



governmentattic.org

"Rummaging in the government's attic"

Description of document: Three Lawrence Livermore/Sandia National Laboratories (LLNL/SNL) reports re Biological Select Agents and Toxins Risk/Threat Assessment and Security, 2005, 2006

Request date: 23-May-2015

Released date: 26-August-2015
2nd release date: 17-September-2015

Posted date: 14-September-2015
Update posted date: 02-November-2015

Titles of documents: Lawrence Livermore National Laboratory Biological Risk and Threat Assessment for Building 368 Biological Safety Laboratory Level 3, July 14, 2005
Lawrence Livermore National Laboratory Plans, Policies and Procedures, Biological Select Agents and Toxins Security Plan, Revision 6, March 9, 2006
Catastrophic Bioterrorism Scenarios: Response Architectures and Technology Implications, March 2006

Source of document: FOIA/PA Officer
NSNSA/Office of the General Counsel
P. O. Box 5400
Albuquerque, NM 87185-5400
Fax: (505) 284-7512
Email: FOIOfficer@nnsa.doe.gov

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



Department of Energy
National Nuclear Security Administration
Office of the General Counsel
P. O. Box 5400
Albuquerque, NM 87185



August 26, 2015

SENT VIA EMAIL

This letter is a final response to your May 23, 2015 Freedom of Information Act (FOIA) request for a copy of the following reports from Lawrence Livermore National Laboratory (LLNL) and Sandia National Laboratories (SNL):

1. LLNL Site Seismic Safety Program, Summary of Findings, UCRL-53674, Rev. 2, April 2002
2. LLNL Biological Risk and Threat Assessment, July 14, 2005
3. LLNL Select Agents and Toxins Security Plan, Revision 6, SSO-POL-010, UCRL-MI-220409 March 9, 2006
4. SNL and LLNL Catastrophic Bioterrorism Scenarios: Response Architectures and Technology Implications, March 2006
5. LLNL B368 Select Agent Risk and Threat Assessment, July 14, 2005

We contacted the Livermore Field Office (LFO), which has oversight responsibility over Lawrence Livermore National Laboratory (LLNL) and the Sandia Field Office (SFO), which has oversight responsibility over the Sandia National Laboratories (SNL) to conduct a search for records responsive to your request. The results of those searches are as follows:

Regarding **Item 1** of your request, the document "LLNL Site Seismic Safety Program: Summary of Findings" is in the public domain and can be found at <http://www.osti.gov/scitech/biblio/15002343/>.

The enclosed document "LLNL Biological Risk and Threat Assessment" is responsive to both **Items 2 & 5** of your request. This document is released to you with deletions pursuant to 5 USC 552(b)(1) (Exemption 1 of the FOIA) and 5 USC 552(b)(7)(f) (Exemption 7(f) of the FOIA). **NOTE:** Justification of all exemptions are below.

The document "*LLNL Biological Select Agents and Toxins Security Plan, Revision 6,*" (responsive to **Item 3** of your request) is enclosed. This document is released to you with deletions pursuant to 5 USC 552(b)(6) (Exemption 6 of the FOIA) and 5 USC 552(b)(7)(f) (Exemption 7(f) of the FOIA).

With respect to **Item 4** of your request, the document is under the jurisdiction of the Department of Homeland Security (DHS). Therefore, by copy of this letter, your request is being transferred to the DHS FOIA Office. That office will respond to you directly regarding your request for a copy of "*Catastrophic Bioterrorism Scenarios: Response Architectures and Technology Implications, March 2006.*"

Pursuant to Title 10, Code of Federal Regulations, Section 1004.6 (10CFR 1004.6), the Office of Classification, Office of Health, Safety and Security, in the Department of Energy (DOE) has completed its review of the documents responsive to your request. These documents, located in the files of LFO, contain information properly classified as National Security Information; therefore they are provided to you with deletions.

Title 5, United States Code, § 552(b)(1) (5 USC 552(b)(1) (Exemption 1), provides that an agency may exempt from disclosure matters that are “(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order. ...” The portions deleted from the subject documents pursuant to Exemption 1 contain information about vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security and are classified under section 1.4(g) of Executive Order 13526 (EO 13526) and information about weapons of mass destruction and are classified under section 1.4(h) of EO13256. It has been determined that release of the information could reasonably be expected to cause damage to the national security.

To the extent permitted by law, DOE, pursuant to 10 CFR 1004.1 will make available records it is authorized to withhold under FOIA whenever it determines that such disclosure is in the public interest. With respect to the information withheld from disclosure pursuant to Exemption 1, DOE has no further discretion under FOIA or DOE regulations to release information currently and properly classified pursuant to EO 13256.

The purpose of Exemption 6 is to protect individuals from the injury and embarrassment that can result from the unnecessary disclosure of personal information. To determine whether disclosure would constitute a clearly unwarranted invasion of personal privacy, the public interest in disclosure, if any, must be balanced against the privacy interests that would be invaded by disclosure of the information. In this case, personally identifying information (name, telephone number, and signature) of contractor employees has been withheld. Release of the information pertaining to these contractor employees will cause inevitable harassment and unwarranted invasion of privacy for those individuals. In addition, release of this information would not shed light on the operations of the federal government. Since its release will not reveal anything of significance to the public, the interest in protecting against the invasion of privacy that would result to the individuals in question far outweighs the public interest in such disclosure.

It is widely held that federal employees have no expectation of privacy regarding their names, titles, grades, salaries, and duty stations. See 5 CFR § 293.311(1994); Core v. United States Postal Serv., 730 F.2d 946, 948 (4th Cir. 1984); National W. Life Ins. Co. v. United States, 512 F. Supp. 454, 461 (N.D. Tex. 1980). Therefore, the disclosure of such information about federal employees would involve little or no invasion of privacy. Contractor employees, however, are not federal employees. Rather, they are private individuals. The Supreme Court has long found a privacy interest in the names of private individuals significant enough to warrant protection from disclosure under Exemption 6.

Pursuant to Exemption (7)(f), the portions of this document withheld are about protection and security measures used to protect Federal buildings and personnel. Exemption (7)(f) of the FOIA protects law enforcement information that “could reasonably be expected to endanger the life or physical safety of any individual.” The ordinary meaning of law enforcement includes not just the investigation and prosecution of offenses already committed but also proactive steps designed to maintain security.

The portions of this document withheld pursuant to Exemption (7)(f), are about protection and security measures used to protect Federal buildings and personnel. Exemption (7)(f) of the FOIA protects law enforcement information that “could reasonably be expected to endanger the life or physical safety of any individual.” The ordinary meaning of law enforcement includes not just the investigation and prosecution of offenses already committed but also proactive steps designed to maintain security.

Pursuant to 10 CFR § 1004.6(d), Dr. Andrew P. Weston-Dawkes, Director, Office of Classification, DOE Office of Health, Safety and Security, is the official responsible for the denial of DOE classified information.

Pursuant to 10 CFR § 1004.7(b) (2), I am the individual responsible for the withholding of information mentioned above pursuant to Exemptions 6 and 7f of the FOIA.

You may appeal our withholding of Exemption 1, 6 & 7 information pursuant to 10 CFR § 1004.8. Such an appeal must be made in writing within 30 calendar days after receipt of this letter, addressed to the Director, Office of Hearings and Appeals, HG-1, U.S. Department of Energy, 1000 Independence Avenue SW, L’Enfant building, Washington, DC 20585. Your appeal must contain a concise statement of the grounds for the appeal and a description of the relief sought. Please submit a copy of this letter with the appeal. Please clearly mark both the envelope and the letter “Freedom of Information Appeal.” Thereafter, judicial review will be available to you in the District of Columbia or in the district where (1) you reside, (2) you have your principal place of business, or (3) the Department’s records are situated.

There are no fees chargeable to you for processing this request. If you have any questions concerning the processing of your request, please contact Christina Hamblen at christina.hamblen@nnsa.doe.gov and refer to our Control Number FOIA 15-00206-H.

Sincerely,



Jane R. Summerson
Authorizing & Denying Official

Enclosures

cc w/copy of FOIA request:
U.S. Department of Homeland Security
Science and Technology Directorate
FOIA Officer: Katrina Hagan
245 Murray Lane
Washington, D.C. 20528
E-mail: stfoia@hq.dhs.gov

COS-2005-107

LEE, HARVEY W



cy2

L90-08-0887

000016862

Lawrence Livermore National Laboratory (U)

Biological Risk and Threat Assessment

for

Building 368 Biological Safety Laboratory Level 3 (U)



July 14, 2005

Conducted by:

Lawrence Livermore National Laboratory
Security Department
Threat Mitigation Analysis Group

NATIONAL SECURITY INFORMATION

Unauthorized Disclosure Subject to
Administrative and Criminal Sanctions

Classified By: Michael A. Netherton

Derived From: CG-SS4 September 2000

Declassify On: X-4

20090003329

List of Figures and Tables (U)	3
List of Acronyms and Abbreviations (U)	4
Executive Summary (U)	5
1.0 Introduction (U)	7
1.1 Purpose of Assessment (U)	7
1.2 Audience (U)	7
1.3 Scope of Assessment (U)	7
2.0 Assessment Team/Process (U)	7
2.1 Assessment Team (U)	7
2.2 Working Groups, Data Collection, and Interviews (U)	7
3.0 Program/Facility Characterization (U)	9
3.1 Mission (U)	9
3.2 Physical and Infrastructure Details (U)	9
3.3 Facility Operations (U)	11
3.4 Regulatory Requirements/Safety Requirements (U)	11
3.5 Emergency Response (U)	11
4.0 Asset Identification and Prioritization (U)	12
4.1 Asset Identification (U)	12
4.2 Asset Prioritization (U)	12
4.3 Select Agent List (U)	12
4.4 Building 368 SAs (U)	13
4.5 Facility-Specific Secondary Assets (U)	22
4.6 Facility Specific Tertiary Assets (U)	23
5.0 Threat Definition and Assessment (U)	24
5.1 General Threat Identification (U)	24
5.2 Risk and Resource Allocation (U)	27
5.3 Design Basis Threat (U)	28
6.0 Vulnerability Assessment (U)	29
6.1 Assessment Results (U)	29
6.2 Identified Vulnerabilities (U)	29
6.3 Protection System Effectiveness (U)	30
7.0 Other Recommendations to Consider (U)	32
8.0 Concurrences and Approvals (U)	33
8.1 Preparation and Review (U)	33
8.2 Approvals (U)	34
Appendix A: List of Pathogens, Agents, and Toxins (U)	35

List of Figures and Tables (U)

Figure 3-1	Facility Layout (U)	10
Table 4-1	Primary Asset Identification (U)	12
Table 4-2	Asset Prioritization (U).....	12
Table 4-3	<i>Clostridium botulinum</i> information sheet (U).....	14
Figure 4-1	<i>Clostridium botulinum</i> photo (U)	14
Table 4-4	<i>Bacillus anthracis</i> information sheet (U).....	15
Figure 4-2	<i>Bacillus anthracis</i> photo(U)	15
Table 4-5	<i>Yersenia pestis</i> information sheet (U)	16
Figure 4-3		16
Table 4-6		17
Figure 4-4		17
Table 4-7	(b)(7)(f)	18
Figure 4-5		18
Table 4-8		19
Figure 4-6		19
Table 4-9	<i>Dengue fever virus</i> information sheet (U)	20
Figure 4-7	<i>Dengue fever</i> photo (U)	20
Table 4-10		21
Figure 4-8	(b)(7)(f)	21
Table 4-11	Secondary Asset Identification (U)	22
Table 4-12	Tertiary Asset Identification (U).....	23
Table 5-1	Threat Definitions (U)	24
Table 5-1	Threat Definitions (continued) (U)	25
Table 5-2	Threat Assessment (U)	26
Table 5-3	Likelihood and Consequences (U)	27
Table 5-4	Risk and Resource Allocation (U)	28
Table 6-1	Adversary Table (U)	31

List of Acronyms and Abbreviations (U)

µm	Micrometer (or micron)
ABSL-3	Animal Biosafety Level-3 Laboratory
APHIS	Animal and Plant Health Inspection Service
B-365	Building 365
BIO	Biosciences Directory
BMBL	Biosafety in Microbiological and Biomedical Laboratories
BMS	Balanced Magnetic Switch
BSL	Biosafety Level
CDC	Centers for Disease Control and Prevention
CFR	Code of Federal Regulations
C&MS	Chemistry and Materials Science Directorate
DOE	United States Department of Energy
DBT	<i>Design Basis Threat (Policy)</i>
DOJ	United States Department of Justice
FSP	<i>Facility Safety Plan</i>
HHS	United States Department of Health and Human Services
HSO	Homeland Security Organization
HVAC	Heating Ventilation and Air Conditioning
IFD	In-Facility Destruction
LANL	Los Alamos National Laboratory
LASO	Los Alamos Site Office
LBNL	Lawrence Berkley National Laboratory
LLNL	Lawrence Livermore National Laboratory
LSO	Livermore Site Office
NAI	Nonproliferation, Arms Control, and International Security Directorate
NNSA	National Nuclear Security Administration
OPSEC	Operations Security
PC	Primary Consequence
PI	Principal Investigator
PIN	Personal Identification Number
RAP	Remote Access Panel
SA	Select Agent
SAA	Select Agent Area
SAHRP	Select Agent Human Reliability Program
SC	Secondary Consequence
SNL	Sandia National Laboratories
SOP	Standard Operating Procedures
SD	Security Department
STL	Sabotage Threat Level
TBD	To Be Determined
TC	Tertiary Consequence
TMAG	Threat Mitigation and Analysis Group
UCOP	University of California Office of the President
USDA	United States Department of Agriculture

Executive Summary (U)

(U) On February 7, 2003, the Interim Final Rule for 42 CFR Part 73 *Possession, Use, and Transfer of Select Agents and Toxins* was made effective (current Final Rule is dated March 18, 2005). The regulation established requirements regarding possession and use in the United States, receipt from outside the United States, and transfer within the United States of select agents (SAs) and toxins.

(U) Requirements exist for facility registration, security risk assessments, safety plans, security plans, emergency response plans, training, transfers, record keeping, inspections, and notifications. The part 73 regulations implement provisions of the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002* (commonly referred to as the Act), Public Law 107-188. The facilities regulated under part 73 are academic institutions and biomedical centers; commercial manufacturing; federal, state, and local laboratories; and research facilities. The Act gives the United States Department of Health and Human Services (HHS) the authority and responsibility for regulating activities regarding SAs and toxins to protect the public health and safety.

(U) Part 73.11 requires facilities subject to the provisions of the regulations to develop and implement a security plan establishing policies and procedures that ensure the security of areas containing SAs and toxins. The security plan must be based on a systematic approach in which threats are defined, vulnerabilities are examined, and risks associated with the vulnerabilities are mitigated. However, requirements in the Act for conducting a biosecurity risk assessment were elementary and vague. Therefore, in March 2003, under direction from the University of California Office of the President (UCOP), representatives from Livermore Site Office (LSO), Los Alamos Site Office (LASO), NNSA Service Center, Lawrence Livermore National Laboratory (LLNL), Los Alamos National Laboratory (LANL), Lawrence Berkley National Laboratory (LBNL), and Sandia National Laboratories (SNL) met to discuss biosecurity regulations and future Department of Energy (DOE) biosecurity order requirements. Notable differences among the labs prompted the need for a joint working group to define and establish common criteria for facility risk assessments, establish consistency in documentation, define what documentation DOE and the National Nuclear Security Administration (NNSA) expect, and to secure agreement from all entities (UC/NNSA/SNL/DOE) about decisions, paths, and processes.

