Cat-1**
Revise Baseline Inspection Program: Safeguards, Access Authorization, and Emergency Planning	Completion would be approximately 6 months subsequent to the rulemaking option chosen from above.								
Evaluate Performance-Based Testing - OSRE or Other	Completion would be 4 months subsequent to completion of the regulatory guidance and in concert with the completion of the baseline inspection program.								
Revise Emergency Planning Exercises	Completion would be 4 months subsequent to completion of the regulatory guidance and in concert with the completion of the baseline inspection program.								

TASK C: Review of NRC Infrastructure and Incident Response Program	Due Date
Reevaluate NRC's Physical Security Measures, Policies, & Procedures	1/18/02
Identify changes to NRC's Physical Security Measures, Policies, & Procedures	3/25/02
Upgrade NRC Physical Security Measures and Revise Policies & Procedures	10/03/03
Evaluate NRC IT Infrastructure	4/15/02
Identify Changes to IT Infrastructure	6/15/02
Implement Changes to IT Infrastructure	10/15/02
Re-evaluate changes in Incident Response Policies, Regulations, Procedures	7/25/02
Re-evaluate NRC's COOP/COG	4/29/02
Re-evaluate Incident Response Exercise & Training Program	2/20/03
Re-evaluate NRC INFOSEC Program	3/18/02
Re-evaluate Capabilities (HQ/Reg) to handle classified information	3/25/02
Re-evaluate Communications w/Federal, State, Local, Licensees, Stakeholders	5/16/02
Evaluate Equipment Changes/Enhancements to transmit classified information	6/20/02
Re-evaluate Infrastructure Staffing needs	4/14/03

ATTACHMENT 6

Comparison Between the Chairman's Memo, the Supplemental Funding Request, and the Proposed Course of Action (U)

Comparison Between the Chairman's Memo, the Supplemental Funding Request, and the Proposed Course of Action

Chairman's Memo to the EDO	Supplemental Funding Request	Proposed Course of Action
evaluate agency's safeguards and security regulatory requirements, policies and guidance to licensees	Funding Request Area #2	Task B13 and B14
evaluate NRC inspection and assessment activities	Funding Request Area #2	Task B16 - B18
evaluate the scope of licensee obligations and those of governmental entities in the event of attacks that exceed NRC's DBT	Funding Request Area #1	Task B2
evaluate the vulnerability of NRC-licensed facilities to attacks that exceed the DBT	Funding Request Area #1 and #2	Task B3
evaluate policies and procedures relating to the protection of critical NRC infrastructure, including both headquarters and regional offices	Funding Request Area #4	Task C2-C7 and Task C15-C17
evaluate the capability for handling and processing classified information in the IRCs including capabilities for making physical modifications for classified briefings	Funding Request Area #4	Task C4 and C10
evaluate the capability to transmit classified information in a timely fashion to appropriate State officials and licensee facilities with the need to know	Funding Request Area #4	Task C11 and C12
evaluate the agency's organizational structure, staffing and training in the security and safeguards area	Funding Request Area #4 (limited)	Task C13 and B15 (limited) [1]

Chairman's Memo to the EDO	Supplemental Funding Request	Proposed Course of Action
evaluate the policies, procedures, and regulations related to the control of the availability and access to information having safeguards and security implications regarding licensed activities	Funding Request Area #5 (limited)	Task C9 - C12
evaluate the agency's emergency response planning, staffing and training for handling protracted events	Funding Request Area #4	Task C13 and Task C5 - C8
establish coordination and communication with other Federal agencies, State and local governments, and licensees	Funding Request Areas #1, #4, and #5)	Task A1, A5 - A6
establish communication with the press, public, and interested parties, as appropriate	Funding Request Area #5	Task A5 - A6
Issues not listed in the Chairman's Tasking Memo		
MC&A	N/A	Task B4 - B19
MOX	N/A	N/A
Future Licensing Activities	N/A	N/A

Notes:

1. Task B13 addresses staffing and training in the safeguards and security areas. Evaluation of the NRC's organizational structure is being conducted separately from this course of action.

ATTACHMENT 7

Details of the Policy Issues (U)

NOTE: POLICY ISSUE # 4 CONTAINS ATTORNEY — CLIENT INFORMATION
LIMITED TO THE NRC UNLESS THE COMMISSION DETERMINES OTHERWISE

POLICY ISSUE # 1
Boundary Between Private/Government Security Responsibility

Issue:

What processes, protocols and arrangements are necessary to ensure an effective response to threats by licensees, local, State, and Federal agencies? Would these new arrangements require modifications to, or deletion of, 10 CFR 50.13?[1]

Sub-issues:

1. How do the threat characteristics and protective measures vary between classes of licensed facilities and activities?

2. How much should licensees contribute to protection of their facilities and activities against terrorists?

3. What balance should be achieved between risk avoidance and risk mitigation in protecting against radiological sabotage? Or against theft and diversion?

4. How can comparability in protecting similar materials at NRC-licensed and Department of Energy owned facilities best be achieved?

Background:

Current Requirements and Responsibilities

In order to examine new or modified processes to ensure an effective response to the current threat, an understanding of our current process is necessary. The current concept for protecting NRC licensed facilities is based on: (1) performance-based measures for protecting against a designed threat[2], (2) providing security measures based upon prescriptive regulations

---

[1] 10 CFR 50.13 - Attacks and destructive acts by enemies of the United States; and defense activities, reads: "An applicant for a license to construct and operate a production or utilization facility . . . is not required to provide for design features or other measures for the specific purpose of protecting against the effects of (a) attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other person, or (b) use or deployment of weapons incident to U.S. defense activities."

[2] 10 CFR 73.1 - Purpose and scope, reads: "(a) *Purpose.* This part prescribes requirements for the establishment and maintenance of a physical protection system which will

rather than a designed threat at certain licensed facilities, and (3) not requiring licensees to provide protection against acts by "an enemy of the United States . . . or use or deployment of weapons incident to U.S. defense activities."

(1) In the 1970s, the NRC determined that certain facilities and activities should be protected against attacks by adversaries within an envelope of potential threats described as the design basis threats[3] in 10 CFR 73.1. These facilities and activities included nuclear power reactors, facilities that fabricate nuclear fuel using weapons usable uranium and plutonium, and transportation of weapons usable nuclear fuel.

(2) For other facilities, the NRC determined that a prescriptive regulatory approach was sufficient and preferable compared to the performance-based approach described above because of reduced consequences of successful attacks on the facilities. These facilities and activities included low-enriched fuel fabrication facilities, enrichment facilities, non-power reactors, spent fuel transportation and storage in dry casks, users of radioactive materials, and other facilities and activities. This regulatory approach resulted in such diverse protection requirements as simply locking up a source to a full armed response strategy.

(3) The agency determined that there were some threats against which the licensee alone could not protect. NRC regulations exempt nuclear power plants from being designed to protect against attacks by "enemies of the United States." This regulatory approach began to evolve in 1967, a few years after the Cuban Missile Crisis. During the licensing of Florida Power and Light's Turkey Point nuclear power reactor, parties in the licensing proceeding raised an issue regarding responsibility for measures to protect against acts by enemies of the United States, due to the plant's proximity to Cuba, or against accidents from the use or deployment of weapons incident to U.S. defense activities. The Atomic Energy Commission (AEC) codified its resolution of the issue in the position currently stated in 10 CFR 50.13. The AEC determined that while the applicant must address physical security for sabotage protection, it was not responsible for protecting against attacks by "an enemy of the United States." However, a clear

---

have the capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used. The following design basis threats, which were referenced in ensuing sections of this part, shall be used to design safeguards systems to protect against acts or radiological sabotage and to prevent the theft of special nuclear material. Licensees subject to the provisions of §72.182, §72.212, §73.20, §73.50, and §73.60 are exempt from §73.1(a)(1)(i)(E) and §73.1(a)(1)(iii)."

[3] DBT has been a hypothetical threat used to develop physical protection systems and provide a standard for evaluation of implemented physical protection programs. Associated DBT attributes are typical of actual adversary attributes that could reasonably be expected, but are not worst case.

definition of enemies of the U.S. was not provided. Likewise, protocols with the defense establishment and various other governmental agencies having the internal security responsibilities for protecting against enemies of the State were not established by the AEC. It should also be noted that this resolution and position seems to have focused on "who" the threat was, rather than "what" the threat was.

As a result, requirements for coordination between licensees and governmental agencies relating to response to threats are substantively limited. Generally, current regulations require the establishment and documentation of liaison with local law enforcement authorities, communications capabilities to law enforcement authorities, integrating the licensee response with the response of other entities, listing available law enforcement authorities and their response capabilities, and informing law enforcement authorities of a threat and requesting assistance.[4] (Note: although the citations listed relate to power reactors, the requirements for Category 1 Fuels Facilities are similarly limited.) Although not required, liaison between nuclear utilities and the FBI has become widespread over the last several years. The staff notes that although § 221b of the AEA assigns the FBI the responsibility for investigation of criminal violations of the AEA and ERA, it does not assign the FBI responsibility for protecting the facility.

Current Design Basis Threat Development

The legislative history of the Energy Reorganization Act of 1974 (ERA), and the Act itself, reflect Congressional concern that the public be adequately protected by safeguards against the consequences of nuclear theft and sabotage. The Act directed the agency to make provisions for and maintenance of safeguards against threats, thefts, and sabotage relating to special nuclear material, and assessing the need for, and the feasibility of, establishing a security agency within the NRC for the performance of the safeguards functions. This last requirement had its genesis in several earlier studies and in subsequent congressional hearings in which substantive questions were raised concerning the adequacy of safeguards, such that, in the interest of public health and safety, prudence might call for direct Federal involvement in security forces. The NRC completed its study in 1976 concluding that the creation of a federalized security force would not result in a higher degree of guard force effectiveness. The NRC determined that it could fulfill its responsibilities to assure adequate physical protection through stringently enforced regulations. Absent a record of attacks on nuclear facilities, the Commission concluded that the use of design basis threats was appropriate. In a manner analogous to the structure of nuclear safety regulation, certain licensees were required to

---

[4]10 CFR 73.55, Appendix C to Part 73 - Licensees Safeguards Contingency Plans. "The goals of the licensee safeguards contingency plans . . . are: . . . (3) to ensure the integration of the licensee response with the responses by other entities." Also, the "Licensee Planning Base" must include under "(d) Law Enforcement Assistance - A listing of available law enforcement agencies and a description of their response capabilities and their criteria for response; and a description of working agreements or arrangements for communications with those agencies."

develop security programs to provide high assurance of protection against the design basis threat (DBT).[5] The plant security plans were based on the premise that onsite protection systems and security personnel must have a high probability of providing protection for a period of time, while reinforcements get to the scene. The NRC presumed that responsibility for neutralizing immediate threats resided in local law enforcement agencies.

The NRC established the design basis threat statements for two types of threats involving two categories of licensees. They were defined in 1977 as radiological sabotage and theft or diversion of strategic special nuclear material.[6] The DBTs were based on extensive analyses of actual terrorist characteristics that were commonly demonstrated and could reasonably be expected in an adversary, on experienced analytical judgement, and on Intelligence Community assessments. Although history is not a reliable predictor of future behavior, it can assist current deliberation and decision making.

Additionally, the need for comparability between the DOE and NRC in threat policy and physical protection for similar materials was recognized in a 1974 National Security Council memorandum which noted the importance of ERDA (now DOE) and NRC coordinated safeguards for strategic special nuclear material and was reinforced by the NRC/ERDA Task Force on Safeguards in 1976. In April of 1980 the National Security Council (NSC) requested that the Department of Defense, Department of Energy (DOE), and NRC review their policies regarding threat. In response, the three agencies reviewed the programs and noted differences in threat policy despite comparability in levels of protection for weapons-usable material. With general regard to the level of security at NRC licensed fuel facilities, the NRC and the ERDA established the policy of coordination of design basis threats and threat policy relating to the protection of weapons-usable materials. Following extensive expenditures for safeguards by DOE facilities, in 1986, an NRC/DOE comparability study of physical security systems was conducted of facilities with weapons-usable material. The NRC staff noted that due to the nature of assets held by DOE, which included highly classified Restricted Data that could be the

---

[5] 10 CFR 73.55 - Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage, states, (a) *General performance objective and requirements*. The licensee shall establish and maintain an onsite physical protection system .... The physical protection system shall be designed to protect against the design basis threat of radiological sabotage.

[6] 10 CFR 73.1 - Purpose and scope, defines the DBT for *Radiological sabotage* as having the following characteristics: (1) a determined violent external assault, attack by stealth, or deceptive actions, of several persons with the following attributes, assistance and equipment: (A) Well-trained . . ., (B) inside assistance . . ., (C) suitable weapons (D) hand-carried equipment . . .(E) a four-wheel drive vehicle. The defined DBT for "(2) *Theft or diversion of formula quantities of strategic special nuclear material* " is essentially the same except that it adds (F) the ability to operate as two or more teams, (iii) A conspiracy between individuals in any position . . .

target of espionage and functioning nuclear weapons which terrorists might attempt to steal, the DOE threat policy is broader in scope than the NRC design basis threats. When examining the variety of protected assets within the DOE complex, the agencies jointly determined that the **focus of comparability would be limited** to those DOE facilities that possessed significant inventories of strategic special nuclear material that could be employed in a nuclear device and the two NRC Category I fuel facilities [emphasis added]. Based on the results of this review, in 1987 NRC staff recommended that in order to maintain comparability, the design basis threat for theft should be modified to include the use of a land vehicle by an adversary for transporting personnel and equipment during an attempted theft. Periodically NRC and DOE staff revisit the comparability question and had been discussing the need to conduct a current review during FY 2002 - FY 2003, prior to the September 11 terrorist attacks.

Discussion:

The events of September 11, 2001, revealed a threat that appears different in some respects from the characteristics in the current DBTs. The coordination, modality and consequences of the successful attack on significant targets within the United States highlighted a potential new paradigm for NRC's security program policy and processes, particularly as they relate to the threat.

As was noted above, the statement in 10 CFR 50.13 was developed in the context of the "Cold War" during which there was a belief that attacks on the United States by foreign governments were consistently possible. That paradigm was shifted by the realization that significant damage could be caused to high value and high symbolic targets in the United States from enemies not clearly affiliated with another government. There was also the realization that an active, efficient, effective large scale threat within the United States, exceeding the capabilities of current protective systems was a reality and not a "design basis.' For example, it was never clearly envisioned that a key characteristic of the threat was the use of a large commercial airliner as a weapon. The new paradigm focused not only attention on the fact that some protective systems were vulnerable, but also that several other NRC licensed nuclear facilities were not required to provide any security based on countering a threat, past or present. The NRC also recognized that some facilities, especially nuclear power plants and fuels facilities, were already capable of protecting against many of the characteristics of the active threat. This was the result of our coordinated threat analysis, regulatory footprint, and pro-active field assessments of performance.

During the hours and days immediately following September 11th, the NRC, as did almost every other local, State and Federal agency, took action to address the increased threat. Although there were no specific threats to NRC-licensed facilities, the NRC advised its licensees to establish additional security measures. These advisories were implemented as prudent measures to protect against the apparent characteristics of the active threat. Also, the NRC established temporary working arrangements and communication links with various intergovernmental entities because some characteristics of the current threat were beyond the

licensees' ability to provide full protection. Licensees of nuclear plants, fuels facilities, non-power reactors and large radio-pharmaceutical manufactures all developed temporary protocols and communications links with the Federal Aviation Administration. NRC and some of its licensees have also developed temporary working communications links with the North American Air Defense Command (NORAD), and armed military aircraft have patrolled airspace over the United States and have responded to perceived threats at nuclear power plants. The U. S. Coast Guard actively patrolled waters off nuclear facilities for a period of time and developed contacts at plants as appropriate. Several States called out and posted National Guard units at nuclear plants, while at others, State Police officers worked next to licensees' armed guards.

These arrangements were formed from the recognition on the part of several agencies that characteristics of the threat must be addressed. It was made clear that licensees alone could not protect against all of the threat characteristics demonstrated on September 11, yet those threats were demonstrated within the United States. It was also recognized that other licensed nuclear facilities and activities required protection.

Changes to our processes and regulations may be needed, as well as, better delineation of the boundary between private and government protection responsibilities.

Proposed Strategy

The staff developed a proposed methodology that responds to this issue (see Fig. 1-2: Recommended Methodology for Resolving Government/Private Responsibility). The methodology is divided into two parts, immediate and longer-term. The immediate methodology begins with an analysis of the September 11 event and extrapolation of threat information to determine a reasonable representation of the current environment (Attachment 10) for which a cooperative response of licensee, local, State, and Federal assets would be necessary to adequately protect public health and safety. The threats included in this environment are those that have been seen utilized or attempted in domestic and foreign environments. The developed threat will be filtered through the experience and training of the practical expertise of our NRC contractors, or other individuals experienced in the practicalities of counter-terrorist operations. This adds to the accuracy of our process by ensuring that commonly used techniques will not be overlooked and adds credence by providing a check and balance regarding the threat characteristics identified. This will also provide an opportunity for determining which threat characteristics are applicable to each class of licensee or class vulnerabilities. The NRC would then apply screening criteria to determine licensee responsibilities and necessary interim compensatory measures that will provide adequate public health and safety protection while a more methodical and thorough review is conducted. The X-threat and proposed division of responsibility are then provided to the Commission for consideration and integration with other intergovernmental entities. Following deliberation, the Commission would impose interim measures through appropriate regulatory means.

The longer-term review would include a reasonable postulation of threats and a determination of associated consequences. Once the threat is established, the specific characteristics (e.g., numbers, weapons, tactics, training, intelligence gathering, etc.) of that threat will be identified. Those specific and tangible characteristics would then be applied to screen each type of facility or activity to determine what vulnerabilities are evident. An assessment of the technical feasibility, commercial capability, and possible mitigative strategies that can be employed would also be determined. A revised screening process would be developed to determine a reasonable DBT for each facility class or a determination that prescriptive requirements are more appropriate to the particular licensee operation (e.g., transportation). Those characteristics that were determined to be beyond the licensee's capabilities would be evaluated to determine which local, State or Federal resources could be effective. (See Fig. 1-1: NRC Coordinate Response Strategy). This information would then be provided to the Commission for review and consideration. The spectrum of threats would then be shared with other Federal entities for coordination and critique. NRC would seek alignment and agreement on appropriate protocols to ensure a comprehensive response strategy. Should no agreements be reached or should protective measures not be available, the Commission would then need to determine whether the risk associated with that threat characteristic(s) should be assumed as acceptable or not.

Guidance Sought from the Commission:

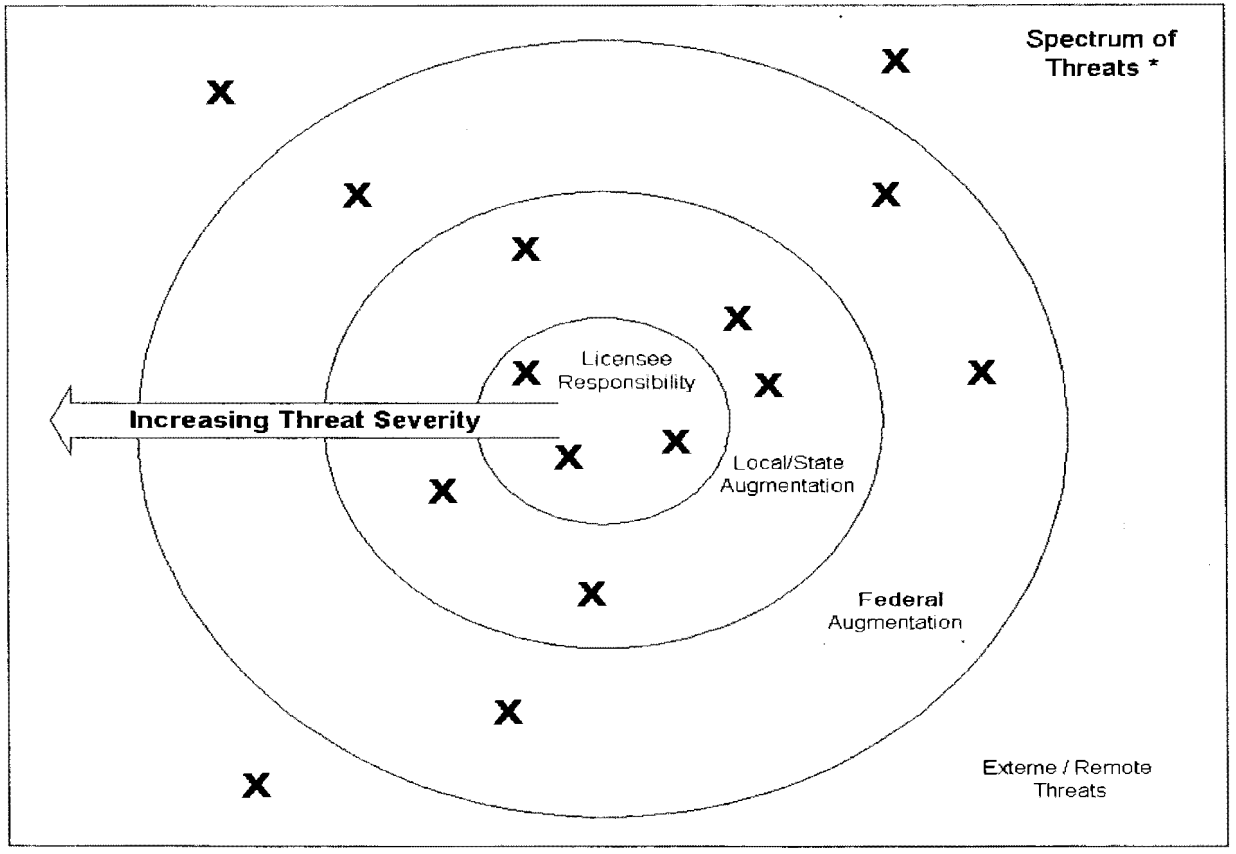
The staff will provide any further detailed information associated with the following issues, if requested by the Commission. The Commission is requested to provide guidance as to:

1. Whether the staff should implement the modified threat assessment approach (as described above) to clearly identify which characteristics of the threat are within licensee's capabilities, and which are not.

2. Whether the staff should revisit the 1976 decision on Federalization of NRC-licensed power reactor security forces?

3. Whether 10 CFR 50.13 should be modified or reinterpreted to reflect a clear delineation of responsibilities for those characteristics beyond the capabilities of a licensee to protect. Whether similar regulations should be written to delineate division of responsibilities for other NRC-licensed facilities.