(U) Taking into consideration all documented biosecurity rules, regulations, and guidelines (i.e., 42 CFR 73, 1003, 7 CFR 331, 9 CFR 121, DOE N 450.7, and Biosafety in Microbiological and Biomedical Laboratories [BMBL] Appendix F), the working group developed a risk and threat assessment process (based on a methodology developed by SNL) that exceeds industry standards. The methodology was separated into four main areas: (1) asset identification and prioritization, (2) threat identification and evaluation, (3) threat design parameters, and (4) security system objectives. This methodology was used, in conjunction with guidelines depicted in the current Design Basis Threat (DBT) dated October 18, 2004, as the baseline criteria for this risk assessment.

(U)
(C) LLNL's Nonproliferation, Arms Control, and International Security Directorate (NAI) and Biosciences Directorate (BIO) maintain three research areas that will soon be actively working with SA pathogens within Building 368 (B-368), a Biosafety Level (BSL) 3 facility. Individuals from the Security Department (SD) Threat Mitigation and Analysis Group (TMAG) conducted this assessment with assistance from BIO personnel utilizing all applicable guidelines and documented requirements that will be in effect upon activation. The TMAG began its assessment by gaining knowledge of B-368 policies and procedures, acquiring access lists, conducting a tour of the facility, and interviewing subject matter experts. After analyzing all applicable information, the group believes that the facility will be in compliance with current security requirements upon activation. In addition to meeting all mandated requirements for individuals having access to the SA, University of California has taken additional steps by creating and implementing a very stringent Select Agent Human Reliability Program (SAHRP) dated March 23, 2005. Additionally, all physical security measures currently in place for the facility were found to be commensurate with order compliance requirements outlined in the current DBT.

(b)(1)

(U) As required by 42 CFR Part 73, annual reviews of this threat assessment will be conducted by the TMAG to verify that policies and procedures are being effectively utilized. Applicable upgrade recommendations will be given at the conclusion of each review to help sustain an effective security culture within the BSL 3 and to help prevent and mitigate hostile acts with SAs.

(b)(1)

1.0 Introduction (U)

1.1 Purpose of Assessment (U)

(U) The purpose of the assessment was to fulfill the requirement listed in 42 CFR Part 73 as well as requirements outlined in the current DBT and to document any weaknesses associated with the B-368 security system. Applicable recommendations and best practices will be incorporated into future LLNL Biological Select Agent and Toxins Security Plans.

1.2 Audience (U)

(U) This assessment is primarily intended to inform LLNL/SD Management of the assessment results and recommendations. It is expected that this report will also be used to similarly inform LLNL Management, LSO, and external entities.

1.3 Scope of Assessment (U)

(U) The scope of this assessment includes the identification, collection, and evaluation of applicable requirements, guidelines, and best practices/industry standards; characterizing the facility; identifying and prioritizing assets; and defining and assessing threats and vulnerabilities.

2.0 Assessment Team/Process (U)

2.1 Assessment Team (U)

(U) The team consisted of subject matter experts from BIO and members from SD's TMAG. Mr. Michael Netherton had the lead for this assessment.

2.2 Working Groups, Data Collection, and Interviews (U)

(U) In addition to verifying order compliance requirements outlined in the current DBT, the basis for this assessment was derived from the Biological Risk and Threat Assessment Methodology Working Group, which was a collaborative effort by LLNL, SNL, LBNL, LANL, NNSA, and UCOP.

(U) The working group defined the following:

- Objectives for the security assessment.
- Asset identification and prioritization.

- Threat identification and evaluation (likelihood of occurrence and consequence of event).
- Threat design-parameter definitions.
- Security system objectives.

(U) While conducting this assessment, members from the TMAG collected data on:

- Heating Ventilation and Air Conditioning (HVAC) systems.
- Electrical power supply/stand-by power.
- Daily operations.
- Physical security systems.
- Access control/access lists.
- Agent shipping and receiving procedures.
- Processing/storage locations.
- Inventory procedures.
- Operations security (OPSEC).
- Facility Layout and key plans.

(U) Applicable information was obtained by conducting interviews with the following individuals:

- Alan Casamajor, Responsible Official.
- Kris Montgomery, Lead Biomedical Scientist and B-368 Senior Lab Coordinator.
- Patsy Gilbert, B-368 Facility Manager.

3.0 Program/Facility Characterization (U)

(U) Before any decisions can be made concerning the level of protection needed, an understanding of what is being protected and the surrounding environment is essential.

3.1 Mission (U)

- (u) (OUO) The mission of the BSL-3 facility is to develop scientific tools to identify and understand the pathogens of medical, environmental, and forensic importance. This information is used to develop, demonstrate, and deliver technologies and systems to improve domestic defense and/or medical capabilities and, ultimately, to save lives in the event of a biological attack in support of our national security's nonproliferation mission.
- (u) (OUO) The Nonproliferation, Arms Control, and International Security (NAI) Directorate at LLNL is the funding organization responsible for defining and authorizing the programmatic work to be performed in B-368. BIO is responsible for executing the work in the facility. NAI has also delegated responsibility for the safety and security management and facility maintenance of B-368 to BIO. Other potential users of the BSL-3 facility are the Homeland Security Organization (HSO) and the Chemistry and Materials Science (C&MS) Directorate.

3.2 Physical and Infrastructure Details (U)

(OUO) B-368 is located near the center of LLNL, directly across from Building 271 (the Protective Force Division). B-368 is a 1,600 ft², one-story permanent prefabricated facility, (b)(7)(f) (one of which is to handle rodents), a mechanical room, clothes-change and shower rooms (Figure 3-1). The facility contains no exterior windows and is illuminated on all four sides during hours of darkness.

(b)(7)(f)

(OUO) The B-368 security system provides access to the change rooms and mechanical room through a locked door controlled by an Argus badge reader plus a personal identification number (PIN). Each room in the facility and all perimeter openings have intrusion detection systems that are set to alarm in the event of an unauthorized entry. This detection system is controlled by Argus. (b)(7)(f)

(b)(7)(f)

(b)(7)(f)

The system maintains an electronic log of all activity for the individual laboratories. The components of this system are shown below in Figure 3-1.

Figure 3-1 Facility Layout (U)
(b)(1)

3.3 Facility Operations (U)

(FOUO) Regular business hours are 6am to 6pm, Monday through Friday, excluding holidays. (b)(7)(f)

(b)(7)(f)

(b)(7)(f)

The number of employees with access to these three research areas is greatly reduced in comparison to the number with access to the facility in general. The Responsible Official verified that only 3 individuals currently have unescorted access to the SA research areas. This number may minimally increase in the future due to operational demands.

3.4 Regulatory Requirements/Safety Requirements (U)

(U) An approved *Facility Safety Plan* (FSP 368, July 2005) and *Standard Operating Procedures* (SOP Rev. 1, July 2005) strictly govern all facility activities (i.e., laboratory practices, shipping/receiving of agents, equipment use, and roles and responsibilities). On March 18, 2005, the Final Rule for 42 CFR Part 73, *Possession, Use, and Transfer of SAs and Toxins*, was made effective. This regulation established requirements regarding possession and use in the United States, receipt from outside the United States, and transfer within the United States of SA and toxins. This assessment considered the above items as well as all documented biosecurity rules, regulations, and guidelines (i.e., 7 CFR 331, 9 CFR 121, DOE N 450.7, and *Biosafety in Microbiological and Biomedical Laboratories*, Appendix F).

3.5 Emergency Response (U)

(FOUO) All medical and fire response to B-368 is performed by on-site emergency responders who are trained to handle the special circumstances associated with each facility. (b)(7)(f)

(b)(7)(f)

4.0 Asset Identification and Prioritization (U)

(U) The identification and prioritization of the assets below were accomplished by the Biological Risk and Threat Assessment Working Group, including TMAG, which met April 8 and 9, 2003². The group made the determinations on threat definitions and target identification in relation to a DOE-controlled biological research lab.

4.1 Asset Identification (U)

(U) Identification is an evaluation of “what” to protect without consideration of the threat or the difficulty of providing physical protection. Table 4-1 lists the primary assets for SA facilities.

Table 4-1 Primary Asset Identification (U)

Assets	Priority
CFR Agents	Primary
Equipment, contaminated with agent.	Primary

The contents of this table are UNCLASSIFIED

4.2 Asset Prioritization (U)

(U) Assets are prioritized according to the severity of loss (i.e., the impact to national security). Table 4-2 defines the criteria used for asset prioritization.

Table 4-2 Asset Prioritization (U)

	Criteria for prioritizing assets
Primary	Affects national security/bioterrorism
Secondary	Assists adversary in achieving a primary consequence or in gaining access to CFR agents.
Tertiary	Impacts operations (Note: could be elevated to secondary or primary depending on uniqueness to counter-bioterrorism operations).

The contents of this table are UNCLASSIFIED

4.3 Select Agent List (U)

(U) For registration purposes, HHS and USDA are required to provide lists of agents. The current list of Animal and Plant Health Inspection Service (APHIS) Plant Pathogens, HHS Select Infectious Agents, and APHIS High-Consequence Livestock Pathogens or Toxins can be found in Appendix A.

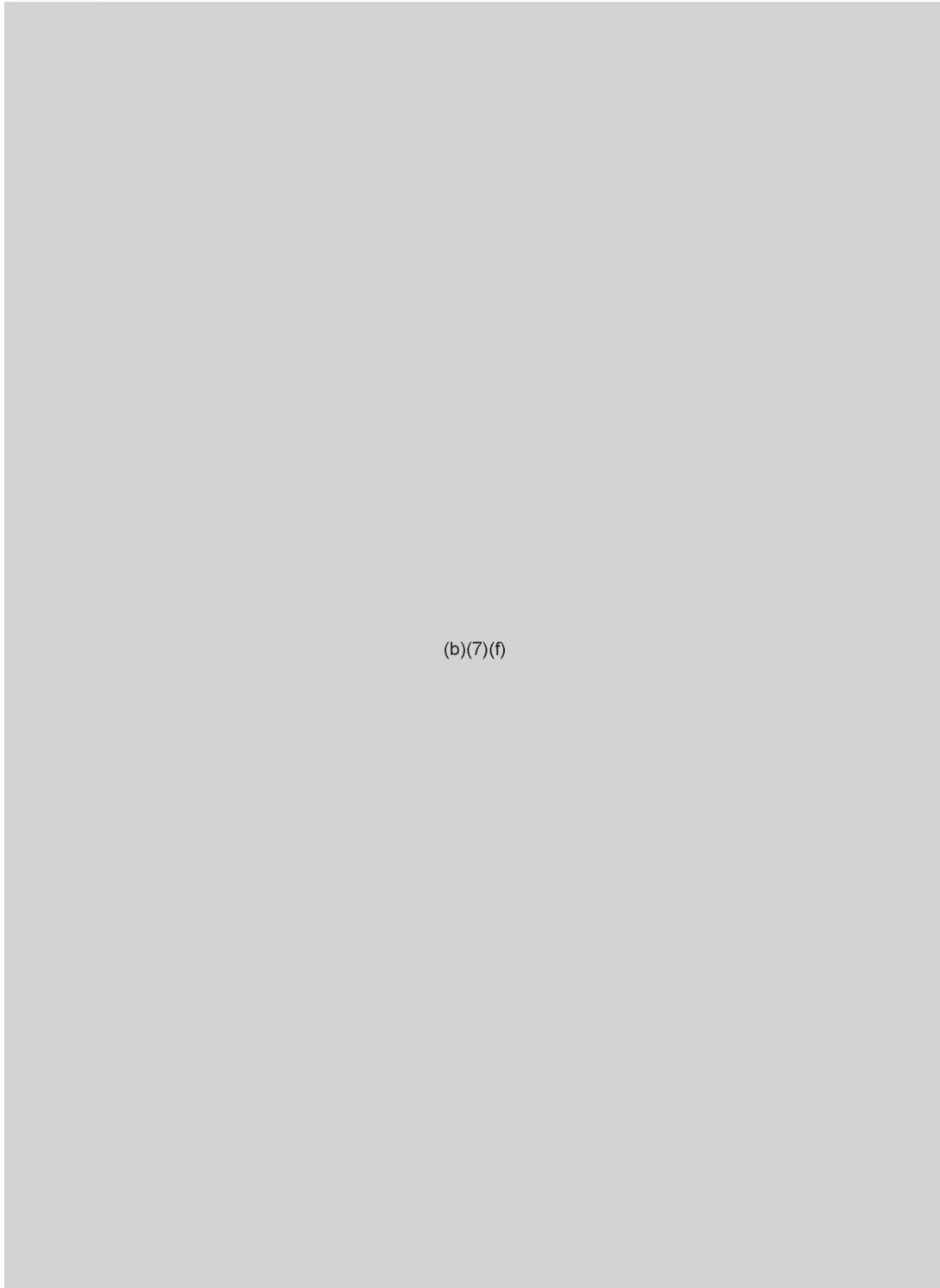
² The UC/NNSA/SNL/DOE Risk and Threat Assessment Methodology Working Group Report is still the most current process pertaining to bio targets/threat characterization.

4.4 Building 368 SAs (U)

(b)(7)(f)

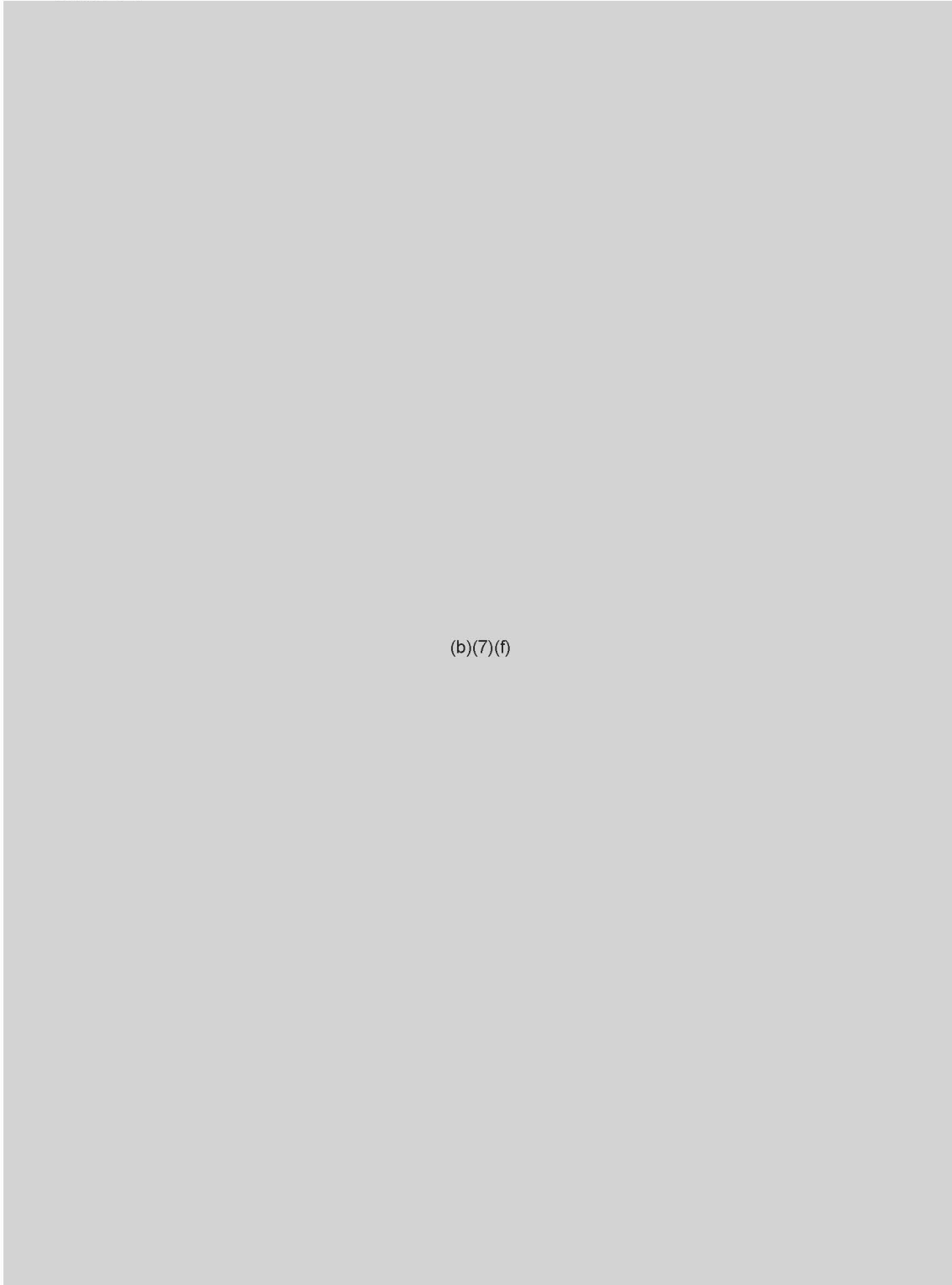
(b)(7)(f) A tracking system has been established for all biohazardous materials used in the BSL-3 facility. Relevant information from each agent's Material Safety Data Sheet is shown below in Tables 4-3 through 4-10. No radiological, high explosives, fissile, or propellant material are allowed in B368.