Figure 1-1:
NRC Coordinated Response Strategy



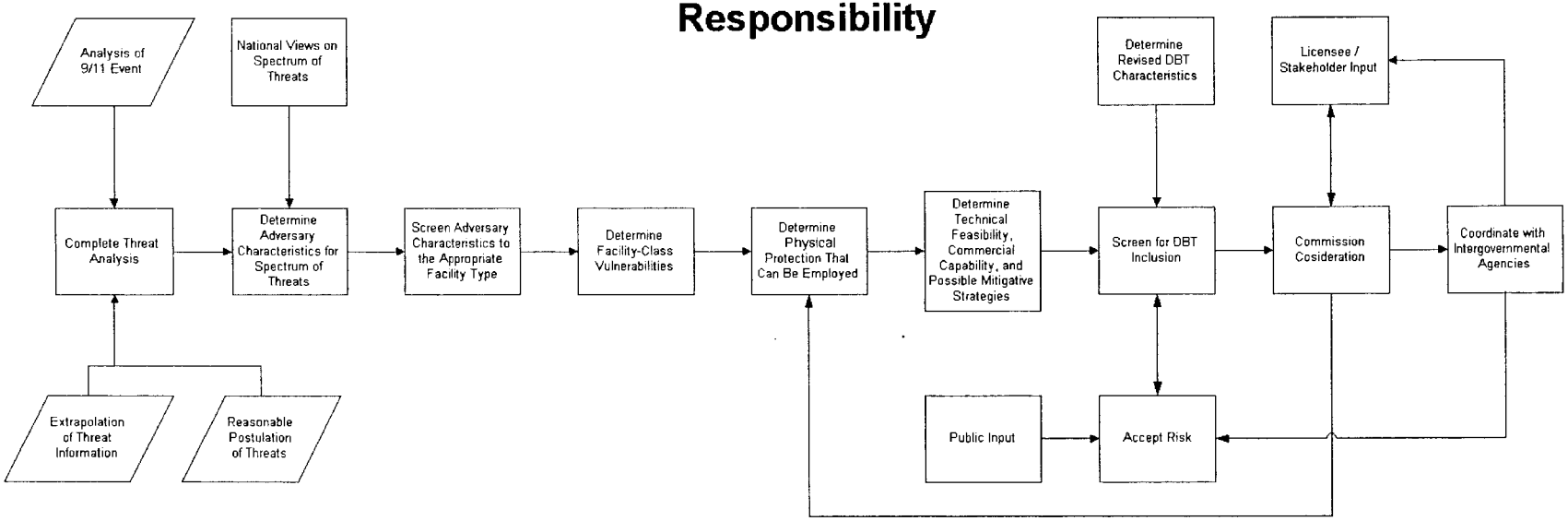
Details of Approach

Refer to Figure 1-2: "Recommended Methodology for Resolving Government / Private Responsibility"

x = postulated threat

* Area of Responsibility varies with Class of License

Figure 1-2:
Recommended Methodology for Resolving Government/Private Responsibility



POLICY ISSUE # 2
NRC Role and Interface in National Infrastructure

Issue:

Should additional NRC-licensed activities be protected as part of the nation's critical infrastructure, and if so, what role should the NRC play in defining and protecting that critical national infrastructure?

Sub-issues:

1. How do licensed activities factor into minimum operations of the economy and government?

2. Would destruction of NRC licensee activities have a sufficient impact on the National infrastructure (e.g., medical diagnostic capabilities and treatment of disease, including cancer, widespread soil contamination, closing nearby businesses or transportation routes, etc.)?

3. What benefit to ensuring public health and safety would result from NRC taking a more central and vocal leadership role in the National Infrastructure process?

Background:

During the first months of NRC's existence (January 1975), a study group was created under the direction of the National Security Council to examine the issue related to whether NRC licensees were "national assets." The study group was chaired by the Energy Research Development Administration (ERDA), with representatives from the Departments of Defense, Justice, and State. The NRC participated as a consultant.[7] The discussion on "national assets" came during deliberations involving the protection of "sensitive safeguards information."

In response to the efforts of the study group, Chairman Hendrie wrote, "While this information [security information relating to nuclear power plants] is no less worthy of protection in the interest of public health and safety, its relationship to the national security is of a different character."[8] The consequence of those deliberations was that the group determined that

---

[7] Commission Paper (SECY-78-347, unclassified version) entitled, "Classification of Sensitive Safeguards Information (Implementation of NSDM-347)" (August 1978).

[8] Letter to Senator Gary Hart, Chairman, Subcommittee on Nuclear Regulation, Committee on Environment and Public Works, from Chairman Joseph M. Hendrie, dated August 2, 1978.

nuclear power plants were not significant with respect to protecting "national security," and safeguards information (security and material control and accountability information) could not be classified. However, information relating to military and foreign relations material at Category 1 fuels facilities was considered National Security Information and was classified. The idea that NRC licensees contributed to the national economy was not considered at that time.

The situation remained unchanged until world events focused attention on terrorist acts. Presidential Decision Directive (PDD) 39 was issued in June 1995.[9] The document included what effectively amounted to an internal look at industrial resources in the United States as potential terrorist targets. For example, it addressed the Federal Aviation Administration's responsibility relating to "air piracy" and introduced the Federal Emergency Management Agency's role on consequence management resulting from the use of weapons of mass destruction. The directive did not address NRC licensed activities.

President Clinton initiated additional action in 1998 when he issued PDD 62 and PDD 63, concurrently.[10] [11] PDD 62 called for a more systematic approach to combating terrorism. It established the Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The Coordinator was to work through the National Security Council. The Office was to oversee a broad variety of relevant policies and programs, including protection of critical infrastructure. Its focus was on coordinating the means to prevent terrorist acquisition of weapons of mass destruction; consequence management for terrorist incidents; and, protection of critical infrastructure and cyber systems.

PDD 63 provided one of the first working definitions of "critical infrastructures." Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, banking and finance, transportation, water systems, and energy services, both governmental and private. PDD 63 also sets national goals relating to the protection of that national infrastructure; mentions the public-private partnership needed to reduce vulnerabilities; and establishes a structure and organization within which goals may be

---

[9] Presidential Decision Directive 39 entitled "United States Policy on Terrorism," (unclassified version), dated June 2, 1995.

[10] Presidential Decision Directive 62, "Combating Terrorism," dated May 22, 1998 (Fact Sheet).

[11] Presidential Decision Directive/NSC-63, "Critical Infrastructure Protection," dated May 22, 1998.

achieved.[12] The organization specifies the Department of Energy as the "Lead Agency" for the entire "electric power" sector of the economy. It does not specifically mention the NRC nor NRC-licensed activities.

NRC staff has taken a pro-active approach in developing DOE contacts regarding PDD 63 and has had periodic meetings with DOE since late 1998, when the staff initiated informal contacts with the DOE Sector Liaison Official.

As PDD 62 and PDD 63 focused primary attention on "critical infrastructure" elements external to government operations, the publication of PDD 67 in October 1998 focused attention primarily inward.[13] It relates to the government's continuity of operation planning (COOP) and continuity of government (COG) operations. PDD-67 required federal agencies, including the NRC, to develop internal plans to ensure the continuity of essential functions, succession to office, delegation of authority, safeguarding of essential governmental resources and records and establishing emergency operating capabilities. In response to PDD-67, an interoffice working group produced the NRC's Plan for Continuity of Operations (COOP).[14] The effective implementation of that plan has continued to the present. The NRC's plan identifies the minimum essential agency functions. It also indicates that the internal NRC function that relates to the external "power infrastructure" is "Functions necessary to assist licensees in safe maintenance and restoration of power production at sites where there is no immediate safety problem; assist the Federal Emergency Management Agency (FEMA) and the Department of Energy."

During a hearing before a joint Senate committee on efforts to combat terrorism on May 8, 2001, and in a letter to Vice President Cheney on June 15, 2001, Chairman Meserve articulated the need to more fully acknowledge NRC's role in combating terrorism.[15]

In July 2001, the Office of Management and Budget requested comments on a proposed Executive Order entitled "Critical Infrastructure Protection in the Information Age." Although NRC comments were not specifically requested, we provided them by letter dated July 30, 2001. Chairman Meserve suggested that the NRC be allowed to appoint a member to the Critical Infrastructure and Continuity Board.

---

[12] "White Paper: The Clinton Administration's Policy on Critical Protection: Presidential Decision Directive," dated May 1998.

[13] Presidential Decision Directive PDD-NSC-67, entitled "Enduring Constitutional Government and Continuity of Government Operations," dated October 21, 1998.

[14] NRC's "Plan for Continuity of Operations (COOP), dated November 1999.

[15] Letter to Vice President Cheney from Chairman Meserve entitled, "Federal Response to Terrorism," dated June 15, 2001.

On September 24, 2001, a bill (S.1456) was introduced in the U.S. Senate that is intended to facilitate the security of the critical infrastructure of the United States . . ."[16] Section 4 of the bill provides an updated definition of "Critical Infrastructure." It "(A) means physical and cyber-based systems and services essential to the national defense, government or economy of the United States, including systems essential for telecommunications (including voice and data transmission and the Internet), electrical power, gas and oil storage and transportation, water supply, emergency services (including medical, fire, and police services), and the continuity of government. (B) includes any industry sector designated by the President pursuant to the National Security Act of 1947 (50 U.S.C. 401 *et seq.*) or the Defense Production Act of 1950 (50 U.S.C. App 2061 *et seq.*) as essential to provide for the execution of the national security strategy of the United States, including emergency preparedness activities pursuant to title VI of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5195 *et seq.*)." This bill also identifies "covered Federal agencies" and lists the Department of Energy, but as in the past, does not list the NRC.

Discussion:

The Licensed Nuclear Industry as Infrastructure:

As noted previously, critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government.

Almost concurrent with the birth of the NRC in 1975, a national security group, chaired by ERDA with representatives from the Departments of Defense, Justice and State, determined that power reactors were not significant with respect to protecting national security. However, information relating to military and foreign relations material at Category 1 fuels facilities was considered relevant to national security. Those determinations appear to have been made with little NRC participation, and were based on a discussion of classification of information, and not on the significance of the activities to the operations of the economy and government.

In the 1990s, the Federal government placed increased attention on protecting our critical national infrastructure at its most vulnerable points, including computer systems. That attention included power plants (of all types). In addition, as the nuclear industry consolidated in the 1980s and 1990s, the fuel cycle became increasingly vulnerable to interruption as the number of critical and unique activities such as conversion and enrichment facilities were reduced.

NRC licensed activities that represent unique components of the nuclear fuel cycle, include one conversion plant, two gaseous diffusion plants, and two fuel fabrication plants that produce fuel for use by the Department of Defense. The NRC also licenses other activities such as radio-

[16] Proposed Senate bill S.1465 dated September 24, 2001, cited as the "Critical Infrastructure Information Security Act of 2001."

pharmaceutical manufacturing, transportation of radioactive material, and storage of high level radioactive waste which, if interrupted or destroyed, could have an adverse impact on several aspects of our society.