Table 4-3



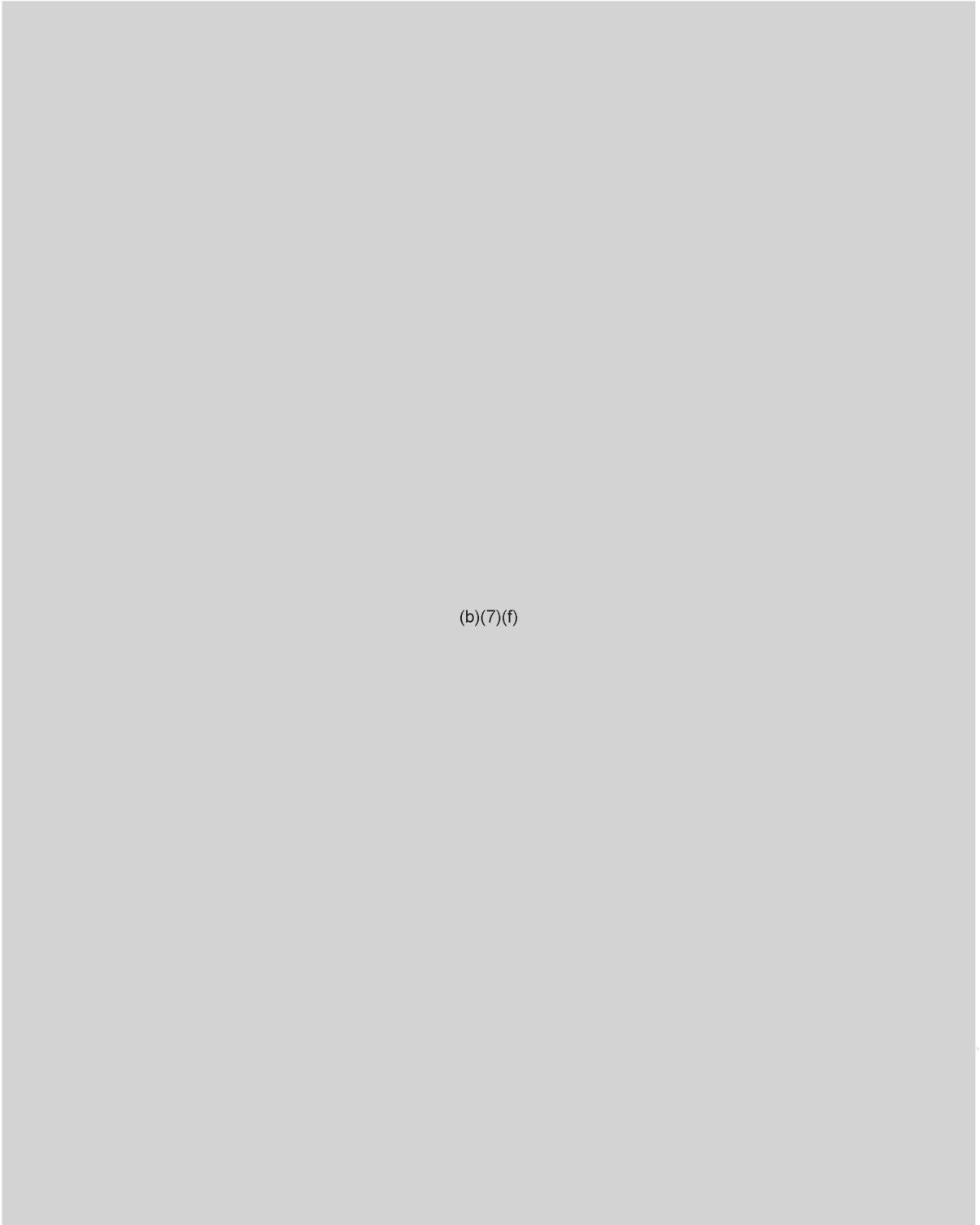
(b)(7)(f)

Table 4-4



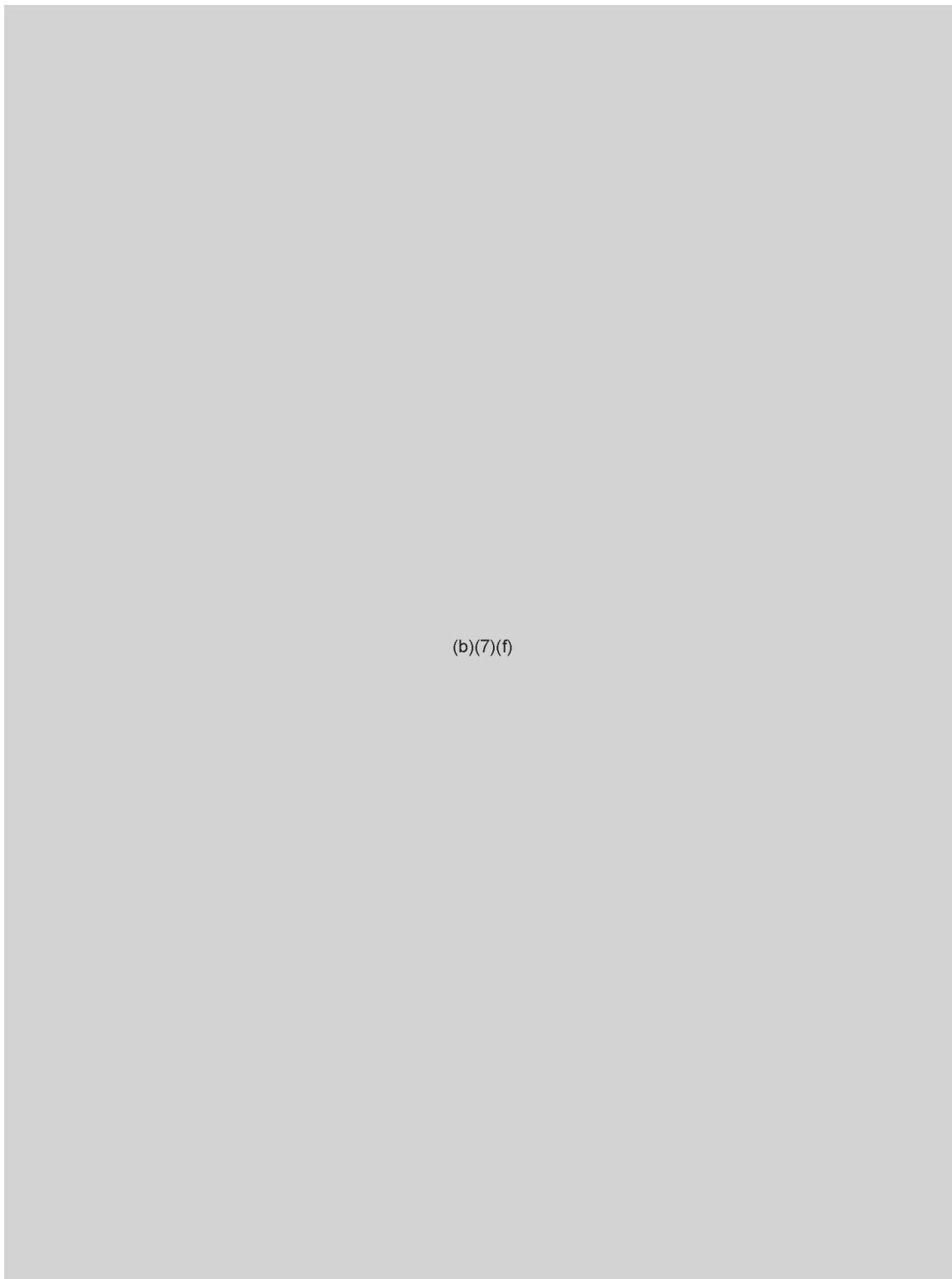
(b)(7)(f)

Table 4-5



(b)(7)(f)

Table 4-6



(b)(7)(f)

Table 4-7

(b)(7)(f)

Table 4-8

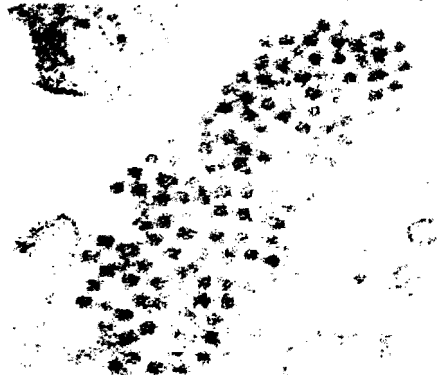


(b)(7)(f)

Table 4-9 Dengue fever virus Information sheet (U)

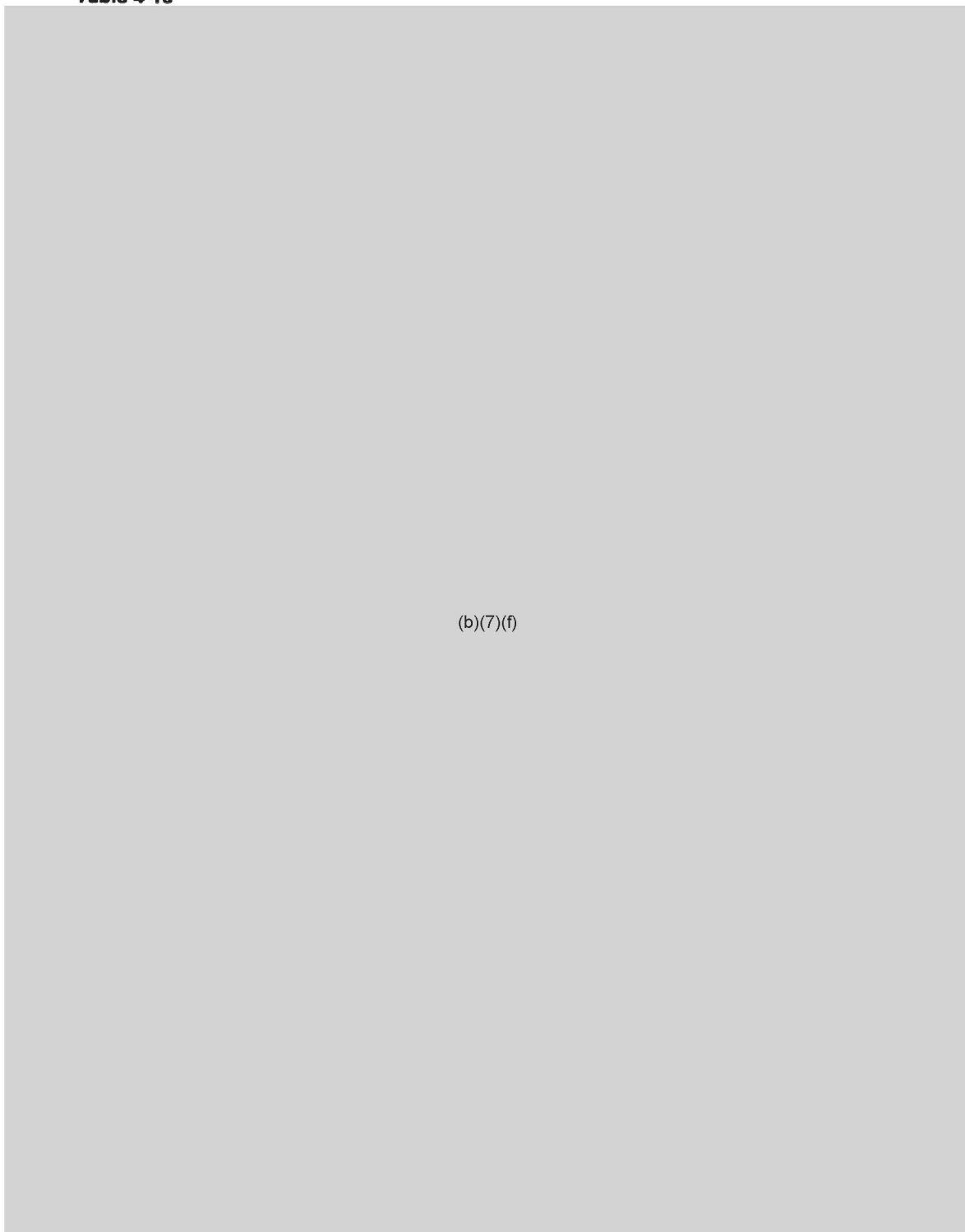
NAME:	Dengue fever virus
SYNONYM OR CROSS REFERENCE:	Dengue fever, breakbone fever, Dengue hemorrhagic fever (DHF), Dengue shock syndrome (DSS)
CHARACTERISTICS:	Spherical enveloped virion 40-50 nm in diameter; single-stranded, positive sense RNA genome surrounded by an icosahedral nucleocapsid; Flaviridae (Flavivirus)
HOST RANGE:	Humans, mosquitoes (as a vector, <i>Aedes spp.</i> , <i>Stegomyia spp.</i>) and non-human primates
INFECTIOUS DOSE:	Unknown
MODE OF TRANSMISSION:	By bite of infectious mosquitoes mainly <i>Aedes aegypti</i> ; most bites occur during the 2 hours after sunrise and several hours before sunset: vertical transmission (infected progeny) does occur, however it is relatively low
INCUBATION PERIOD:	From 3 to 14 days; usually 4 to 7 days
COMMUNICABILITY:	Not directly transmitted from person-to-person; patient infectious for mosquitoes from shortly before to the end of the febrile period, usually 3 to 5 days; mosquitoes infectious 8 to 12 days after blood meal and remains so for life
DRUG SUSCEPTIBILITY:	No specific antivirals
SUSCEPTIBILITY TO DISINFECTANTS:	Susceptible to common disinfectants; 70% ethanol, 1% sodium hypochlorite, 2% glutaraldehyde
SURVIVAL OUTSIDE HOST:	Virus stable in dried blood and exudates up to several days at room temperature
PHYSICAL INACTIVATION:	Sensitive to heat: low pH inactivates dengue virus
PRIMARY HAZARDS:	Accidental parenteral inoculation; contact with broken skin or mucous membrane; aerosols are an uncommon route of laboratory infections but may be a potential source
CONTAINMENT REQUIREMENTS: (Recommended)	Biosafety level 2 practices and containment facilities for all activities involving the virus, manipulation of known or potentially infectious tissues and infectious vectors
STORAGE:	In sealed containers that are appropriately labeled

The contents of this table are UNCLASSIFIED

Figure 4-7 Dengue fever photo (U)

The contents of this figure are UNCLASSIFIED

Table 4-10



(b)(7)(f)

4.5 Facility-Specific Secondary Assets (U)

(U) Table 4-11 lists the secondary assets for SA facilities.