The residual consequences of a successful terrorist attack on licensed nuclear activities could also have a significant indirect impact on our national infrastructure. The NRC licenses 103 operating power reactors. The nuclear power generation industry produces a significant amount of the electrical energy used in the U.S. The loss of a single operating reactor may have no significant impact on the national power grid. However, radiation releases resulting from a successful act at an operating power reactor could contaminate large areas for long periods disrupting other portions of our national infrastructure such as commerce, transportation, agriculture, water supplies, etc. Additionally, some activities (such as large irradiators) licensed by NRC possess or produce material that could be used as, or in deploying, radiological dispersal devices, which could be considered "weapons of mass destruction." The destruction of NRC licensed or Agreement State materials facilities might have a significant impact on the personal heath services industry. Certain other licensed activities are involved in processing material from foreign countries and their destruction might impact U.S. foreign affairs. Each of these areas can be construed as relating to activities "essential to the minimum operations of the economy and government." (emphasis original).

NRC's Role in Policy Development and Protection:

During the 1970s, a national security group was formed to examine whether certain information relating to NRC licensed activities should be classified. That determination would be based on their significance to "national security." The group was chaired by ERDA and included representatives from the Departments of Defense, Justice and State. Those determinations appear to have been made with peripheral NRC participation, and were based on the "national security" significance, rather than on the significance of the activities to the operations of the economy and government. That process appears to have been carried forward through the 1980s and into the early 1990s with little change in or challenge to NRC's role.

However, beginning in the 1990s the threat environment changed and terrorist acts became more deadly. Elements of our nation's infrastructure increasingly became targets of terrorists. Examples included the bombing of Pan Am Flight 103 in late 1991, the World Trade Center truck-bombing in early 1993 and the truck bomb which destroyed the Federal Building in Oklahoma City.

Efforts to combat terrorism by the Federal Government escalated throughout that period. However, not until PDD 39 was issued in June 1995 was a formal and structured program drawn together. The document included what effectively amounted to a call for an internal look at resources in the United States as potential terrorist targets, and defines terrorism as a potential threat to "national security" and a criminal act. It did not define critical infrastructure,

and only mentions Department of Energy as playing a role in providing technical expertise for event response.

In October 1997 the President's Commission on Critical Infrastructure issued its report calling for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures, such as telecommunications, finance and banking, transportation, energy and essential government services. As a follow on, PDD 62 and PDD 63 were issued. PDD 62 called for a more systematic approach to combating terrorism. PDD 63 draws together interagency efforts to evaluate those issues and produce a workable framework for critical infrastructure protection. PDD 63 states that the Federal government should serve as a model to industry on how best to protect its own private sector elements of the critical infrastructure. It designated GSA as the Federal agency responsible for coordinating activities to improve infrastructure protection.

PDD 63 also identifies eight agencies as "Tier One" agencies. The Department of Energy was designated as the Lead Agency for the energy sector. As the Lead Agency, DOE was directed to work with the private sector to address problems related to critical infrastructure protection. PDD 63 also directs Lead Agencies to identify a Sector Coordinator from the private sector to represent the views of industry in joint infrastructure protection efforts; the North American Electric Reliability Council (NERC) agreed to be the [private] Sector Coordinator for energy. NERC assumed the role of the energy sector's Information Sharing and Analysis Center (ISAC), which collects information on cyber threats from power utilities and forwards information to the National Infrastructure Protection Center (NIPC).[17]

In October 1998, GSA informed the NRC that the NRC and several other agencies had been inadvertently omitted from the list of agencies required to respond to PDD 63. Later, GSA designated the NRC as a "Tier Two" agency. By letter dated October 30, 1998, Chairman Jackson requested that "Tier Two" agencies also submit a Critical Infrastructure Plan (CIPP) and we subsequently respond to GSA with a plan to protect NRC's internal infrastructure. (See footnote 11). We completed that effort on May 26, 1999 with the submittal of NRC's "Critical Infrastructure Protection Plan." The plan was revised and updated in October 2001. This plan primarily looks inward as directed by PDD-63.[18]

PDD 63 specifies the Department of Energy as the "Lead Agency" for the infrastructure sector "electric power." The Directive does not acknowledge the unique emergency response, oversight, and communications relationships that the NRC has with the nuclear industry.

---

[17] SECY-01-0042, "Agency Response to Presidential Decision Directive 63," dated May 15, 2001.

[18] "United States Nuclear Regulatory Commission "Critical Infrastructure Protection Plan (CIPP)," revised May 26, 1999, and updated in October 2001.

Consequently, most of the NRC staff's efforts relating to national infrastructure have been focused on internal NRC matters, such as protection of the NRC's computer assets against cyber-attack.

NRC staff has taken a proactive approach in developing DOE contacts regarding PDD 63. NRC staff has had periodic meetings with DOE since late 1998, when the staff initiated informal contacts with the DOE Sector Liaison Official. Since then the staff has maintained that informal contact with DOE on this issue. There were no defined activities for the NRC in support of DOE in their role as Lead Agency for the energy sector. As of March 15, 2001, DOE had issued no formal tasks to NRC.

Throughout this period, the NRC continued to be actively engaged with our licensees in efforts to ensure that our licensees were providing adequate protection. We have conducted an active inspection and evaluation program aimed at identifying and correcting deficiencies in on-site security, while improving our involvement in emergency response activities. During the last 25 years, NRC has developed, implemented and improved upon communications protocols, oversight processes, unique technical expertise and relationships with the private nuclear industry that are valuable to addressing potential national infrastructure issues, including security.

Guidance Sought from the Commission:

1. The Commission is requested to provide guidance regarding the degree to which the NRC should play a more direct and substantial role in shaping national policy regarding protection of NRC licensees and Agreement State activities as critical infrastructure.

2. The Commission is requested to provide guidance as to whether the staff should proceed in developing the bases for including additional NRC-licensed facilities/activities as elements of the critical national infrastructure.

3. The Commission is requested to provide guidance as to whether the staff should reassess the agency's position on whether the NRC's internal infrastructure is critical.

POLICY ISSUE # 3
Balancing National Security Interests With Public Information Needs

Issue:

To what degree should information that may be potentially helpful to an adversary, and is currently in the public domain or created in the future, be restricted from public access and how should this be done? How should the agency balance the need to protect such information with fulfilling the agency's public access mandates? What role does public access to information play in fulfilling the agency's goals in encouraging public participation in the regulatory process? To what extent and under what processes should stakeholders be involved in the agency's comprehensive review?

Sub-issue:

- Should the Commission consider the degree to which meaningful public involvement in the regulatory process can be most effectively obtained or reconsider the NRC's current public participation policy, in light of the security restrictions due to the current threat environment?

Before September 11, on most important NRC initiatives, the agency would have sought to engage all stakeholders in the process through a variety of forms of participation to factor public comments into the decision making process and to increase public confidence in the ultimate course of action. We could expect active involvement from Federal agencies, States, and regulated parties as well as members of the public in these processes. The review suggested here does not limit our continued interaction with stakeholders, but encourages consideration of other options while maintaining awareness of any national security implications.

As discussed in this paper, the staff anticipates that the agency will, among other things:

- continue developing safety evaluation reports, environmental impact statements, inspection reports, enforcement actions, and other documents in support of our decision making process
- continue its interactions with Federal agencies, States, regulated parties, foreign regulators and other international bodies
- continue routine and extraordinary communications with Congress
- gradually return appropriate information to the NRC's external Web site
- continue responding to inquiries from the media and public

- address terrorism issues raised in adjudications
- expect additional interactions with and requirements from other U.S. government departments, agencies and entities created as result of the September 11 event like the Homeland Security Council and Office, and
- respond in some fashion to requests for action (i.e., petitions) submitted under 10 CFR 2.206

Background:

The staff believes the combination of planning, coordination, and execution capabilities, demonstrated by the terrorists who perpetrated the September 11 attacks, and the usefulness of current publicly-available information to an adversary's threat analysis, target identification, and vulnerability analysis process, necessitate a fundamental reconsideration of what information is considered "sensitive" and should not be publicly available. This reconsideration must also take into account the fact that a large amount of "sensitive" information, as defined under threat criteria, is already in the public domain and the potentially significant costs associated with removal of this information. However, the staff also believes that this issue should be viewed in the context of a long-term information protection policy and that while short-term vulnerabilities may exist, they should not have a long term impact on our nation's security. Accordingly, the NRC staff intends to undertake a systematic reevaluation of what information should be made publicly available and what information should be restricted from public disclosure. This issue paper addresses the bases for such actions along with balancing those actions with other NRC requirements to provide stakeholders with access to information in order to participate in a meaningful way in the regulatory process. This paper also raises the question of the significance of broad public access to "sensitive" information in enhancing public confidence in and understanding of our safety and security missions.

The NRC's statutory requirements include protection of information from disclosure — National Security Information (NSI), Restricted Data (RD), and Safeguards Information (SGI) — under the National Security Act of 1947 and the Atomic Energy Act of 1954 (AEA). Federal statutory requirements also require the NRC to provide the public with access to information, with certain exceptions, e.g., 1) providing public access to information - the Freedom of Information Act (FOIA), 2) conducting its business in public — the Government in the Sunshine Act (GISA), and 3) providing public access to recommendations from non-government entities — the Federal Advisory Committee Act (FACA). Additionally, the NRC has established a Public Confidence performance goal for stakeholders to view the NRC as an independent, open, efficient, clear, and reliable regulator by providing stakeholders with clear and accurate information about, and a meaningful role in, our regulatory programs.

For processes covered under the Administrative Procedure Act, such as rulemaking or adjudicatory hearings, public access to a minimal set of information is prescribed. For rulemakings, the Commission may include such explanatory statements (i.e., the technical and regulatory bases) as it deems appropriate [see 10 CFR 2.804(b)(6)]; however, all such explanatory material and regulatory analyses are equally available to any interested person. For adjudicatory hearings, protective orders may be used to permit parties to the hearing to review "sensitive" information, while protecting the information against disclosure.

NRC Management Directive 3.4 identifies the types of information that are prohibited from public disclosure (e.g., classified or SGI information), are not routinely released to the public for policy reasons (e.g., legal work products), and are routinely released to the public. The bulk of the information submitted to or generated by the NRC is routinely released to the public. Typical publicly-available information has consisted of license-application material (e.g., safety analysis reports and environmental reports) or NRC-generated material (e.g., safety evaluation reports, inspection reports, and enforcement actions). This information now resides in various records systems, including the NRC Public Document Room (PDR), the Nuclear Documents System (NUDOCS), the Agencywide Documents Access and Management System (ADAMS), public libraries (former local PDRs), federal document repositories, and other federal agencies [e.g. the Library of Congress, the Government Printing Office (GPO), and the National Technical Information Service (NTIS)]. Additionally GPO's and NTIS' missions include the selling of NRC documents (e.g., NUREG reports and the entire "48X" microfiche collection). This widespread dissemination of information was part of the NRC's effort to facilitate stakeholder participation and, as a byproduct, public confidence in the NRC's regulatory process. The staff has developed initial guidance for identifying what types of information should be released to the public and has provided this guidance to the Commission for review.[19] Furthermore, a significant quantity of the NRC's previously released information is now on third-party Web sites.

Historically, the NRC has classified limited quantities of information as either NSI or RD (e.g., Category I fuel facilities, Naval Nuclear Propulsion Information, or Navy spent fuel shipping containers). Larger quantities of information have been controlled as SGI (e.g., physical protection information for power reactors and transportation of spent fuel and programs for material control and accounting).