Table 4-11 Secondary Asset Identification (U)

Assets	Priority
Facility: Containment integrity Facility: Security infrastructure Facility: Shipping and receiving area Facility: Use and storage facilities Programmatic equipment	Secondary
Information-unclassified Agent inventories Security plan List of approved individuals/HR data Security database/access records Inspection records Transfer documents Incident reports-security and safety Assessment reports	Secondary
Programmatic equipment, uncontaminated Unique and difficult to replace Non-self protecting (i.e., portable, capable of reverse engineering)	Secondary

The contents of this table are UNCLASSIFIED

4.6 Facility Specific Tertiary Assets (U)

(U) Table 4-12 lists the tertiary assets for SA facilities.

Table 4-12 Tertiary Asset Identification (U)

Assets	Priority
Personnel - researchers - operational personnel/support - personnel - security personnel - responsible official Information (unclassified) - agent inventories - documents - people - systems - agent attribution - facility (physical structure)	Tertiary
Emergency Response Plan Safety plans Training records Research protocols Operational procedures/conduct of operations Drawings/As built	Tertiary
Equipment, uncontaminated Standard Unique and replaceable	Tertiary
Facility: Record storage areas	Tertiary

The contents of this table are UNCLASSIFIED

5.0 Threat Definition and Assessment (U)

5.1 General Threat Identification (U)

(U) Table 5-1, "Threat Definitions," provides a description of the physical threat to the identified assets. The description includes motivations, characteristics, capabilities, and potential actions.

Table 5-1 Threat Definitions (U)

Adversary Class	Threat Definition	Adversary Information	
Insider Type 1	A Department-of-Justice-(DOJ-) approved person with unescorted, authorized (line mgr and noted on CDC registration) access to CFR agents.	Motivation/ characteristics	(b)(7)(f)
		Tactics/ potential actions	
		Capabilities	
Outsider Type 2	Not a DOJ-approved person with escorted, authorized access (visitors, maintenance workers, emergency responders, restricted person).	Motivation/ characteristics	
		Tactics/ potential actions	
		Capabilities	

The contents of this table are UNCLASSIFIED ~~FOUO~~

Table 5-1 Threat Definitions (continued) (U)

Adversary Class	Threat Definition	Adversary Information	
Outsider Type 3:	Unauthorized access with intimate knowledge of security systems and operations. (Security system admin, Facility mgr Engineers, Guards, former employee).	Motivation/ Characteristics	(b)(7)(f)
		Tactics/ Potential Actions	
		Capabilities	
Outsider Type 4:	Unauthorized access with only general knowledge of security system and operations (terrorists, activist/extremist criminals)	Motivation/ Characteristics	
		Tactics/ Potential Actions	
		Capabilities	
(b)(7)(f)			

The contents of this table are ~~UNCLASSIFIED~~ ~~FOUO~~

(U) Table 5-2, "Threat Assessment," describes predetermined adversary potential goals and tactics and relating probability of occurrence to consequence of loss.

Table 5-2 Threat Assessment (U)

Adversary Type (AT)	Tactic	Potential Action	Probability of Occurrence ³	Consequence
Insider Type 1	Stealth	Intent to steal CFR agent	(b)(7)(f)	Primary (PC)
Insider Type 1	Stealth/Force	IFD		Tertiary (TC)
Insider Type 1 Information ⁴	Stealth	Stealing information		Secondary (SC)
Insider Type 1 Information	Stealth	Destroying information		Tertiary
Outsider Type 2	Stealth	Intent to steal CFR agent		Primary
Outsider Type 2	Force	IFD/Dispersal		Tertiary
Outsider Type 2 Information	Stealth	Stealing information		Secondary
Outsider Type 2 Information	Stealth	Observing information		Secondary
Outsider Type 3	Stealth	Steal CFR agent		Primary
Outsider Type 3	Overt	IFD		Tertiary
Outsider Type 2 Information	Covert	Stealing information		Secondary
Outsider Type 3 Information	Covert	Observing information		Secondary
Outsider Type 4	Overt	IFD, political activist		Tertiary
Outsider Type 4	Covert	IFD, political activist		Tertiary
Outsider Type 4	Overt	Steal CFR agent, terrorist		Primary
Outsider Type 4	Covert	Steal CFR agent, terrorist		Primary
Outsider Type 4	Covert	Steal CFR agent, criminal		Primary
Outsider Type 4 Information	Covert	Observe information		Secondary
Outsider Type 4 Information	Covert	Stealing information	Secondary	
(b)(7)(f)				

The contents of this table are UNCLASSIFIED ~~Rev~~

³ The probability of occurrence is directly related to the identified tactics/potential actions for each threat type identified in Table 5-1.

⁴ "Information," i.e., CFR-defined records and all other info that could assist an adversary as defined by the entity, includes paper and electronic information.

5.1.1 Occurrences and Consequences (U)

(U) Table 5-3 connects likelihood and consequences to applicable adversary types/goals.

Table 5-3 Likelihood and Consequences (U)

Likelihood and Consequence	Adversary Type	Risk Level
----------------------------	----------------	------------

(b)(1)

The contents of this table are CONFIDENTIAL

5.2 Risk and Resource Allocation (U)

(U) This step is used to determine the level of risk and resource allocation. The protection system should protect against the defined high-risk threats. Medium- and low-risk threats that are accepted should have incident response plans developed. Very-low-risk threats should be addressed with no-cost, best-management practices and procedures. Table 5-4 depicts risk and resource allocation.

Table 5-4 Risk and Resource Allocation (U)

Probability of Occurrence			
Likely	Likely TC		
Unlikely	Unlikely TC	Unlikely SC	
Level of Consequence	Tertiary	Secondary	Primary
Risk Levels	Very Low	Low	
Resource Allocation/Protective Measures	Procedural changes	Develop incident response plans	

The contents of this table are UNCLASSIFIED

5.3 Design Basis Threat (U)

(U) The current DBT identifies B-368 as a TL-4 facility. (b)(1)

5.3.1 Threat Types (U)

(b)(1)

6.0 Vulnerability Assessment (U)

(U) The methodology utilized to identify vulnerabilities featured a tabletop analysis of SA areas. Members of the TMAG conducted the tabletop analysis with the assistance of subject matter experts related to the facility. Prior to conducting the analysis, the TMAG performed data collection, personnel interviews, and a facility review. With the accuracy of pertinent information verified and the tabletop analysis complete, the TMAG then finalized the assessment by exposing any potential vulnerabilities and providing recommendations for improving the overall security posture of the facility.

6.1 Assessment Results (U)

(b)(1)

6.2 Identified Vulnerabilities (U)

~~(S)~~

(b)(7)(f)

6.3 Protection System Effectiveness (U)

(b)(7)(f)

(b)(1)

Table 6-1 Adversary Table (U)
(b)(1)

The contents of this table are CONFIDENTIAL

7.0 Other Recommendations to Consider (U)

(U) Although there are currently no security enhancements to consider, the TMAG will conduct annual reviews of this threat assessment to verify that policies and procedures are being effectively utilized or when the DBT is modified. Applicable upgrade recommendations will be given at the conclusion of each review to help sustain an effective security culture within the BSL 3 and to help prevent and mitigate hostile acts with SAs.

8.0 Concurrences and Approvals (U)

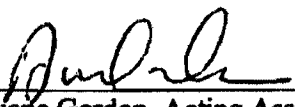
8.1 Preparation and Review (U)

(U) Prepared By:


Lawrence Livermore National Laboratory

(U) Reviewed By:

Lawrence Livermore National Laboratory

 8/15/05

Duane Gordon, Acting Assistant Manager Date
Safeguards and Security Division
National Nuclear Security Administration
Livermore Site Office

 8/15/05

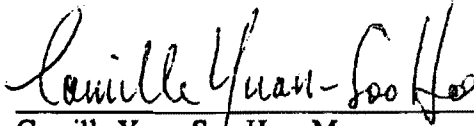
Richard W. Mortensen, Deputy Manager Date
National Security Operations
National Nuclear Security Administration
Livermore Site Office

8.2 Approvals (U)

(U) Approved By:

Lawrence Livermore National Laboratory

Lawrence Livermore National Laboratory

 8/15/05

Camille Yuan-Soo Hoo, Manager Date
National Nuclear Security Administration
Livermore Site Office

Appendix A: List of Pathogens, Agents, and Toxins (U)

APHIS Plant Pathogens, HHS Select Infectious Agents, and USDA High Consequence Livestock Pathogens or Toxins (U)

Viruses

1. African horse sickness virus ^B
2. African swine fever virus ^B
3. Akabane virus ^B
4. Avian influenza virus (highly pathogenic) ^B
5. Blue tongue virus (exotic) ^B
6. Camel pox virus ^B
7. Cercarial dermatitis virus (Herpes B virus) ^B
8. Classical swine fever virus ^B
9. Crimean-Congo haemorrhagic fever virus ^B
10. Eastern equine encephalitis virus ^X
11. Ebola viruses ^B
12. Foot and mouth disease virus ^B
13. Goat pox virus ^B
14. Japanese encephalitis virus ^B
15. Lassa fever virus ^B
16. Lumpy skin disease virus ^B
17. Malignant catarrhal fever ^B
18. Marburg virus ^B
19. Menangle virus ^B
20. Monkeypox virus ^B
21. Newcastle disease virus (exotic) ^B
22. Nipah and Hendra complex viruses ^X
23. Peste des petits ruminants ^B
24. Plum pox potyvirus ^B
25. Rift Valley fever virus ^X
26. Rinderpest virus ^B
27. Sheep pox ^B
28. South American haemorrhagic fever viruses [(Junin, Machupo, Sabia, Flexal, Guanarito)] ^B
29. Swine vesicular disease virus ^B
30. Tick-borne encephalitis complex (flavi) viruses [Central European Tick-borne encephalitis, Far Eastern Tick-borne encephalitis (Russian Spring and Summer encephalitis, Kyasanur Forest disease, Omsk Hemorrhagic Fever)] ^B
31. Variola major virus (Smallpox virus) and Variola minor (Alastrim) ^B
32. Venezuelan equine encephalitis virus ^X
33. Vesicular stomatitis virus (exotic) ^B

Prion

1. Bovine spongiform encephalopathy agent ^B

Toxins

1. Abrin ^B
2. Botulinum neurotoxins ^X
3. *Clostridium perfringens* epsilon toxin ^X
4. Conotoxins ^B
5. Diacetoxyscirpenol ^B
6. Ricin ^B
7. Saxitoxin ^B
8. Shigatoxin and Shiga-like ribosome inactivating proteins ^X
9. Staphylococcal enterotoxins ^X
10. Tetrodotoxin ^B
11. T-2 toxin ^X

Bacteria

1. *Bacillus anthracis* ^X
2. Botulinum neurotoxin producing strains of *Clostridium* ^X
3. *Brucella abortus* ^X
4. *Brucella melitensis* ^X
5. *Brucella suis* ^X
6. *Burkholderia mallei* ^X
7. *Burkholderia pseudomallei* ^X
8. *Coxiella burnetii* ^X
9. *Cowdria Ruminantium* (Heartwater) ^B
10. *Francisella tularensis* ^X
11. *Liberobacter africanus*, *Liberobacter asiaticus* ^B
12. *Mycoplasma capricolum*/M. F38/M. *mycoides* capri (contagious caprine pleuropneumonia agent) ^B
13. *Mycoplasma mycoides* (contagious bovine pleuropneumonia agent) ^B
14. *Ralstonia solanacearum* Race 3 ^B
15. *Rickettsia prowazekii* ^B
16. *Rickettsia rickettsii* ^B
17. *Xanthomonas oryzae* pv. *oryzicola* ^B
18. *Xylella fastidiosa* (citrus variegated chlorosis strain) ^B
19. *Yersinia pestis* ^B

Fungi

1. *Coccidioides immitis* ^X
2. *Coccidioides posadasii* ^B
3. *Peronosclerospora philippinensis* ^B
4. *Phakopsora pachyrhizi* ^B
5. *Sclerotinia reyesii* var. *zoeae* ^B
6. *Synchytrium endobioticum* ^B

Exemptions

The following agents or toxins are exempt if the aggregate amount under the control of a principal investigator does not, at any time, exceed:

- 0.5 mg of Botulinum neurotoxins
- 5 mg of *Staphylococcal* enterotoxins
- 100 mg of abrin, *Clostridium perfringens* epsilon toxin, conotoxin, ricin, saxitoxin, shigatoxin, shiga-like ribosome inactivating protein, and tetrodotoxin
- 1,000 mg of diacetoxyscirpenol and T-2 toxin

The following agents or toxins are also exempt:

- Any agent or toxin that is in its naturally occurring environment provided it has not been intentionally introduced, cultivated, collected, or otherwise extracted from its natural source.
- Non-viable SA organisms or nonfunctional toxins.
- The vaccine strains of Junin virus (Candid #1), Rift Valley fever virus (MP-12), Venezuelan Equine encephalitis virus vaccine strain TC-83.

The medical use of toxins for patient treatment is exempt.

Genetic Elements, Recombinant Nucleic Acids, and Recombinant Organisms

1. SA viral nucleic acids (synthetic or naturally derived, contiguous or fragmented, in host chromosomes or in expression vectors) that can encode infectious and/or replication competent forms of any of the SA viruses.
2. Nucleic acids (synthetic or naturally derived) that encode for the functional form(s) of any of the listed toxins if the nucleic acids: a) are in a vector or host chromosome; b) can be expressed *in vivo* or *in vitro*; or c) are in a vector or host chromosome and can be expressed *in vivo* or *in vitro*.
3. Listed viruses, bacteria, fungi, and toxins that have been genetically modified.

Other Restrictions

1. Experiments utilizing recombinant DNA that involve the deliberate transfer of a drug resistance trait to the listed agents that are not known to acquire the trait naturally, if such acquisition could compromise the use of the drug to control disease agents in humans, veterinary medicine, or agriculture.
2. Experiments involving the deliberate formation of recombinant DNA containing genes for the biosynthesis of listed toxins lethal for vertebrates at an LD50 < 100 ng/kg body weight.

The contents of this table are UNCLASSIFIED



Lawrence Livermore National Laboratory

Plans, Policies and Procedures

Biological Select Agents and Toxins Security Plan

Revision 6

March 9, 2006

OFFICIAL USE ONLY	
May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption and category.	
<u>Exemption 2, Circumvention of Statute</u>	
Department of Energy review required before public release	
Date: <u>March 9, 2006</u>	
Name/org:	(b)(6)

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This work performed under the auspices of the U.S. Department of Energy by University of California, Lawrence Livermore National Laboratory under Contract W-7405-ENG-48.

Review and Approval

Prepared by:

(b)(6)

3/21/06
Date

**Program Security Representative
Security Department**

Reviewed by:

(b)(6)

3/29/06
Date

LLNL Responsible Official

(b)(6)

3/27/06
Date

**Deputy Department Head
Security Department**

**Duane G. Gordon
Assistant Manager
National Nuclear Security Administration
Safeguards and Security Organization
Livermore Site Office**

Date

Approved by:

(b)(6)

4-3-06
Date

Safeguards and Security Organization

**Camille Yuan-Soo Hoo
National Nuclear Security Administration
Livermore Site Manager**

Date

Document Revision History

REV #	Date	Author	Summary of Changes
Initial	12 June 2003	(b)(6)	
Rev 1	1 December 2003		Added procedures for registration of facilities and staff risk assessment for individuals. Added inventory guidelines.
Rev 2	7 January 2004		Clarified alarm response procedures and SDO reporting.
Rev 3	19 May 2004		Modified by LSO comments.
Rev 4	11 June 2004		Further modifications by LSO comments.
Rev 4	19 July 2004		RCR sent to LSO for approval.
Rev 4	18 November 2004		Received approved RCR from LSO.
Rev 5	13 December 2004		Addition of requirement to abide by LLNL policies and procedures, addition of SAHRP as attachment.
Rev 6	9 March 2006		Annual Review, rescinding (b)(7)(F) (b)(7)(F) select agent plans and incorporating them as appendices of this plan. Addition of wording to meet comments made by CDC during the August 2005 inspection.