Discussion:

Traditionally, the NRC has been philosophically committed to openness in providing the public with access to information relating to NRC-licensed facilities and activities as it performs its regulatory functions. The NRC has used the term "stakeholders" to identify persons with an

---

[19] COMSECY-01-0030, "Guidance to the Staff on Release of Information to the Public," dated October 29, 2001.

interest in the NRC's regulatory actions. Stakeholders include the general public, Congress, NRC licensees, other Federal agencies, States, Indian Tribes, local governments, industry, industry workers, technical societies, the international community, and citizen groups. These stakeholders have relied on information provided by the NRC to raise safety and security concerns to the NRC on proposed and existing facilities (e.g. in licensing hearings (both initial issuance and amendment of licenses and in 10 CFR 2.206 petitions). The staff anticipates that, in the interim, the NRC will continue to interact with stakeholders in those forms of participation required by law or long-standing policy. To this end, the staff notes that discussions with stakeholders of this proposed course of action and early interactions with stakeholders in developing regulatory changes which result from this course of action may be beneficial. These interactions will of course be governed by the need to protect NSI, SGI, and sensitive information. Every opportunity to increase involvement with other Federal departments and agencies should also be considered to allow us to benefit from the experience others have in addressing similar issues as well as providing our agency with a sense of national direction being considered by officials with oversight responsibility. Consequently, because of the NRC's openness policy, there may be objection (including possible legal action) to curtailing access to information. However, in light of the terrorists' capabilities demonstrated in planning for the September 11, 2001, attacks, the staff believes the NRC must redefine the type of information that could be useful to an adversary planning an attack or sabotage and balance protection of that information against the public's right or need to know information relative to plant and activity safety or other pertinent matters.

Furthermore, the length of time assumed for some NRC processes (e.g., license renewal) are predicated upon public access to the underlying information (e.g., a license application or an environmental report). For example, protecting substantial parts of a license renewal application or the licensee's existing final safety analysis report (FSAR) as sensitive information and restricting access would have an impact on the public's ability to review the application and could further affect the assumptions on the length of time necessary for the NRC to conduct reactor license renewal proceedings.

Any person can use the FOIA process. A number of considerations should be taken into account when deciding on a strategy in order to withhold information subject to FOIA. Legal authority must be found in one of FOIA's 9 exemptions from disclosure. Similarly, GISA has its own exemptions patterned closely after FOIA. FACA expressly relies on FOIA for withholding authority. The NRC has previously protected NSI from disclosure under exemption 1, SGI under exemption 3, and 10 CFR 2.790(d)(1) information [i.e., sensitive safeguards information not explicitly listed under 10 CFR 73.21] under exemption 4. However, practical and legal difficulties arise when attempting to protect or retrieve information currently available in the public domain.

NSI is protected from unauthorized disclosure under Executive Order (EO) 12958,[20] where disclosure could harm national security.[21] SGI is protected from unauthorized disclosure under § 147 of the AEA. In classifying information under EO 12958, great deference is given to agency expertise for "unique insights" into applicability. Furthermore, EO 12958 also recognizes "mosaic" or "compilation" theory and authorizes classification for otherwise innocuous pieces of information that, when assembled together, could reveal a damaging picture. Such theory may be useful in a fresh look at information that could be misused for malevolent purposes, although by itself, the information may appear harmless. The NRC has not classified information related to power reactors, and other activities such as transportation of spent fuel, because a nexus had not been shown between these activities and national security [i.e., these facilities or activities did not fall under Category 1.5(e)] [see Policy Issue No. 2 above for further information]. Clearly, a review of that policy may yield a different conclusion.

AEA § 147 explicitly requires protection of information related to: 1) control and accounting procedures or security measures for special nuclear material, 2) security measures for physical protection of certain source and byproduct material, and 3) security measures for the physical protection and location of vital areas in power reactor or production facilities. However, other "sensitive" information for power reactors or other types of NRC-licensed facilities and activities are not covered by this statute or the NRC's implementing regulation in 10 CFR 73.21.

A range of strategies can be pursued by the NRC to ensure that the availability of sensitive information to a potential adversary is minimized. These strategies would involve a broad effort to identify significant information and to remove that information from the public domain and would involve two parallel paths. One longer-term path would involve the staff revising NRC MD 3.4 to reduce the type of information that is routinely available to the public. The second, shorter path would involve the staff applying expanded definitions of NSI and/or SGI to additional sensitive information. In the interim, the staff will continue to review selected information for its sensitivity and removal from public access. Staff has developed criteria for screening and identifying "sensitive" information and is currently using these criteria. Currently, the staff is restricting access to paper and microfiche records in the PDR and having librarians screen public requests. The staff has also been in contact with selected former LPDR libraries, each of which have jurisdiction over the collections they possess, and the GPO to discuss options for removing or restricting access to NRC documents in Federal Government

---

[20] EO 12958, "Classified National Security Information," dated April 17, 1995, as amended by EO 12972, dated September 18, 1995, and EO 13142, dated November 18, 1999.

[21] The NRC principally classifies NSI information under Categories 1.5(f) and 1.5(g). Category 1.5(f) - U.S. government programs for safeguarding nuclear materials or facilities. Category 1.5(g) - vulnerabilities or capabilities of systems, installations, projects, or plans relating to national security. However, classification under Category 1.5(e) also extends to scientific, technological, or economic matters relating to the national security.

Depository Libraries. Options are limited due to GPO policy and the manner in which the NRC stored documents.

Moreover, due to the costs of removal and because some information is not under the NRC's control, some information now considered potentially sensitive may remain publicly available. For example, the staff is aware that NTIS has sold copies of the entire "48X" microfiche collection to at least 18 private subscribers. The 48X collection contains all the Agency public documents from 1981 to 1999 and has over 2 million records. A single record can be an individual page or over a thousand pages. The staff has also identified a list of NUREGs that contain potentially sensitive information and provided this list to external entities (e.g., NTIS and GPO) with a request to restrict these documents from public access. Furthermore, the staff is aware that third party organizations have developed Web sites that contain NRC information. The agency's ability to remove sensitive information from these Web sites is problematic at best and impossible at worst.

Any reconsideration of whether information should be classified as NSI would occur as a follow on to the decisions made in Policy Issue No. 2 in evaluating whether sufficient nexus exists between NRC-licensed facilities and activities and the critical national infrastructure to warrant classification (e.g., electric power generation, naval fuel fabrication, sole source radiopharmaceutical fabrication, or transportation of spent fuel and high-level waste, etc.). Decisions to classify specific types of information would be coordinated with the Office of Homeland Security or Homeland Security Council and the Information Security Oversight Office of the National Archives and Records Administration. Other key federal departments and agencies would be consulted, as necessary. The previous public availability of this information would also be factored into any classification decisions. For example, while EO 12958, section 1.8(c) expressly prohibits reclassification of information after it has been declassified and released to the public, the EO is silent on information that was never previously classified and is currently in the public domain. Finally, subsequent to classification of information as NSI, the staff would implement existing agency requirements to protect information that was critical to national security.

There may only be a small difference in the costs associated with prospective control of future documents and collections between an approach that identifies what information should be restricted from public access versus what information should be publicly available. However, there could be a significant difference in the costs associated with retrospectively implementing these controls for existing collections between an approach that identifies what information should be restricted from public access versus what information should be publicly available. Above a "critical" number of records, identification and removal of sensitive records may not be practicable. Once a "critical" number of records is considered sensitive and must be restricted from public access, permanent removal of the entire existing collections from public access is the only viable option. This decision could be different for federal depository libraries and former LPDRs. In any case, the collections would be subsequently rebuilt over time as new documents are submitted (e.g., a licensee could submit a sensitive and nonsensitive version of

the periodic update of its FSAR). However, such an approach would increase licensee costs and NRC costs to create and handle two documents. Furthermore, permanent removal of the entire collection would likely engender significant opposition from some stakeholders.

In other alternatives, the NRC could work to ensure sensitive information is not consolidated in a small number of locations thereby making it difficult to obtain for a determined, sophisticated adversary over a sustained period of time. Other strategies could involve a strict definition of any information which would reveal any sensitive information or a strategy which removes only the most sensitive of information.

A decision to classify information that is now unclassified would have significant internal and external implications. Internal implications would involve staff (increased resources to respond to FOIA requests and questions from stakeholders), facilities (increased need for secure work space and classified material storage areas), telecommunications (increased need for secure telephones and the need for a secure LAN), and additional staff security clearances, training and oversight to handle, store, process, and communicate a significantly increased volume of classified material. Availability of redacted versions of newly classified documents also would need to be considered. Significant changes to the NRC's business practices and to staff's "cultural mind set" would need to occur. Additionally, State, local, and Tribal government offices, licensees, certificate holders, and applicants would need to establish procedures for hiring staff with security clearances, storage, handling, and communication of classified information. Each of these locations would also require an NRC facility clearance under 10 CFR Part 95 to store classified material. Finally, licensee, certificate holder, and applicant staffs and government officials would need to obtain, and the NRC would need to process, new security clearances under 10 CFR Part 10, and access authorizations under 10 CFR Part 25 to permit authorized individuals to access classified information.

Finally, while the staff believes that there is a clear nexus between the availability of past and future information and public confidence in the NRC's actions, the net impact on overall public confidence of current and potential actions on restricting access to sensitive information is not determinable at this time. Some stakeholders will have greater confidence in the NRC's actions as a means of reducing a potential vulnerability, through the removal or minimization of publicly-available sensitive information. However, to other stakeholders, this action may be viewed as a means of permitting the NRC to hide controversial information (i.e., licensee performance and safety weaknesses). The NRC has been working for over two decades on its "openness" policy and the pullback of information after the September 11 attacks has already resulted in negative feedback from highly-vocal stakeholders. Significant resources would be expended to continue the NRC's "openness" policy and provide the maximum amount of redacted information to stakeholders commensurate with the protection of national security.

Guidance Sought from the Commission:

The Commission is requested to provide guidance as to :

- Whether the staff should undertake a review of MD 3.4 and related regulations and redefine what types of information should be routinely released to the public.

- Whether the staff should seek to limit [restrict] public access to sensitive information or to prohibit public access to sensitive information (i.e., the material would meet one of the FOIA exemptions)?

- Whether the staff should propose changes to the NRC's Strategic Plan associated with the public confidence strategy in recognition of the new terrorist threat and the NRC's increased need to restrict access to sensitive information?

- Whether the staff should undertake a review of our openness policy and determine whether alternate means to obtain meaningful public participation in the NRC's regulatory process are sufficient?

POLICY ISSUE # 4
Protecting the Public from Releases of Hazardous Chemicals at NRC-Licensed Facilities

Issue:

Should the NRC require protection of NRC-licensed facilities against sabotage intended to cause large releases of hazardous chemicals from those facilities?

Sub-issues:

1. What are the threat, risk, and vulnerability of chemical sabotage at NRC-licensed facilities and activities? Do these vulnerabilities pose a large enough risk to warrant enhanced protection?

2. What safety goal or objectives should be used to judge the adequacy of protection against chemical sabotage and releases?

3. Would the safety goal be consistently applied to other, non-nuclear chemical manufacturing, storage, and distribution plants? If not, why should we protect the national infrastructure in an inconsistent manner?

4. What jurisdictional issues must be addressed?

Background:

The NRC, EPA and OSHA currently do not have specific requirements for protection of hazardous chemicals against sabotage.[22] The NRC's authority to regulate chemicals is, at best, implicit and is likely limited to chemicals directly used to process licensed materials or directly used in the operation of licensed facilities or those that could affect licensed materials. It likely does not extend to protection of bulk chemical storage areas which are located on a licensed site unless that chemical storage is reasonably determined to affect the safety of NRC licensed materials or activities. EPA's statutory authority includes the Emergency Planning and Community Right to Know Act of 1986 (EPCRA) which requires States to create State Emergency Response Commissions (SERCs) and local communities to form Local Emergency Planning Committees (LEPCs). However, EPCRA is not designed to prevent chemical

---

[22] As of October 26, 2001, EPA has appointed a counter-terrorism workgroup that "will synchronize that agency's various national security initiatives." Included in these initiatives is a workgroup on bio-terrorism that includes toxic chemicals and pesticides.

accidents, but rather, to inform the public of hazardous chemicals used and stored on site and to prepare emergency response plans for chemical accidents. OSHA's statutory authority under the Clean Air Act Amendments of 1990 (CAA), required OSHA to develop chemical accident prevention and emergency response regulations to protect workers at facilities for above threshold quantities of highly hazardous substances. OSHA promulgated these requirements as part of the Process Safety Management of Highly Hazardous Chemicals standard (PSM) rule, 29 CFR 1910.119, which became effective in 1992. EPA's response to the CAA was the Risk Management Program (RMP) or 40 CFR Part 68. RMP is similar to OSHA's PSM rule except for the major requirement to perform an Offsite Consequence Analysis (OCA), which is an estimate of the worst case and alternative accidental release of listed chemicals to the atmosphere around a facility. However, accident prevention in both rules is strictly limited to worker training issues, maintenance, procedural issues, and quality assurance. These regulations do not consider acts of sabotage.

Discussion:

After the Sequoyah Fuels Corporation accident in 1986, that resulted in a fatality, NRC worked with both the OSHA and the EPA to clarify federal responsibilities for protecting workers and members of the public against chemical and other non-radiological hazards. Those efforts included the execution of two Memoranda of Understanding (MOUs) with OSHA, implementation of the responsibilities under those MOUs, and consultation in support of the revisions to the requirements in 10 CFR Part 70, for fuel fabrication facilities. The MOUs categorize hazardous chemical risks into four categories: (1) radiation risk from licensed material; (2) hazardous chemical risks produced by licensed materials; (3) plant conditions which affect the safety of radioactive materials; and (4) plant conditions that result in occupational risk, but do not affect the safety of licensed radioactive materials. Under the MOUs, NRC generally covers the first three areas and OSHA covers the fourth area. The MOU that was established between the NRC and EPA concerned Clean Air Act standards to minimize regulatory duplication and conserve resources in the control of radionuclide emissions, and did not directly consider chemical or chemical sabotage issues.

Despite this progress in working with the EPA and OSHA, requirements for protection of workers and members of the public against chemical and other non-radiological hazards do not consider chemical releases from malevolent acts. Such malevolent acts could be as simple as puncturing a bulk storage tank.

The existing physical security requirements for the majority of NRC-licensed facilities that have large quantities of bulk chemicals are based upon requirements for protection of low strategic significance special nuclear material (SNM). For these facilities, licensees are only required to monitor for unauthorized penetrations and activities associated with licensed materials. One of the NRC-licensed facilities having the greatest chemical risk is not required to have any

physical protection requirements since it does not possess SNM. In this case, the physical protection afforded is basic industrial asset protection (i.e., standard industrial fencing and night watchmen).

The staff also notes that Senator Corzine (D - New Jersey) introduced legislation on October 31, 2001, titled the "Chemical Security Act of 2001 (Act) [S.1602], that would require the EPA and the Department of Justice (DOJ) to issue regulations for reducing the risks from chemicals and potential sources of chemical releases into the environment. The Act would create wide ranging authority for EPA to address security concerns posed by chemicals and chemical plants. The bill would require EPA and DOJ to develop a list of "high priority" chemicals and sources that pose significant risks and develop rules to mitigate risks. Additionally, a general duty requirement would be placed on any owner operator of a facility that falls within the "high priority" category to prevent a chemical release, and minimize the consequences when a chemical release occurs. The Committee on Environment and Public Works, Subcommittee on Superfund, Toxics, Risk, and Waste Management, held hearings on S.1602 on November 14, 2001.

Guidance Sought from the Commission:

The Commission is requested to provide guidance as to:

- Whether the Commission should pursue resolution of long-standing jurisdictional issues between the NRC, EPA and OSHA regarding responsibility for protecting chemical components or activities against acts of terrorism and sabotage on NRC licensed sites or involving NRC licensed materials.

- Whether the staff should increase its participation and visibility on interagency committees and working groups related to chemical issues to assure that NRC positions are well represented during the developmental stages of policy development as opposed to after the fact.

ATTACHMENT 8

Interim Actions Relating to Policy Issues (U)

INTERIM ACTIONS RELATING TO POLICY ISSUES	Due Date
Policy Issue 1- Boundary Between Private/Government Responsibility (requesting feedback from Commission by due date)	1/15/02
Established presence at FBI Special Incident Operations Center.	9/11/01C
Conducted selected Security Audits- Fuel Facilities/Cat-2.	11/16/01C
Established initial contact with the Office of Homeland Security and the Department of Energy regarding design basis threat revision.	Ongoing
Provided onsite representative to the Office of Homeland Security	10/01C
Selected Security Audits-Fuel Facilities/Cat-1	12/6/01
Selected Security Reviews-Power Reactors	1/1/02
Staff Propose Interim Compensatory Measures: (in order of priority as discussed in paper) - Decommissioning Reactors - Power Reactors - Fuel Facilities - Conv - Fuel Facilities - GDP - Transportation - Non Power Reactors - ISFSI - Indust/Med - Fuel Facilities - Cat-1 - Fuel Facilities - Cat-3	 12/21/01 11/28/01 11/28/01 12/15/01 1/15/02 1/11/02 1/15/02 1/15/02 12/15/01 12/21/01

INTERIM ACTIONS RELATING TO POLICY ISSUES	Due Date
Policy Issue 2- NRC Role/Interface in National Infrastructure Arena (requesting feedback from Commission by due date)	1/15/02
Establish Lines of Contact - Intergovernmental Communications w/Federal, State, Local and Tribes	2/14/02
Determine Appropriate Levels of Communication	3/15/02
Establish Communications Protocol & Expectations	5/18/02
Policy Issue 3- Balancing National Security Interests with Public Information Needs (requesting feedback from Commission by due date)	1/15/02
Submitted COMSECY-01-0030, "Guidance to the Staff on Release of Information to the Public," to the Commission, which contained criteria for discretionary release of information to the public.	10/29/01C
Develop Near-Term Communications Plan with Stakeholders	1/25/02
Develop Long-Term Stakeholder Communication & Participation Plan	3/18/02
Shutdown NRC's external web site, scrubbed it, and restored portions of the web site	10/17/01C
Continue restoring portions of the web site as reviews are completed	ongoing
Policy Issue 4- NRC Responsibility regarding Chemical Sabotage (requesting feedback from Commission by due date)	1/15/02
Establish interim compensatory measures for uranium conversion facilities	11/28/01
Establish interim compensatory measures for GDP's	12/15/01

ATTACHMENT 9

Foreign Government Responses and International Coordination (U)

Foreign Government Response and International Coordination

Purpose:

The purpose of this attachment is to inform the Commission of actions taken by foreign governments in response to the terrorist attacks of September 11, 2001. The staff is providing this information to assist the Commission in evaluating the staff's proposed actions for NRC-licensed facilities.

Discussion:

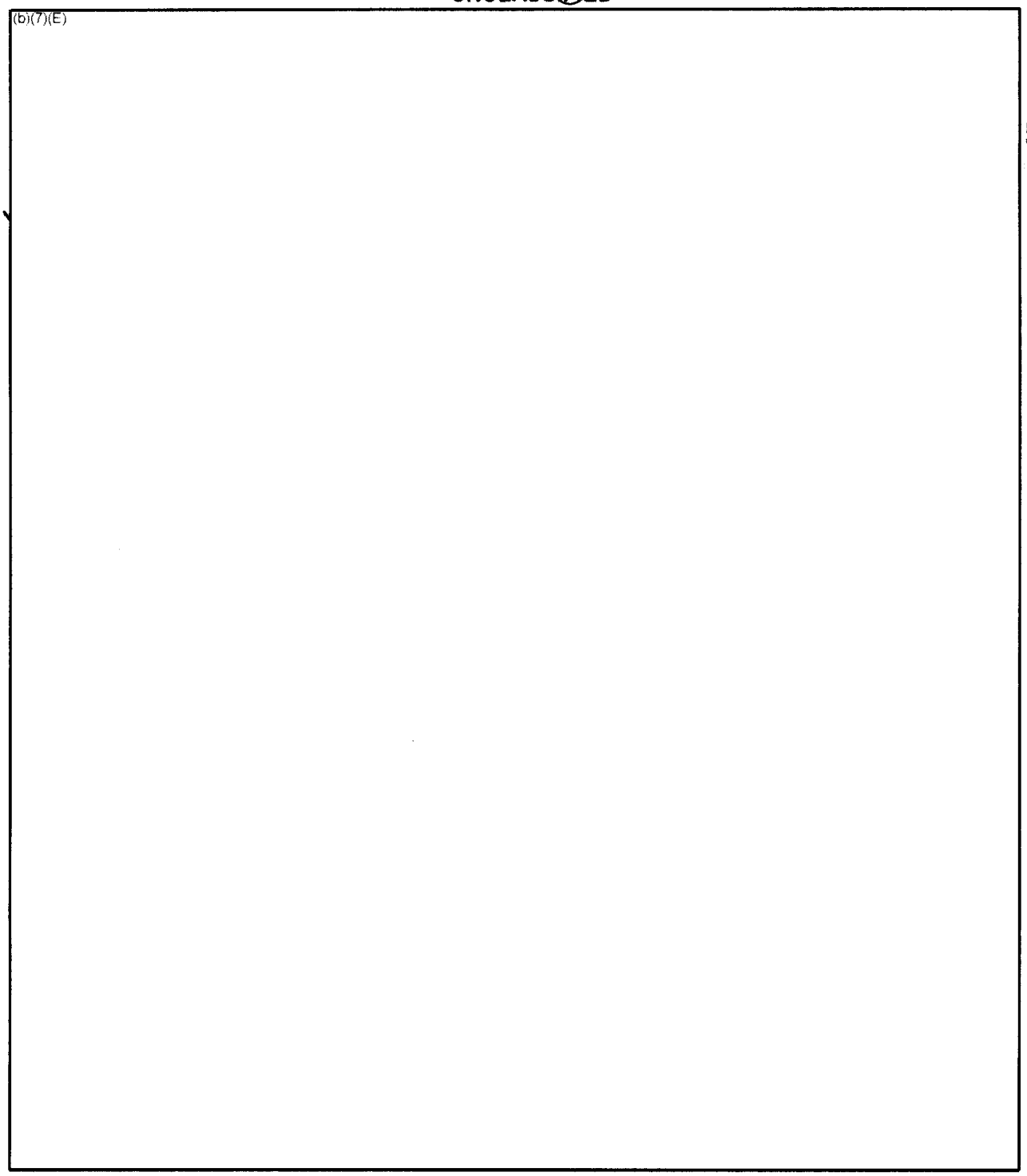
Immediately after the events of September 11, 2001, the NRC took measures to assure that NRC licensed facilities were notified of the situation, and requested those facilities to take actions to improve the security posture at those facilities. Most other countries, although not all, have taken some action. In general, the range of activities and actions that were described include the following:

- Increased communication between the regulator and operator on security issues
- Elevated security levels/readiness at nuclear facilities
- Activated crisis response centers
- Increased guard force patrols
- Increased support from local law enforcement and military at the facilities
- Restricted airspace and waterways around the facilities
- Limited access into the facilities
- Increased communications with the public on terrorist related risks to the facility
- Removed information from web sites and other sources that could be of value to a terrorist
- Initiated vulnerability assessments (by either the regulator or the facility operator) of hypothesized terrorist attacks (to include airplanes and other methods) and the potential consequences of such acts
- Evaluated the adequacy of security plans and emergency response plans.