Table of Contents

Acronyms	viii
1.0 Purpose	1
2.0 Scope	1
3.0 References	2
4.0 Definitions	3
5.0 Roles and Responsibilities	5
5.1 The Responsible Official (RO)	5
5.2 Select Agent Principal Investigators (PI)/ Responsible Individual (RI)	6
5.3 Select Agent Program Security Representative (PSR)	7
5.4 Security Department (SD) Threat Mitigation Analysis Group (TMAG)	7
5.5 Security Department Protective Force Division (PFD)	7
5.6 Individual Responsibilities	8
5.7 Select Agent Manager (SAM)	9
5.8 Select Agent Facility Manager (SAFM)	9
5.9 Facility Point of Contact (FPOC)	10
5.10 Associate Program Leader for Select Agent Science (APL)	10
5.11 Senior Laboratory Coordinator (SLC)	10
5.12 Padlock Custodian	10
5.13 Assurance Office Manager	10
6.0 Description of Work	10
7.0 Security Risk and Threat Assessment of Biological Select Agents or Toxins	11
8.0 Facility Registration	11
9.0 Staff Security Risk Assessment	11
10.0 Select Agent Human Reliability Program (SAHRP)	12
11.0 Access Authorization	12
11.1 Unescorted Access	12
11.2 Visitor Access	12
11.3 Foreign National Access	12
11.4 Cleaning Access	13
11.5 Access Additions & Deletions	13
12.0 SA Access	13
12.1 Building Resident Access	13
12.2 SAA Access Recordkeeping	13
13.0 Terminations	14

14.0	Accountability and Control of Biological SAs and Toxins.....	15
14.1	Inventory	15
14.2	Inventory Records.....	15
14.3	Inventory Oversight	15
15.0	Disposal.....	15
16.0	Receipt and Shipping of SAs by LLNL.....	16
17.0	Transfer of Select Biological Agents and Toxins	16
17.1	Offsite.....	16
17.2	Onsite.....	17
17.3	(b)(7)(F)	17
18.0	Physical Security	17
18.1	Facility Access Procedures.....	17
18.2	(b)(7)(F)	18
19.0	18
20.0	General Security	19
21.0	Personnel Suitability.....	19
21.1	Employee Assistance Program (EAP).....	19
21.2	Alcohol and Substance Abuse Prevention for Employees (ASAP).....	19
21.3	ASAP Education Program for Management.....	19
21.4	Select Agent Human Reliability Program (SAHRP)	19
22.0	Information Security.....	20
23.0	Cyber Security	20
24.0	Feedback and Improvement.....	20
24.1	Annual Security Risk Assessments	20
24.2	Security Plan Review	20
24.3	Security Incident Review	21
25.0	Espionage.....	21
26.0	Operations Security	21
27.0	Visitors.....	21
28.0	Training	21
28.1	Approved Authorized Personnel	21
28.2	Visitor Security Briefing.....	21
28.3	Drills or exercises	22
29.0	Emergency Response.....	22
29.1	Security Incidents.....	22
29.2	Security Alarm Response	23

30.0	Incident Reporting	23
30.1	Report Contents.....	24
30.2	Report Notification Process.....	24
31.0	Public Relations	25
32.0	Change Control	25
Attachment 1	Select Agent Visitor Security Briefing.....	26
Attachment 2	Select Agent Laboratory Access Record	27
Appendix A -	(b)(7)(F)	28
1.0	Purpose	28
2.0	Scope	28
3.0	Description of Work	28
4.0	Security Risk and Threat Assessment of Biological SAs or Toxins.....	28
5.0	Facility Registration.....	28
6.0	Access Authorization for Visitors.....	28
6.1	Visitor Access to the hallway	28
6.2	Visitor Access to the laboratories.....	28
6.3	Physical Security	28
Appendix B -	(b)(7)(F)	30
1.0	Purpose	30
2.0	Scope	30
3.0	Description of Work	30
4.0	Security Risk and Threat Assessment of Biological SAs or Toxins.....	30
5.0	Facility Registration.....	30
6.0	Access	30
6.1	Access Authorization	30
6.2	Building Resident Access.....	30
6.3	Access Requirements.....	31
6.4	Access System Enrollment.....	31
6.5	Access to the Mechanical Room.....	32
6.6	Access to the laboratory area during maintenance windows.....	32
6.7	Access during an emergency.....	33
6.8	Building Access Procedures	33
6.9	Badge Exchange	34
6.10	Laboratory Access Procedures	34
6.11	Escorted Access Procedures	34
6.12	Physical Security	35
6.13	(b)(7)(F)	36

6.14	(b)(7)(F)	37
6.15	Cyber Security	37

Acronyms

ADC	Authorized Derivative Classifier
APHIS	Animal and Plant Health Inspection Service
APL	Associate Program Leader
ARO	Alternate Responsible Official
ASAP	Alcohol and Substance Abuse Program
BIO	Biosciences Directorate
BMBL	Biosafety for Microbiological and Biomedical Laboratories
BSL	Biosafety Level
BSO	Biosafety Officer
CAS	Central Alarm Station
CBNP	Chemical and Biological National Security Program
CDC	Center for Disease Control
CFR	Code of Federal Regulations
CSO	Cyber Security Operations
DADO	Deputy Associate Director of Operations
DDH	Deputy Department Head
DHHS	Department of Health and Human Services
DOE	Department of Energy
DOJ	Department of Justice
EAP	Employee Assistance Program
ES&H	Environment, Safety and Health
ESHO	Environment, Safety and Health Officer
FBI	Federal Bureau of Investigation
FPOC	Facility Point of Contact
HRP	Human Reliability Program
ISSM	Integrated Safeguards and Security Management
IWS/SP	Integrated Worksheet/Safety Plan
LANL	Los Alamos National Laboratory
LBI	Limited background investigation
LBNL	Lawrence Berkley National Laboratory
LLNL	Lawrence Livermore National Laboratory
LSO	Livermore Site Office
LTRAIN	Livermore Training Records and Information Network
MDD	Materials Distribution Division
NACI	National agency check with inquiries
NHI	Nonproliferation, Homeland and International Security Directorate
NNSA	National Nuclear Security Administration
OPSEC	Operations Security
ORPS	Occurrence Reporting and Processing System
PAS	Proximity Access System
PFD	Protective Force Division
PI	Principal Investigator
PIN	Personal Identification Number
PPOC	Program Point of Contact
PSR	Program Security Representative
RI	Responsible Individual

RO	Responsible Official
SA	Select Agent or Toxins
SAA	Select Agent Area
SAFE	Security Awareness For Employees
SAFM	Select Agent Facility Manager
SAHRP	Select Agent Human Reliability Program
SAM	Select Agent Manager
SD	Security Department
SDO	Security Duty Officer
SIRO	Security Incident Reporting Office
SLC	Senior Laboratory Coordinator
SNL	Sandia National Laboratory
SOP	Standard Operating Procedure
SPA	Safe Plan of Action
SPO	Security Police Officer
SRA	Security risk assessment
SRLM	Security responsible line manager
TMAG	Threat Mitigation Analysis Group
UC	University of California
UCI	Unclassified Controlled Information
USDA	United States Department of Agriculture

1.0 Purpose

The Lawrence Livermore National Laboratory (LLNL) *Biological Select Agents and Toxins Security Plan* provides an integrated safeguards and security management (ISSM) approach to implementing a protection program for LLNL's Select Agent¹ (SA)/toxin use and storage areas.

This security plan complies with the Code of Federal Regulations (CFR) requirements of 42 CFR Part 73, US Department of Health and Human Services (DHHS), March 18, 2005; 7 CFR Part 331, US Department of Agriculture (USDA), March 18, 2005; 7 CFR Part 121, USDA, March 18, 2005 (hereafter referred to as the CFRs) and the guidance provided in Appendix F of the Biosafety for Microbiological and Biomedical Laboratories (BMBL)².

A risk methodology, that was agreed to during a meeting of the University of California (UC)/National Nuclear Security Administration (NNSA)/Sandia National Laboratories (SNL)/Department of Energy (DOE) Risk and Threat Assessment Methodology Working Group, held in Albuquerque, NM, April 8-9, 2003, guides the development of the security risk and threat assessments. The security plan format was developed through collaboration between LLNL, Los Alamos National Laboratory (LANL), Lawrence Berkeley National Laboratory (LBNL), UC, NNSA, and DOE.

All SA work will be done in accordance with the Institutional Select Agent Management Structure in which the security of the SAs is monitored by the SA Program Security Representative (PSR). All Directorates owning or managing a Select Agent Area (SAA) will abide by this institutional plan and develop an appendix to this plan outlining any additional security information or requirements specific to their SAA. The facility specific appendices will be developed in collaboration with the Responsible Official (RO) and the PSR assigned to the owning Directorate.

The SAA personnel will abide by the LLNL institutional policies and procedures, such as cyber and information security, which are not specifically addressed in this plan. All operations are governed by DOE/NNSA classification guidance, or other guidance as appropriately determined by the local Classification Officer of authority to be adequate and not contradictory with DOE/NNSA guidance.

2.0 Scope

This plan applies to personnel entering any select agent facility at LLNL. All personnel assigned to a select agent facility or working in the facility temporarily are responsible for understanding and implementing the requirements of this document and for ensuring any visitors under their escort are briefed on their responsibilities prior to being escorted into the facility. Individuals who are unable to meet all of the requirements of this security plan will be removed from the select agent facility access list.

¹ Lists of the Select Agents, which this plan applies to, can be obtained from the Responsible Official (RO) or from the internet at <<http://www.cdc.gov/od/sap/>>.

² *Biosafety in Microbiological and Biomedical Laboratories (BMBL) 4th Edition*, U.S. Department of Health and Human Services, Centers for Disease Control and Prevention and National Institutes of Health, Fourth Edition, May 1999, Appendix F as updated on the internet <<http://www.cdc.gov/od/ohs/biosfty/bmb4/b4af.htm>>, December 5, 2002

3.0 References

42 CFR Part 73, *Possession, Use, and Transfer of Biological Agents and Toxins*, (humans) US Department of Health and Human Services (DHHS), March 18, 2005

7 CFR Part 331, *Agriculture Bioterrorism Protection Act of 2002: Possession, Use, and Transfer of Biological Agents and Toxins* (plants) US Department of Agriculture (USDA), March 18, 2005

9 CFR Part 121, *Agriculture Bioterrorism Protection Act of 2002: Possession, Use, and Transfer of Biological Agents and Toxins* (animals) USDA, March 18, 2005

(b)(7)(F)

Biosafety for Microbiological and Biomedical Laboratories (BMBL), Center for Disease Control, 4th edition, as updated on the internet at <http://www.cdc.gov/od/ohs/biosfty/bmbl4/b4af.htm>, December 5, 2002

Biosciences Standard Operating Procedure, *Exchanging Select Agent*

Biosciences Standard Operating Procedure, *Inventory Of Select Agents*.

Biosciences Standard Operating Procedure, *Receiving Biological Materials*

Biosciences Standard Operating Procedure, *Shipping Biological Materials*

CG-CB-2, *Classification Guide for Chemical/Biological Defense Information*

CG-SS-4, *Classification and UCNI Guide for Safeguards and Security Information*

DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, Change 1, March 7, 2006

DOE M 470.4-2, *Physical Protection Program Manual*, Change 1, March 7, 2006

DOE M 470.4-3, *Protective Force*, Change 1, March 7, 2006

DOE M 470.4-4, *Information Security*, August 26, 2005

DOE M 470.4-5, *Personnel Security*, August 26, 2005

DOE O 470.4, *Safeguards and Security Program*, August 26, 2005.

DOE O 470.3, *Design Basis Threat (DBT) Order*, October 18, 2004, as updated to DOE O 470.3A by memo dated November 29, 2005.

Institutional Select Agent Management Structure, January 6, 2006
Lawrence Livermore National Laboratory Locks, Keys and TESA Policy and Procedures, September 30, 2005

LLNL Site Safeguards and Security Plan, January 31, 2005

Material Distribution Division Operating Procedures, Section 200.20, Infectious Substances and Etiologic Agent

Material Distribution Division Operating Procedures, Section 301.1, Basic Receiving and Distribution

UC/NNSA/SNL/DOE Risk and Threat Assessment Methodology Working Group Report, April 2003.

4.0 Definitions

Approved Person— A person who has been reviewed by the Department of Justice (DOJ) and approved by the DHHS or USDA to access biological SA or Toxins in accordance with 42CFR73.8. Unless a shorter period of time is granted under 42CFR73.8, an approval for an individual will be valid for 5 years unless terminated sooner.

Associate Program Leader for Select Agent Science (APL) – Oversees direction of Select Agent research and funding. The APL reports to Deputy Division Leader for Chem/Bio Programs.

Authorized Approved Person— An Approved Person, who is authorized by a LLNL line manager to access SA or toxins in specific use/storage areas, and is enrolled in the Select Agent Human Reliability Program (SAHRP).

(b)(7)(F)

Biological Agent— Any microorganism (including, but not limited to, bacteria, viruses, fungi, rickettsiae, or protozoa) or infectious substance, or any naturally occurring, bioengineered, or synthesized component of any such microorganism or infectious substance, capable of causing death, disease, or other biological malfunction in a human, an animal, a plant, or another living organism; deterioration of food, water, equipment, supplies, or material of any kind; or deleterious alteration of the environment.

DHHS Select Agent or Toxin – A biological agent or toxin defined by the Department of Health and Human Services (DHHS) in 42 CFR 73, "Possession, Use, and Transfer of Select Agents and Toxins."

Facility Point of Contact – For the purposes of this document, a representative of the SAFM who coordinates facility maintenance activities and acts as backup to the SAFM for select agent laboratory access systems enrollment.

Laboratory – The individual room where SAs are handled.

Overlap Agent or Toxin – A biological agent or toxin as defined in both 42 CFR 73 "Possession, Use, and Transfer of Select Agents and Toxins" and 9 CFR Part 121, "Agricultural Bioterrorism Protection Act of 2002; Possession, Use, and Transfer of Biological Agents and Toxins."

Padlock Custodian – An individual appointed by the SAFM to maintain padlocks used to secure Select Agent storage containers.

(b)(7)(F)

Piggybacking – Entering a security area with or behind a cleared authorized person who has vouched for the accompanying individual's authorization for access. (See also **Vouching**.)

Principal Investigator (PI)/Responsible Individual (RI) – The programmatic person responsible for activities in a specific laboratory.

(b)(7)(F)

Select Agent Area (SAA) – The room or laboratory where SA/toxin is used and/or stored.

Select Agent Facility Manager (SAFM) – The individual providing safety, security and facility operation direction for select agent area activities. The person responsible for ensuring all security requirements have been met prior to approving access to the Select Agent Area.

Select Agent Human Reliability Program (SAHRP) – A LLNL security and safety reliability program to select, train, certify and monitor individuals whose work requires unescorted access to Select Agents or toxins listed by the DHHS. The SAHRP process is outlined in the LLNL Select Agent Human Reliability Program Implementation Plan. The LLNL Assurance Office Manager acts as the certifying official for the SAHRP.

Select Agent Manager (SAM) – The individual appointed by the Nonproliferation, Homeland and International Security Directorate (NHI) to provide program direction for select agent activities.

Select Agent or Toxin (SA) – All of those biological agents or toxins included in 42 CFR 73, "Possession, Use, and Transfer of Select Agents and Toxins" or 7 CFR 331/9 CFR 121, "Agricultural Bioterrorism Protection Act of 2002; Possession, Use, and Transfer of Biological Agents and Toxins."

Senior Laboratory Coordinator (SLC)— The individual appointed by NHI to provide daily supervision of SA research activities.