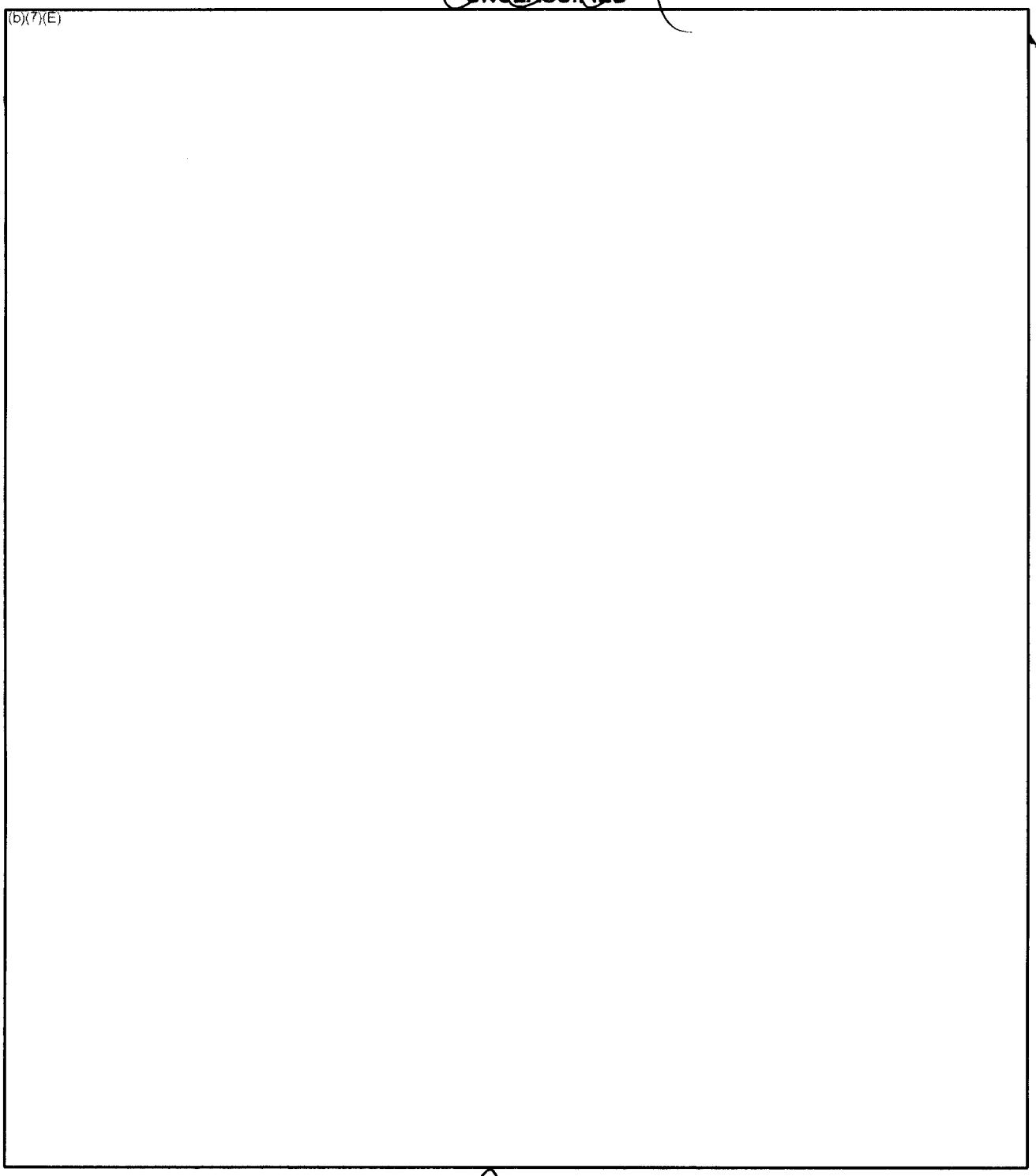
The staff did not obtain the following information through official government-to-government channels. Instead, the information was obtained from a variety of sources, including: (1) NRC management participation in recent international meetings; (2) foreign counterpart discussions; (3) intelligence traffic; and (4) publicly-available information sources.

(b)(7)(E)

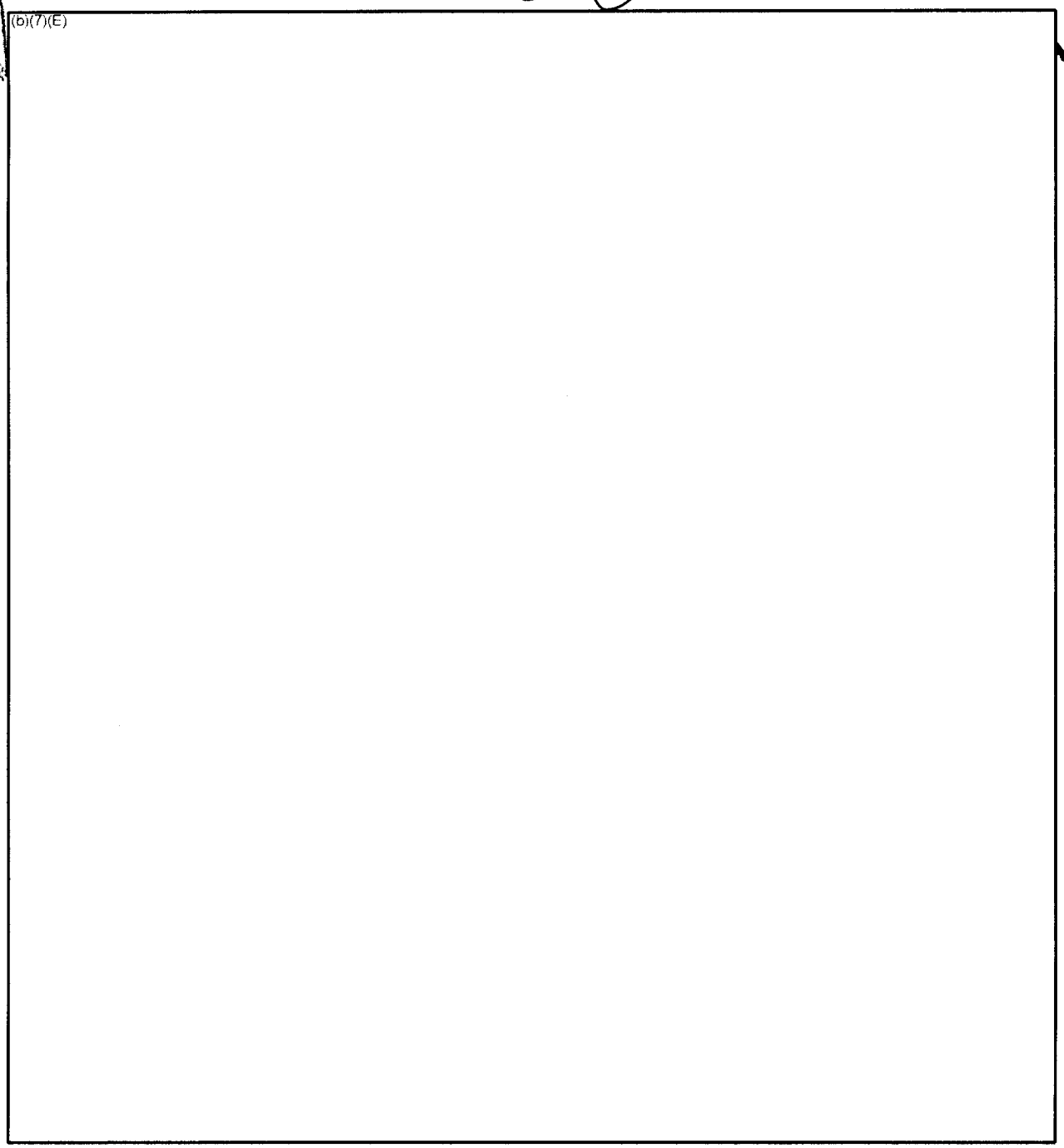
(b)(7)(E)



(b)(7)(E)



(b)(7)(E)



International Atomic Energy Agency (IAEA) Activities:

In the immediate aftermath of the terrorist attacks on 11 September, the IAEA General Conference adopted a resolution (GC(450/RES/14)) "requesting the Director General to review the activities and programs of the Agency with a view to strengthening the Agency's work relevant to preventing acts of terrorism involving nuclear materials and other radioactive materials." In recent meetings at IAEA Headquarters in Vienna, Austria, the Agency was called upon by a number of experts from Member States to enhance its efforts to assist in narrowing the gap between potential threats and the protective measures currently in place.
The IAEA underlined the fact that the primary responsibility for response to potential acts of terrorism rests with each individual State, which must strike their own balance between the role of national security and the responsibilities of nuclear facility operators. However, IAEA has proposed a number of additional or enhanced activities that the Agency might undertake. A draft document proposing this path forward has been developed to present to the Board of Governors in order to seek feedback. It is intended, on the basis of this feedback and consultations to be held with Member States, to issue a revised document for consideration by the IAEA Board of Governors at its March 2002 session.

Finally, understanding that terrorism is a global threat and the response to it must be global in nature, the proposals put forward in this draft document would require the sustained support of all Member States in order to be effective, because the strength of anti-terrorist measures is determined by the weakest link in the chain, and the implementation of these proposals would, in turn, benefit all Member States. Much of the responsibility in each case would rest with the Member States themselves, with the Agency providing guidance, co-ordination, training, and review services in the particular areas of its own expertise. In this connection, the Agency feels it is important that they be empowered with the necessary authority in the spheres where it has legal obligations, and that this authority be fully realized through the universal acceptance of the related legal instruments by Member States. If Member States approve proposals for enhanced and additional activities at its March 2002 session, the IAEA Secretariat could start initial implementation immediately at that time.

~~CONFIDENTIAL~~
~~OFFICIAL USE ONLY~~

ATTACHMENT 10

[redacted]

The classified information has been removed from this document.

This copy of the document is UNCLASSIFIED.