Toxin— The toxic material or product of plants, animals, microorganisms (including, but not limited to bacteria, viruses, fungi, rickettsiae, or protozoa) or infectious substances, or a recombinant or synthesized molecule, whatever their origin and method of production, including any poisonous substance or biological product that may be engineered as a result of biotechnology, produced by a living organism; or any poisonous isomer or biological product, homolog, or derivative of such a substance.

USDA Select Agent or Toxin— A biological agent or toxin included in 7 CFR 331/9CFR 121, "Agricultural Bioterrorism Protection Act of 2002; Possession, Use and Transfer of Biological Agents and Toxins."

Visitor— A visitor is any individual who is not an authorized, approved individual and who needs to access the SAA to further the business of that facility. Visitors include scientific collaborators, inspectors, NNSA oversight personnel, and maintenance staff. All visitors shall have authorization to access the LLNL site and possess a valid DOE identification badge. In general, all SAs or toxins should be secured whenever a visitor is in the SAA. The only exception to this is that a scientific collaborator may observe a SA activity for the purpose of advising on the process. Under no circumstances shall a visitor have direct access to a SA.

Vouching— Visually verifying the access authorization of another person for the purpose of piggybacking into a security area. (See also Piggybacking.)

5.0 Roles and Responsibilities

Roles and Responsibilities for persons involved in the SA Program are outlined in this section. Roles and Responsibilities for SA facilities which require additional personnel are listed in the facility specific appendix in this plan.

5.1 The Responsible Official (RO)

The RO is an approved person, designated by LLNL, with the authority and responsibility to ensure that the requirements of the SA regulations are met. Specific security related responsibilities of the RO include ensuring compliance with the regulations (CFRs) and this Security Plan including the following:

- Developing and implementing security plans in accordance with 42 CFR 73.11, 7 CFR 331.11, and 9 CFR 121.12.
- Maintaining a list of individuals who have been reviewed by DOJ, approved by DHHS or USDA, and authorized by LLNL management for access to SA or toxins.
- Authorizing, in concert with the Principal Investigator/Responsible Individual (PI/RI), only DOJ reviewed and DHHS or USDA approved individuals within LLNL to have unescorted access to registered SAs or toxins.
- Ensuring appropriate training in security procedures for all personnel is conducted.
- Ensuring SAs or toxins are transferred only to registered individuals or entities.

(b)(7)(F)

- Ensuring that all visitors are informed of and follow LLNL's SA security requirements and procedures.

- Providing immediate notice of the discovery of any theft, loss, or release of a biological agent or toxin. Maintaining detailed records of information necessary to give a complete accounting of all of the entity's activities related to agents or toxins.
- Briefing management on security concerns or incidents and keeping them informed on program items that need special security considerations.
- Ensuring that the *LLNL Environment, Safety & Health Manual* is current and comprehensive with regard to security policies and procedures that govern practices at LLNL SAAs.
- Ensure security plans are coordinated with safety and emergency response plans for compatibility.
- Reviewing the LLNL SA Security Plan annually, and after any security incident and making modifications as necessary.
- Approving, with the PSR, new SAAs.
- Reviewing the specific SAA security plan after any security incident occurring at the area.
- Ensuring all PI/RIs meet educational and experience criteria necessary for safely working in a biological laboratory.
- Providing documentation to the SAFM regarding permit approval for SA employees.
- Conducting random reviews of the inventory records.
- Conducting annual inventories of the SAs.

In the absence of the RO, the Alternate Responsible Official (ARO) assumes all of the roles and responsibilities of the RO.

5.2 Select Agent Principal Investigators (PI)/ Responsible Individual (RI)

The PI/RI plan and manage the work in their respective laboratories.

The SA PI/RI are responsible for:

- (b)(7)(F)
- Concurring, in concert with the SAM, additions to the access list for their laboratory.
 - Permitting access to SA/toxin use or storage areas only to authorized, approved individuals or properly escorted visitors.
 - Ensuring visitors are escorted and continually monitored by approved, authorized individuals when they are in the laboratory.
 - Ensuring that storage containers for SAs or toxins are locked when they are not in direct view of approved, authorized staff.
 - Ensuring that locks and keys used for locking refrigerators/freezers and storage boxes are provided only to approved, authorized individuals and that the keys are controlled and accounted for.
 - Ensuring that all packages are inspected upon entry to or exit from a SA or toxin use and/or storage area for evidence of gross tampering, appropriate labeling and permitting.
 - Reporting any SAs or toxins incidents to the RO and SAM.
 - Approving any visits to their laboratory.
 - Maintaining inventory and access records.
 - Obtaining RO and CDC/Animal and Plant Health Inspection Service (APHIS) approvals before transferring SAs or toxins.

- Ensuring all personnel working in the SAA meet educational and experience criteria necessary for safely working in a biological laboratory.
- Assuring their staff receive appropriate training to comply with classification policies and procedures.

5.3 Select Agent Program Security Representative (PSR)

The PSR serves as a liaison between the Security Department (SD), the Livermore Site Office (LSO) Safeguards and Security Division, the RO, and the Directorate owning a SAA.

The PSR is responsible for:

- Coordination of security services and acts in an advisory capacity for security issues.
- Briefing management on security concerns or incidents and keeping them informed on program items that need special security considerations.
- Working with Program/Directorate management to develop an understanding of and support for SD efforts and activities.
- Approving, with the RO, new SAAs.
- Writing security plans (i.e. for new construction, visits) for non-routine activities with security requirements.
- Developing with the SAA owning Directorate specific security responsibilities.
- Assisting Program/Directorate with special security needs as requested (i.e., Operations Security (OPSEC), physical security, computer security).
- Reviewing the LLNL SA Security Plan annually, and after any incident of security concern, should one occur.
- Updating the LLNL SA Security Plan as needed.

5.4 Security Department (SD) Threat Mitigation Analysis Group (TMAG)

TMAG conducts the security risk and threat assessment of biological SAs or toxins, which forms the basis for the SA/toxin security plans.

The TMAG is responsible for:

- Reviewing the SA Security Risk and Threat Assessments annually.
- Updating the SA Security Risk and Threat Assessments as needed.
- Reviewing the LLNL SA Security Plan annually, and after any incident of security concern, should one occur.

5.5 Security Department Protective Force Division (PFD)

PFD responds to security incidents involving SAs and toxins.

PFD is responsible for:

- Responding to security alarms involving the SAs or toxins while the SAs or toxins are protected by the alarm system.
- Writing incident reports for any incident involving the SAs or toxins such as the loss of keys or access cards or alarm responses.
- Removing or providing assistance to the facility personnel for the removal of unauthorized personnel in the SA facility.
- In accordance with existing federal and/or state law, dealing with criminal activity that occurs prior to or during emergency event at a SAA. PFD Orders specifically

outline procedures as to arrest, search, seizure, detention and the use of force in these circumstances.

5.6 Individual Responsibilities**5.6.1 Authorized approved personnel working in a SA facility are responsible for:**

- Understanding and implementing the requirements of the LLNL *Biological Select Agents and Toxins Security Plan*.
- Understanding and implementing the requirements of the facility specific appendix located at the end of this plan.
- Maintaining SAHRP enrollment when applicable
- Ensuring that all visitors are informed of and follow LLNL's SA security requirements and procedures. (see Appendix 1)
- Providing immediate notice of the discovery of any theft, loss, or release of a biological agent or toxin.
- Informing management on security concerns or incidents and keeping them informed on program items that need special security considerations.

(b)(7)(F)

- Reporting any SAs or toxins incidents to the RO.
- Maintaining detailed records of information necessary to give a complete accounting of all of the entity's activities related to agents or toxins.
- Reporting to the RO any sign that inventory or use records for SAs or toxins, have been altered or otherwise compromised.
- Inspecting packages they bring into or remove from a SA or toxin use or storage area for evidence of gross tampering, appropriate labeling and permitting.
- Reporting immediately to the RO any abnormalities discovered during the package inspection.
- Ensuring that storage containers for SAs or toxins are locked when they are not in direct view of approved, authorized staff.
- Ensuring that locks and keys or combinations used for locking refrigerators/freezers and storage boxes are provided only to approved, authorized individuals and that the keys are controlled and accounted for.
- Allowing only persons needed to further the business of the SA facility to enter the facility or any of the individual SA laboratories within the facility. Questions regarding access should be addressed to the RO or SAFM.

(b)(7)(F)

- Permitting access to SA or toxin use or storage areas only to authorized, approved individuals or properly escorted visitors.
- Ensuring visitors are escorted and continually monitored when they are in the laboratory.
- Ensuring visitors have no direct access to SAs.
- Taking all training identified for access to the SAA in a timely manner.
- In accordance with Laboratory policy, complying with the directives of LLNL Security personnel during an emergency event. Failure to comply will result in appropriate disciplinary action up to and including dismissal.

5.6.2 For those persons visiting a SA facility including scientific collaborators responsibilities are as follows:

- Remaining with the escort at all times while in the SAA.

- Following all directions of their escort.

(b)(7)(F)

- Not permitting others to enter the building.

5.6.3 For authorized approved persons escorting visitors in SA facilities responsibilities are as follows:

- Briefing the visitor on security requirements prior to entry into the SAA.
- Remaining with the visitor at all times while in the SAA.

(b)(7)(F)

- Ensuring a Safe Plan of Action (SPA) has been completed.

5.6.4 Security Department Alarm Testers and Security Administrators are responsible for:

- Scheduling alarm testing with the SAFM.
- Entering the SA Facility only with an approved authorized building resident.
- Informing the PSR of any discrepancies or problems with the alarm systems in the SA facilities.

5.7 Select Agent Manager (SAM)

The SAM is responsible for:

(b)(7)(F)

- Providing direction for SA activities.
- Approving, in conjunction with the SAFM and the SLC, access to SA laboratories for scientific collaborators.
- Implementing inventory procedures.
- Overseeing of all aspects of SA work except those specifically the responsibility of the RO.
- Working with the PSR to ensure security requirements are satisfied.

(b)(7)(F)

- Ensuring SAHRP enrollment is current.

The SA Manager's designated alternate is the APL unless otherwise noted in the facility specific appendices attached to this document.

5.8 Select Agent Facility Manager (SAFM)

The SAFM is responsible for:

(b)(7)(F)

- Reviewing of an employee's compliance with security requirements prior to allowing access to a SA laboratory.

(b)(7)(F)

- Providing SA laboratory access to authorized approved personnel with concurrence from the SAM.
- Briefing personnel on the operation of the use of the access system.
- Review of an employee's compliance with training, safety, security, and permit requirements prior to allowing access.

(b)(7)(F)

- Requesting documentation from the RO regarding CDC permit approval for SA employees.
- Reporting security related incidents to the SAM and Security.
- Authorizing facility personnel to act as escorts during maintenance windows.
- Authorizing all individuals escorted into the facility.
- Approving, in conjunction with the SLC and the SAM, access to SA laboratories for scientific collaborators.

(b)(7)(F)

The SAFM designated alternates are the Facility Point of Contact (FPOC) and the Alternate FPOC.

5.9 Facility Point of Contact (FPOC)

The FPOC is responsible for:

(b)(7)(F)

- Scheduling maintenance windows in concurrence with the SAFM, SAM, and SLC.

5.10 Associate Program Leader for Select Agent Science (APL)

The APL is responsible for:

(b)(7)(F)

- Requesting SA access for PI/RIs.

5.11 Senior Laboratory Coordinator (SLC)

The SLC is responsible for:

- Providing daily supervision of the research activities.
- Approving, in conjunction with the SAFM and the SAM, access to SA laboratories for scientific collaborators.

5.12 Padlock Custodian

The Padlock Custodian is responsible for:

(b)(7)(F)

5.13 Assurance Office Manager

- Acting as the certifying official for the SAHRP

6.0 Description of Work

LLNL is funded to conduct research that requires working with biological SAs or toxins, including those regulated by the DHHS and plant and animal SAs or toxins that are regulated by the USDA.

(b)(7)(F)

7.0 Security Risk and Threat Assessment of Biological Select Agents or Toxins

LLNL conducts a security risk and threat assessment of the areas where biological SAs or toxins are used and/or stored. The assessments³ are in compliance with 42 CFR Part 73, 7 CFR Part 331 and 9 CFR Part 121.

The Biological Risk and Threat Assessments are conducted in accordance with a methodology developed by a SA working group that met in Albuquerque on April 8 and 9, 2003.⁴ Participants represented Los Alamos National Laboratory (LANL), Lawrence Livermore National Laboratory (LLNL), Lawrence Berkley National Laboratory (LBNL), Sandia National Laboratory (SNL), Department Of Energy (DOE), the DOE National Nuclear Security Agency (NNSA), and the University of California (UC).

The assessment considers the threats, the attractiveness of the assets, the use/storage facilities, shipping/receiving processes, and existing procedures and security systems to assess the effectiveness of current protective measures. The SAA specific security plans are based on that assessment of effectiveness.

8.0 Facility Registration

The specific location, whether it is an individual room or a suite of rooms, used to conduct SA work shall be registered with CDC. To register a location, the RO will need the following information:

- What SAs are to be used.
- The form in which the SA exists.
- The names of all workers who will have access to these materials.
- The PI/RI's curriculum vitae.
- A sketch and description of the room or rooms to be used.

A copy of Sections 4 and 5 of the CDC's "Application for Laboratory Registrations for Possession, Use and Transfer of Select Biological Agents and Toxins" form (CDC Form 0.1319 or APHIS Form 2044) may be obtained from the RO or the CDC's Web site at the following Internet address: <http://www.cdc.gov/od/sap/downloads2.htm>

9.0 Staff Security Risk Assessment

Every employee who has unescorted access to SA materials has a security risk assessment from the US DOJ and is approved by CDC/APHIS to work in the building. To receive a risk assessment, workers shall be identified by their PI/RI and requested to fill out DOJ Form 961, Sections III and IV which are available from the RO or the Federal Bureau of Investigation (FBI) Web site at: <http://www.fbi.gov/terrorism/bioterrorfd961.htm>. Workers will also be requested to provide two copies of their fingerprints. The RO will forward the form 961 and the fingerprint cards to the FBI for review and approval.

The security risk assessment process shall be completed for everyone with access to SAs, regardless of their security clearance level.

³ LLNL's Security Risk Assessment of Biological Select Agents/Toxins, August, 2003

⁴ UC/NNSA/SNL/DOE Risk and Threat Assessment Methodology Working Group, April 8-9, 2003.

The RO shall maintain an up-to-date list of all workers authorized to access SAs.

Any person who loses their CDC approval will immediately be removed from any duties involving SA handling or access control responsibilities.

10.0 Select Agent Human Reliability Program (SAHRP)

All personnel working with SAs will participate in a human reliability program. Most SA personnel will be in the SAHRP however satisfactory participation in the Human Reliability Program (HRP) will be acceptable in lieu of the SAHRP.

A complete description of the SAHRP may be obtained from the LLNL Assurance Office.

Any person who loses their SAHRP or HRP certification status will immediately be removed from all SA access lists and any duties involving SA handling or access control.

11.0 Access Authorization

11.1 Unescorted Access

Authorization for unescorted access to SAs or toxins requires:

- An individual must be successfully screened through the DOJ security risk assessment (SRA) process.
- The individual must be approved by HHS or USDA to access specific SAs or toxins, in specific locations.
- The individual's line management must authorize the access.
- The RO must approve access to the SAs or toxins before the individual can access them.
- All individuals having direct access to the SA material must be enrolled in the SAHRP or HRP.

After all five steps are fulfilled, the individual is considered to be an authorized approved person who can have unescorted access to the specific SAs or toxins in the specific locations for which the person is registered.

11.2 Visitor Access

Any person other than an authorized approved person as described above must:

- Have a business reason for being in the SA or toxin area.
- Be escorted by an authorized approved person at all times while in the SAs or toxin area.

Unauthorized persons in the SAA will be reported to PFD immediately and removed from the SAA.