By: Krista Ziebell, #3220
Information Security Specialist
December 30, 2014

~~OFFICIAL USE ONLY~~
~~CONFIDENTIAL~~

DERIVED FROM: Multiple Sources 11b2/a
SOURCE/DATE
REASON: 1.5 C, D, G X-2
DECLASSIFY ON:
EXEMPTION
CLASSIFIER:
NUMBER

I. Introduction

(U) In the aftermath of the terrorist attacks of September 11, 2001 and the continuing uncertainty about future terrorist intentions, the Commission recognized the need to give focused attention to evaluate necessary adjustments in licensee and Federal, State, and local response capabilities. As part of the comprehensive review of NRC's safeguards and security programs, staff has conducted an initial assessment of the current threat environment which takes into account insights from the recent terrorist attacks as well as adversary characteristics from other national and international terrorist activities. Using interim criteria developed by the Task Force to discriminate between the appropriate role of licensees, and the role of local, State and Federal entities, staff has developed examples for the Commission's consideration to illustrate how this approach could be used to establish interim compensatory measures for licensees where additional physical security is indicated considering the current threat environment. Staff is evaluating potential interim compensatory measures for all categories of licensees and could provide these to the Commission by the end of January. Once guidance from the Commission is received, staff could dialogue with licensees to establish the practicality and sustainability of the interim compensatory measures at specific sites and could establish requirements within sixty days.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Att. 1

[redacted]

[redacted]

Lt. 1

[redacted]

[redacted]

Ex. 1

[redacted]

[redacted]

[redacted]

[redacted]					
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

	[redacted]			[redacted]	
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Ex. 1

Ex. 1

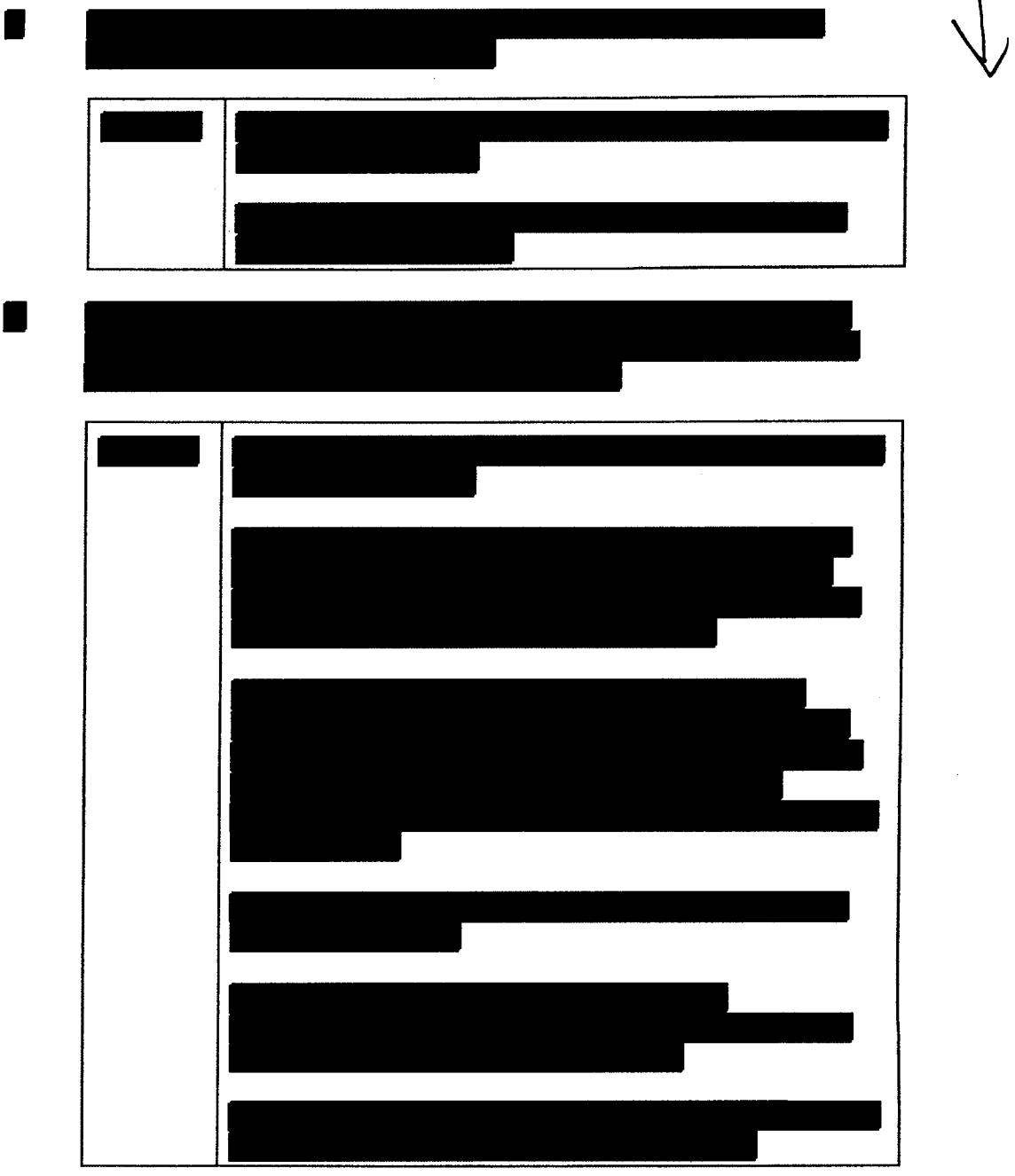
[redacted]

Att. 1

Lt. 1

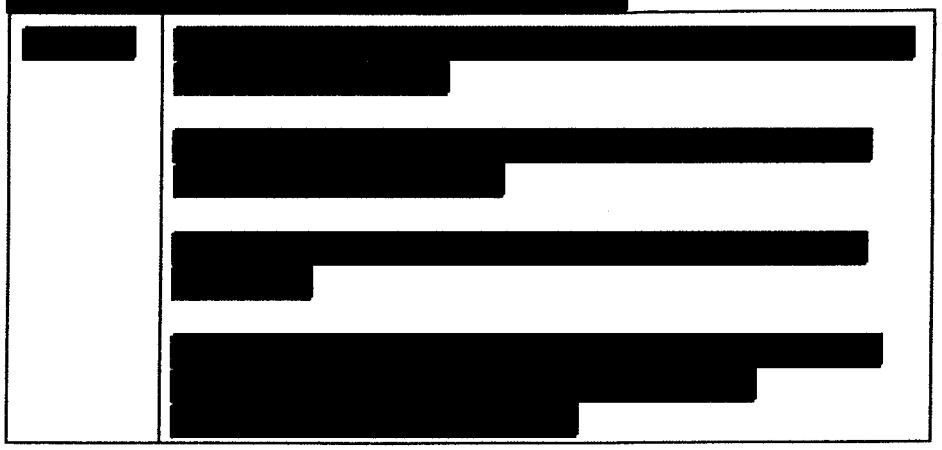
[redacted]

Ex. 1



Ex. 1

- [redacted]



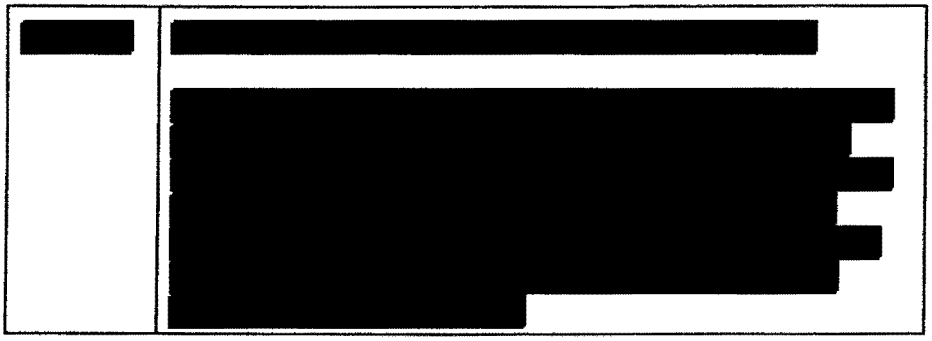
- [redacted]

Ext. 1

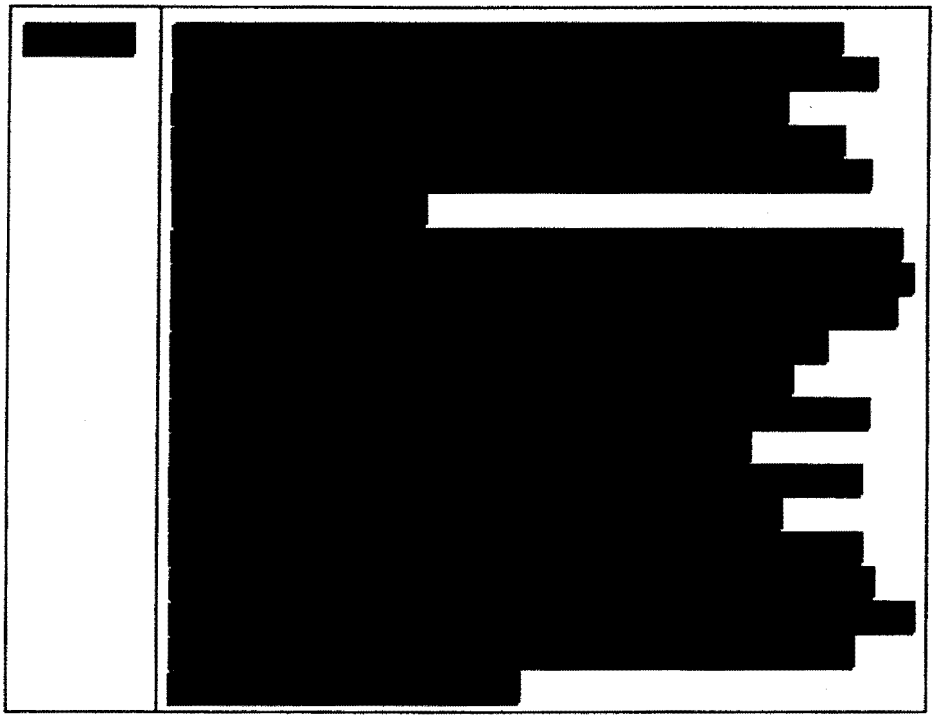
[redacted]

Ent. 1

[redacted]



[redacted]



VII Conclusion

(U) The staff believes that implementing the proposed course of action is a prudent strategy to incorporate incremental near-term interim compensatory measures and longer-term measures which would take advantage of more robust threat analysis and vulnerability assessment. It also reflects a graded strategy in that the priority of activities and scale of protection reflect differences among licensee classes in vulnerabilities, potential consequences of sabotage or malevolent use, and relative attractiveness as targets. Staff believes the proposed interim compensatory measures, which build upon existing capability at the licensed facilities, draw an appropriate line between licensee and Federal, State and local security for the current threat environment.

(U) While the extent of support by Federal, State, and local entities is being determined, the staff believes that, in the short-term, the risk beyond what is currently being protected is acceptable, given the interim compensatory measures that are proposed for licensees, and that no specific, credible threats have been identified against commercial nuclear facilities. Also, current protection for most licensed activities is equal or greater than protection at other comparable industrial facilities. Finally, Federal, State, and local entities have previously supported site security and can be assumed to respond in the event of an actual terrorist attack as was demonstrated in the September 11 event. With the Commission's approval, the staff will implement proposed interim compensatory measures for nuclear power plants and the uranium conversion facility, and is proceeding with an assessment of need for interim compensatory measures for other categories of licensees.