11.3 Foreign National Access

11.3.1 Foreign Nationals assigned to a SA facility must have the following:

- Approved VTS.

(b)(7)(F)

11.3.2 Foreign National visitors must have pre-approved access from the following:

- SA Manager or SA Facility Manager.
- Foreign National Interactions Office.
- OPSEC Committee SME.
- Have a business reason for being in the SA or toxin area.
- Be escorted by an authorized approved person at all times while in the SAs or toxin area.

11.4 Cleaning Access

Routine cleaning of the SAA is the responsibility of the PI/RIs and their staff.

Procedures for maintenance and repairs are in the Standard Operating Procedures (SOP) for each building containing SAs or toxins.

11.5 Access Additions & Deletions

(b)(7)(F)

12.0 SA Access**12.1 Building Resident Access**

(b)(7)(F)

- The SAM will meet with the individual to be enrolled and brief them on the operation of the security system. In the SAM's absence, the APL can enroll individuals unless otherwise noted in the facility specific appendices attached to this document.

(b)(7)(F)

12.1.2 Laboratory Access

- Access to an individual laboratory where SAs are handled must be made in writing by the PI/RI for the specific room to the SAM.
- The SAM will confirm with the SAFM that the individual is fully qualified in terms of safety training and security risk assessment before enrolling them on the lock for the laboratory.

(b)(7)(F)

12.2 SAA Access Recordkeeping

SA regulations require extensive documentation of SA activities. Documentation is needed in order to maintain a record of who has had access to SAs and what activities they have performed. This documentation shall include laboratory and storage container access information.

(b)(7)(F)

The use of initials or ditto marks in the records is not allowed. Personnel will fill out the required blocks with complete names, times, and dates.

12.2.1 Laboratory Access

(b)(7)(F)

12.2.2 Storage Container Access

(b)(7)(F)

12.2.3 Records Retention

All access records created in meeting the requirements of this document shall be retained in a safe, secure location for a minimum of three years. Inventory records will be retained for three years after the last stock of the agent has been consumed or destroyed.

The PI/RI shall maintain these records for the current year. Annually, these records shall be transferred to the RO for archival storage. Archive copies of these records should be provided to the RO to be kept away from the work area.

13.0 Terminations

Whenever a worker terminates involvement with a SA activity, the PI/RI or APL shall inform the RO who shall notify CDC/ APHIS that the individual no longer has access to SAs within the responsibility of that PI/RI.

Whenever a PI/RI terminates involvement with SAs, either because the project is completed or because they terminate their employment within the SA program or at LLNL, the PI/RI shall:

- Either destroy (Section 15, Disposal) or transfer (Section 17, Transfers) to an appropriate entity, all SA materials under their responsibility.
- Transfer all records required in Section 14.2, Inventory Records of this document to the RO.

14.0 Accountability and Control of Biological SAs and Toxins

LLNL is the owner of all SAs located on the site. Only personnel on the LLNL CDC permit will be allowed to handle the SAs. SAs isolated from environmental or clinical samples will not be added to a PI/RI's inventory until CDC or APHIS has been informed and indicated proper disposition.

In the event an outside agency is authorized to locate a SAA at LLNL and act as the owner entity this security plan will be modified to reflect the presence of the separate entity.

14.1 Inventory

SAs will be inventoried in accordance with the following requirements:

- An inventory database will be maintained by the RO.
- The RO and Bio-Safety Officer (BSO) will review the inventory records annually to verify the completeness and accuracy of the inventory.
- Procedures for maintaining the inventory is covered in the Biosciences SOP, *Inventory of Select Agents*.

(b)(7)(F)

- The Security Department will be notified at any time there is an issue, concern, or discrepancy with the inventory.

14.2 Inventory Records

The PI/RI shall maintain an inventory of all SAs in their charge that includes:

- Name, characteristics, and source of the material.
- Quantity of material held on the first date of inventory (toxins only).
- The quantity acquired, the source, and date of acquisition.
- The quantity, volume, or mass destroyed or otherwise disposed of, and the date of each action.
- The quantity of material used and the date of the use (toxins only).
- The quantity transferred, the date of transfer, and the PI/RI to whom it was transferred (both internal and external transfers).
- The current quantity of material held (toxins only).
- Any SA or toxin lost, stolen or otherwise unaccounted for.
- Any discrepancies will be documented in a nonconformance report.

14.3 Inventory Oversight

LLNL's RO is responsible for assuring that detailed records of information necessary to give a complete accounting of all activities related to SAs or toxins are maintained in accordance with the CFRs. The RO reviews the inventory annually.

15.0 Disposal

When an activity involving SAs is completed and the PI/RI has no further use for the materials, they shall be either transferred to another PI/RI who does have a need for them, or they shall be destroyed. The PI/RI will notify the RO of proposed destruction.

SAs to be destroyed will be under the control of an approved, authorized person until the destruction process has been started. Under no circumstances will SAs awaiting destruction be left unattended.

16.0 Receipt and Shipping of SAs by LLNL

SAs or toxins in transit to or from LLNL will be handled according to LLNL Procurement & Material Distribution Department, Material Distribution Division (MDD) Operating Procedures, Section 301.1, *Basic Receiving and Distribution*, and Section 200.20, *Infectious Substances and Etiologic Agents*.

(b)(7)(F)

All Shipping and Receiving personnel responsible for handling the SA packages or having access to the SA package storage cage will be on the CDC permit.

(b)(7)(F)

17.0 Transfer of Select Biological Agents and Toxins

LLNL's RO is responsible for ensuring compliance with the regulations for transfer of SAs or toxins. All transfers of SAs, whether between LLNL and other institutions, or between LLNL PI/RIs, shall be documented and controlled as described in this section.

17.1 Offsite

All SA transfers between LLNL and any outside organization shall be documented and approved by the shipper and receiver ROs, and either CDC or APHIS. The mechanism for this process is CDC Form 2. An identical form used to document/approve transfers of agricultural SAs is called APHIS Form 2. These forms can be obtained from the RO or the CDC Web site at: <http://www.cdc.gov/od/sap/addforms.htm>.

The RO will retain copies of the Form 2 for three years after the last of the subject inventory has been consumed or destroyed. In the event that the RO is unavailable, an Alternate RO may approve a transfer.

PI/RIs wishing to receive overlap organisms from out-of-state or out of the country must also possess a valid USDA permit (VS-16) to import organisms. USDA issues these permits directly to the PI/RI and it is the responsibility of the PI/RI to obtain one that specifies each organism and shipper they will be working with. Copies of the application for this permit may be obtained from the RO or USDA Web site at: <http://www.aphis.usda.gov/vs/ncie/bta.html>.

A copy of this permit must accompany any Form 2 for an interstate shipment of overlap organisms that is submitted to the RO for approval. Note that this requirement does not include any shipments of toxins or shipments of organisms within the state of California.

PI/RIs wishing to ship organisms out of the country must comply with applicable export control regulations. LLNL export control guidance can be found at <http://www.llnl.gov/expcon/policy.html>.

Transfers to or from LLNL will be approved only when an Integrated Worksheet/Safety Plan associated with the work has been approved.

17.2 Onsite

On site transfers will be conducted according to the Biosciences SOP, *Excluding Select Agent*. All transfers of SA materials between PI/RIs onsite shall be documented and approved by the RO. The shipper and receiver shall complete a CDC Form 2 and have it approved by the RO before the transfer is made. In the event that the RO is unavailable, an Alternate RO may approve a transfer.

Transfers onsite will be approved only if both the shipper and receiver have approved IWSs /SPs in force.

The RO will maintain a copy of the Form 2 for three years after the last of the subject SA has been consumed or destroyed.

17.3

(b)(7)(F)

18.0 Physical Security

(b)(7)(F)

18.1 Facility Access Procedures

(b)(7)(F)

18.2

(b)(7)(F)

19.0

(b)(7)(F)

(b)(7)(F)

20.0 General Security

All persons working with SAs have the same responsibility to meet the general security requirements as the rest of the LLNL population.

Topics of general security interest at LLNL are available at the LLNL internal security website located at <http://www-r.llnl.gov/securityprogram/index.html>

Some topics that are covered are:

- Controlled and Prohibited Items.
- Controlled Item Permit Application.
- Locks and Keys.
- Lost and Found.
- Security Escorts.
- Security Signs.
- Site Access and Gate Information.

21.0 Personnel Suitability

The Laboratory commits to maintain a drug-free workplace in compliance with both the Drug-Free Workplace Act of 1988 and 10 CFR 707. LLNL has an established substance abuse awareness, assistance, and training program.

21.1 Employee Assistance Program (EAP)

Employee Assistance Program services are made available to all employees involved in the DOE contract. This is an in-house service managed by a clinical psychologist and consisting of a staff of professional counselors who are trained in treating personal problems, including substance abuse.

21.2 Alcohol and Substance Abuse Prevention for Employees (ASAP).

This course is required for all employees. It reviews the risks that substance abuse poses to the health and safety of Laboratory employees, the Laboratory's drug and alcohol prohibitions, the possible consequences for violating these prohibitions, and to the Laboratory's national security responsibilities.

21.3 ASAP Education Program for Management.

This course is required for all Laboratory first line supervisors and managers. Course content covers the impact that substance abuse can have on the workplace and the specific strategies for dealing with performance and drug crisis management. Participants learn about the Laboratory's ASAP program, including policies on testing for cause and fitness for duty. Information is made available on how to handle an employee under the influence, and how not to "enable" substance abuse by an employee.

21.4 Select Agent Human Reliability Program (SAHRP)

In addition to meeting education, experience, and training requirements, LLNL requires participation in the SAHRP in order to be authorized to have unescorted access to SAs or toxins. The SAHRP is administered by the LLNL Assurance Office. Participation in the Human Reliability Program (HRP) is acceptable in meeting the SAHRP requirement.

22.0 Information Security

The DOE classification guides, CG-CB-2, *Classification Guide for Chemical/Biological Defense Information* and CG-SS-4, *Classification and UCNI Guide for Safeguards and Security Information* will be used to determine the sensitivity level of information generated in regards to the SA and toxins, the SA facilities, and the security of the SAs.

All information determined to be unclassified controlled information (UCI) will be handled in accordance with UCI requirements.

LLNL makes information concerning information security available at the LLNL internal security website located at <http://www-r.llnl.gov/securityprogram/index.html>. Some topics that are covered are:

- Authorized Derivative Classifier List.
- Classification and Export Control.
- Classified Document Protection.
- Security Awareness for Employees (SAFE).
- Document Review and Release.
- Operations Security (OPSEC).
- Unclassified Controlled Information (UCI).

23.0 Cyber Security

LLNL's cyber security group manages cyber security for the Laboratory. The cyber security group is responsible for providing for protection of electronic data and networks. Cyber security information available at the LLNL internal security website located at <http://www-r.llnl.gov/securityprogram/index.html>. Some topics that are covered are:

- Cyber Security (CSO).
- Computer Incident Advisory Capability.
- Computer Security Task Force.
- DOE Information Security.
- Incidental IT Use Policy.

Further information can be obtained at the Chief Information Officer website at <http://www-r.llnl.gov/cio/>

24.0 Feedback and Improvement

24.1 Annual Security Risk Assessments

The RO, PSR, and the TMAG staff will conduct a review of the SA security risk assessments annually and when design parameters change to determine if modifications need to be made to the documents.

24.2 Security Plan Review

The RO is responsible for reviewing the LLNL *Biological Select Agents and Toxins Security Plan* annually, and after any security incident, should one occur.

24.3 Security Incident Review

The security plan and applicable appendix will be reviewed by the RO and PSR following any security incident. If applicable the results of this review will be provided to the TMAG for possible modification to the SA security risk assessments.

25.0 Espionage

The LLNL Security Awareness For Employees (SAFE) office is responsible for counterintelligence activities. The SAFE office provides awareness training for workers who are associated with high-risk programs such as special access authorization and human reliability programs.

26.0 Operations Security

OPSEC staff are available to conduct an evaluation of the effectiveness of an organization's implementation of OPSEC methodology, resources, and tools to determine the effectiveness to the organization's OPSEC program. Organizations that are responsible for use/storage of SAs or toxins may request an evaluation if they wish to do so. LLNL's OPSEC Committee meets to discuss OPSEC and counterintelligence awareness, issues, and concerns.

27.0 Visitors

All visits to the SAA must have a justification for the access request. The Badge Office staff ensures that the appropriate background checks and paper work are completed prior to visits to LLNL made by non-LLNL employees.

PI/RIs or the RO are responsible for working with the LLNL Badge Office when requests for visits to the SAA are made, ensuring any necessary paperwork is completed prior to the visit, and that the badge is retrieved and returned to the Badge Office after the visit.

The Directorate owning the SAA will provide any necessary training and explanation of responsibilities from a security standpoint to visitors prior to access to the area.

28.0 Training**28.1 Approved Authorized Personnel**

Training presented to approved authorized personnel regarding SA security will be determined according to the particular needs of the individual, the work they will do, and the risks posed by the SAs or toxins. Procedures for using security devices located in the SAA will be given to all authorized approved persons accessing the SA laboratories. Training will be documented in the Livermore Training Records and Information Network (LTRAIN) and refreshed annually.

28.2 Visitor Security Briefing

All visitors must receive the SA Visitor Security Briefing prior to entry into the SAA. See Attachment 1. In addition, all visitors to a SAA are required by the SA SOPs to have a SPA completed prior to entry into the area. Completion of the SPA is a function of the facility personnel. On the SPA will be noted that the security briefing has been presented to the visitor.

28.3 Drills or exercises

Drills or exercises to test the security plan will be conducted annually using protocols for drills and exercises managed by the LLNL Emergency Programs. Emergency Programs has overall responsibility for coordinating emergency preparedness and management activities within Hazards Control Department as well as coordination of LLNL's institutional emergency preparedness program.

29.0 Emergency Response

LLNL's safety and security organizations are responsible for developing emergency response plans for the SAs or toxins, including their use and storage areas. The RO will review the plans and ensure they are compatible with SA requirements.

(b)(7)(F)

All safety plans for SA work contain provisions for responding to foreseeable emergencies such as spills or unintended exposures. When these provisions require support from outside organizations such as the LLNL Fire Department, the PI/RI shall inform the responding organization of the hazards involved in the activity and the level of support that may be required. This can be in the form of Fire Department run cards or inclusion in emergency plans.

- Employees evacuating a SA facility in an emergency will move to the muster area identified in their Self Help Plan.

(b)(7)(F)

29.1 Security Incidents

(b)(7)(F)

- The RO is responsible for reporting the loss or theft of listed agents or toxins, release of listed agents or toxins, or alteration of inventory records to DHHS, USDA, DOE and LLNL authorities concurrently.

(b)(7)(F)

29.2 Security Alarm Response

(b)(7)(F)

30.0 Incident Reporting

The following incidents shall be reported to the RO (b)(7)(F)

- Theft or loss of SA materials, even if all of the material is subsequently recovered.
- Uncontrolled release of SA materials.
- Occupational exposure to a SA material.

The RO is responsible for providing reports to LLNL Security, CDC, APHIS, and DOE/NNSA, as appropriate. Initial reports shall be made by telephone or E-mail and shall be followed up in writing within seven days.

Incidents that may be a threat to the safety of workers and/or the public shall be reported to DOE/NNSA under the schedules of Document 4.3, "Occurrence Reporting and Processing of Operations Information," in the *Environmental Safety & Health Manual*.

(b)(7)(F)

(b)(7)(F)

Incidents that may be a threat to both safety and security at LLNL shall be reported to DOE under both of the above provisions.

30.1 Report Contents

For loss or theft, the report shall include at a minimum:

- Identification of the material lost or stolen.
- Estimate of the quantity.
- Estimate of the time the loss or theft occurred.
- Location from which the material was lost or stolen.

For a release or exposure, the report shall include at a minimum:

- Identification of the material involved.
- Estimate of the quantity released.
- Time and duration of the release.
- Environment into which the release occurred (e.g., inside or outside).
- Location of the release.
- Number of individuals potentially exposed to the material.
- Actions taken to respond to the release and the resultant hazards.

30.2 Report Notification Process

Upon notification of a reportable incident, the RO shall contact CDC or APHIS, as indicated on the Centers for Disease Control/ Animal and Plant Health Inspection Service (CDC) Web site (<http://www.cdc.gov/od/sap/addforms.htm>) within two hours of discovery. Initial reporting with all of the information listed in section 3.10.2 shall be made by phone or E-mail.

Within seven days of the initial report, a written report shall be filed using CDC Form 0.1316 or APHIS Form 2043. Copies of these forms may be found in on the CDC Web site (<http://www.cdc.gov/od/sap/addforms.htm>) or on the APHIS Web site (http://www.aphis.usda.gov/programs/ag_selectagent/index.html).

DOE Occurrence Reporting Processing System (ORPS). Any incident that may be threat to safety to workers and/or the public that is reported to CDC or APHIS meets the conditions of a reportable occurrence under Document 4.3, "Occurrence Reporting & Processing of Operations Information," in the *ES&H Manual*, either as an occupational exposure or an environmental release.

Incidents that may be a threat to security shall be reported to DOE, through the LLNL Incidents and Infractions Section, under the terms of DOE Notice 471.13, "Reporting Incidents of Security Concerns" and the LLNL Implementing Procedures "Reporting Incidents of Security Concern." Incidents that may be a threat to both safety and security at LLNL shall be reported to DOE under both of the above provisions.

All safety incident reporting shall be coordinated with the LLNL Occurrence Reporting Office.

The RO is responsible for reporting the loss or theft of listed agents or toxins, release of listed agents or toxins, or malicious alteration of inventory records to DHHS, USDA, DOE and LLNL authorities concurrently.

31.0 Public Relations

The Laboratory Public Affairs Office is responsible for Public Affairs and Community Relations, and Government Relations.

32.0 Change Control

The *LLNL Biological Select Agents and Toxins Security Plan* will be reviewed annually by the RO and PSR. Updates to the Plan will be made by the PSR as necessary and with the concurrence of the RO and SD Deputy Department Head (DDH).

At any time a security incident occurs at the SAA the Plan will be reviewed by the RO, PSR, and the TMAG staff to address any possible vulnerability indicated or that might arise from the incident. The PSR will change the Security Plan according to the results of the incident review.

Annually and at any time a security incident occurs at B368 this security plan will be reviewed by the RO, SAFM, PSR, and TMAG staff to address any possible vulnerability indicated or that might arise an incident or changes in requirements. The PSR will update the security plan according to the results of the review.

Attachment 1 Select Agent Visitor Security Briefing

This area is a Select Agent research area and has special federally mandated security rules. All visitors must comply with the security rules described below.

- Visitors must have a business need to enter the Select Agent laboratories.
- Visitors must be approved by the Principal Investigator/Responsible Individual in charge of the laboratory prior to the visit occurring.
- Visitors must be under the escort of an authorized, approved person while in the Select Agent laboratory.
- Visitors must remain with their escort throughout the visit to the laboratory.
- Visitors must sign in and sign out of each Select Agent laboratory they enter using either manual or electronic means.
- Visitors may not at any time touch, handle, or have access to the Select Agents or toxins.

Any visitor who does not comply with the above rules will be removed from the laboratory and reported to the LLNL Security Incidents and Infractions Officer. Further investigation of the incident will be conducted by the LLNL Security Department and may be reported to the Department of Energy/NNSA.

Attachment 2 Select Agent Laboratory Access Record

User's and Visitor's Log Book for Building: _____ Room: _____

Fill in all applicable fields. Do not use initials or ditto marks.

All visitors must be so identified and escorted at all times.

WHEN YOU LOG OUT MAKE SURE THAT YOU DO SO ON THE CORRECT LINE

Date	Name	Time in	Time out	Check if Visitor	Visitor Escort

Appendix A - (b)(7)(F)

1.0 Purpose

This document establishes the security requirements and procedures for (b)(7)(F) in conjunction with The Lawrence Livermore National Laboratory (LLNL) *Biological Select Agents and Toxins Security Plan*.

2.0 Scope

This plan applies to personnel entering (b)(7)(F). Personnel are responsible for understanding and implementing the requirements of this document as it pertains to their roles and responsibilities while in (b)(7)(F).

3.0 Description of Work

(b)(7)(F)

4.0 Security Risk and Threat Assessment of Biological SAs or Toxins

The LLNL Security Department Threat Mitigation Analysis Group conducted a security risk and threat assessment of (b)(7)(F) *Select Agent and Toxin Risk Assessment*."

5.0 Facility Registration

(b)(7)(F)

6.0 Access Authorization for Visitors

6.1 Visitor Access to the hallway

Any person other than an authorized approved person must:

- Have a business reason for being in the SA/toxin area (e.g., maintenance or inspection).
- Be approved by the SAFM, SAM, or SLC.

6.2 Visitor Access to the laboratories

Individuals who have not been granted unescorted access to a particular laboratory may enter that laboratory providing:

- They have a business need to be in the laboratory (e.g., maintenance or inspection).
- All SAs have been secured and the laboratory has been decontaminated, unless the purpose of the visit is to observe SA activity.
- They are escorted by an authorized approved person at all times while in the SAs/toxin area.
- They are approved to visit by the SAFM or PI/RI responsible for the laboratory.

6.3 Physical Security

6.3.1

(b)(7)(F)

~~Official Use Only~~

LLNL Select Agent Security Plan, Rev 6
SSO-POL-10

March 9, 2006

Appendix A – (b)(7)(F)

6.3.2

6.3.3

(b)(7)(F)

~~Official Use Only~~

Page 31 of 37

Appendix B - (b)(7)(F)

1.0 Purpose

This document establishes the security requirements and procedures for (b)(7)(F) in conjunction with The Lawrence Livermore National Laboratory (LLNL) *Biological Select Agents and Toxins Security Plan*.

2.0 Scope

This plan applies to personnel entering (b)(7)(F). Personnel are responsible for understanding and implementing the requirements of this document as it pertains to their roles and responsibilities while in (b)(7)(F).

3.0 Description of Work

(b)(7)(F)

4.0 Security Risk and Threat Assessment of Biological SAs or Toxins

The LLNL Security Department Threat Mitigation Analysis Group conducted a security risk and threat assessment of (b)(7)(F) *Select Agent and Toxin Risk Assessment*."

5.0 Facility Registration

(b)(7)(F)

6.0 Access

6.1 Access Authorization

(b)(7)(F)

6.2 Building Resident Access

(b)(7)(F)

6.2.3 Enrolled individuals will be briefed on the operation of the security systems.

6.2.4 The SAFM will confirm with the LLNL RO that the individual is fully qualified in terms of safety training and security risk assessment before giving final approval for unescorted access.

6.3 Access Requirements

6.3.1

(b)(7)(F)

6.3.2 Service personnel (both LLNL and contractors) who have an occasional need to enter the mechanical room may do so with the permission of someone who has unrestricted access. A full-time escort is not required in this area.

6.3.3

(b)(7)(F)

6.3.4 Visitors, with the exception of scientific collaborators, are allowed access to (b)(7)(F) laboratory area providing:

- There is a legitimate reason for the visitor being in the SA/toxin area (e.g., maintenance or inspection);
- The visitor is escorted by an authorized approved person at all times while in the SAs/ toxin area;
- All SAs must have been secured and the laboratory decontaminated prior to visitor entry;

(b)(7)(F)

6.3.5 Scientific Collaborators may be authorized entry into a SA laboratory to allow the observation of a process providing:

- They are escorted by an authorized approved person at all times while in the SAs/ toxin area.
- They have been issued a proximity access system token.
- Unnecessary SAs have been secured.
- They do not handle or manipulate the SA used in the process.

(b)(7)(F)

6.4 Access System Enrollment

6.4.1

(b)(7)(F)

Requests for individuals to be enrolled must be made to the SAM. The SAM shall meet with the individual to be enrolled and brief them on the operation of the security system. In the SAM's absence, the SLC may enroll individuals.

6.4.2

(b)(7)(F)

6.4.3

6.4.4

(b)(7)(F)

6.4.5

6.4.6

6.4.7

6.5 Access to the Mechanical Room

6.5.1

6.5.2

(b)(7)(F)

6.5.3

6.6 Access to the laboratory area during maintenance windows.

6.6.1 Maintenance windows will be scheduled by the FPOC in concurrence with the SAM, SAFM, and SLC.

6.6.2 All SAs will be locked away during all maintenance windows.

(b)(7)(F)

(b)(7)(F)

6.7 Access during an emergency

(b)(7)(F)

6.8 Building Access Procedures

(b)(7)(F)

(b)(7)(F)

6.9

(b)(7)(F)

6.10 Laboratory Access Procedures

6.10.1 Personnel are assigned lockers in the change room. The lockers will be locked when not attended.

6.10.2 Personnel will change from their street clothes into the personnel protection equipment (PPE) in the change room. The PPE will not have pockets.

6.10.3

6.10.4

6.10.5

6.10.6

6.10.7

6.10.8

(b)(7)(F)

6.11

(b)(7)(F)

6.12

(b)(7)(F)

6.12.3

(b)(7)(F)

6.12.4

(b)(7)(F)

6.13

(b)(7)(F)

6.14

(b)(7)(F)

6.15

(b)(7)(F)



September 17, 2015

Sent Via Email

Re: FOIA Request 2015-STFO-086

This is the acknowledgement and final response to your Freedom of Information Act (FOIA) request to the Department of Energy (DOE) National Nuclear Security Administration (NNSA), dated August 26, 2015, and seeking the following regarding Lawrence Livermore National Laboratory (LLNL) and Sandia National Laboratories (SNL): 1) LLNL Site Seismic Safety Program, Summary of Findings, UCRL-53674, Rev. 2, April 2002, 2) LLNL Biological Risk and Threat Assessment, July 14, 2005, 3) LLNL Select Agents and Toxins Security Plan, Revision 6, SSO-POL-010, UCRL-MI-220409 March 9, 2006, 4) SNL and LLNL Catastrophic Bioterrorism Scenarios: Response Architectures and Technology Implications, March 2006, and 5) LLNL B368 Select Agent Risk and Threat Assessment, July 14, 2005. While processing your request, the NNSA referred your request for the Catastrophic Bioterrorism Scenarios: Response Architectures and Technology Implications March 2006 to the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) for direct response to you. Your request was received in S&T on August 31, 2015.

A search of S&T's Chemical and Biological Defense Division files for the key terms Catastrophic Bioterrorism Scenarios: Response Architectures and Technology Implications, March 2006 produced a total of 211 pages. Of those pages, I have determined that 2 pages of the records are releasable in their entirety, 8 pages are partially releasable, and 201 pages are withheld in their entirety pursuant to Title 5 U.S.C. § 552 (b)(6) and (b)(7)E).

Enclosed are 10 pages of reasonably segregable documents with certain information withheld as described below.

FOIA Exemption 6 exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right privacy.

[The types of documents and/or information that we have withheld may consist of birth certificates, naturalization certificates, driver license, social security numbers, home addresses, dates of birth, or various other documents and/or information belonging to a third party that are

considered personal.] The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

Exemption 7(E) protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law. I determined that disclosure of the information contained in this report include assessments of defensive architectures and the adequacy of response countermeasures, as well as identifying gaps in knowledge and preparedness and information pertaining to enhancing the response countermeasures, which if released could reasonably be expected to risk circumvention of the law. The information withheld also includes sensitive research analysis which if released could reasonably be expected to risk circumvention of the law. See *Boyd v. DEA*, No. 01-0524, 2002 U.S. Dist. LEXIS 27853, at *11-13 (D.D.C. Mar. 8, 2002) (upholding protection under both clauses of Exemption 7(E) for highly sensitive research analysis in intelligence report).

Provisions of the FOIA [AND PRIVACY ACT] allow us to recover part of the cost of complying with your request. In this instance, because the cost is below the \$14 minimum, there is no charge.

The Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. If you wish to contact OGIS, you may email them at ogis@nara.gov or call 1-877-684-6448.

You have a right to appeal the above withholding determination. Should you wish to do so, you must send your appeal and a copy of this letter, within 60 days of the date of this letter, to: Associate General Counsel (General Law), Mailstop 0655, U.S. Department of Homeland Security, Washington, DC 20528, following the procedures outlined in the DHS regulations at 6 C.F.R. § 5.9. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS regulations are available at www.dhs.gov/foia.

If you need to contact our office again about this matter, please refer to **2015-STFO-086**. This office can be reached at stfoia@hq.dhs.gov or (202) 254-6342.

Sincerely,



Katrina Hagan
FOIA Officer

Enclosure: Catastrophic Bioterrorism Scenarios: Response Architectures and Technology Implications March 2006, 10 pages

Catastrophic Bioterrorism Scenarios: Response Architectures and Technology Implications

Prepared for
The Department of Homeland Security

Prepared by
Sandia National Laboratories
Lawrence Livermore National Laboratory
Washington Institute

March 2006

May be exempt from public release under the Freedom of Information Act (5 U.S.C 552) exemption number and category 2, Circumvention of Statute.

Department of Energy review required before public release.

Name/Org: (b) (6) Date: 11/15/05

Catastrophic Bioterrorism Scenarios: Response Architectures and Technology Implications

Prepared for
The Department of Homeland Security

Prepared by
Sandia National Laboratories
Lawrence Livermore National Laboratory
Washington Institute

March 2006

Principal Investigators:

(b) (6), Sandia National Laboratories
(b) (6) Livermore National Laboratory
(b) (6), Sandia National Laboratories
(b) (6), Washington Institute
(b) (6) Livermore National Laboratory
(b) (6) Lawrence Livermore National Laboratory

ACKNOWLEDGMENTS

This report documents work performed under the sponsorship of the Department of Homeland Security within the Science and Technology Directorate in FY04 and FY05 under the guidance of (b) (6) and (b) (6). The project was led by (b) (6) of Sandia National Laboratories and (b) (6) Livermore National Laboratory. Principal investigators for the scenario analyses included (b) (6) of Sandia National Laboratories, (b) (6) of the Washington Institute, and (b) (6) and (b) (6) of Lawrence Livermore National Laboratory.

TABLE OF CONTENTS

Executive Summary	1
Introduction.....	5
Scenario Descriptions	9
Aerosol release of <i>Bacillus anthracis</i>	11
Aerosol Release of <i>Variola major</i>	31
Intentional release of foot-and-mouth disease virus	51
Food Contamination.....	67
Defensive Architectures	73
Aerosol release of <i>Bacillus anthracis</i>	77
Aerosol Release of <i>Variola major</i>	89
Intentional release of foot-and-mouth disease virus	105
Food Contamination.....	135
Gap Assessment	153
Aerosol Releases of <i>Bacillus anthracis</i> and <i>Variola major</i>	155
Intentional release of foot-and-mouth disease virus	189
Food Contamination.....	195
Next Steps in Architecture Analysis.....	199
Aerosol Releases of <i>Bacillus anthracis</i> and <i>Variola major</i>	201
Intentional release of foot-and-mouth disease virus	209
Food Contamination.....	213
Acronyms.....	215

EXECUTIVE SUMMARY

This report summarizes a family of studies that examined four catastrophic bioterrorism scenarios. These studies were undertaken to describe the technical parameters, and their uncertainties, that define a scenario, as well as the performance of defensive architectures and response countermeasures when facing such an attack scenario. On the basis of quantitative and qualitative assessment of the scenario impact—that is, the consequences of a specific scenario and the performance of a specific defensive architectural configuration—the studies identified gaps in knowledge and preparedness, and provide information to support enhancements in the nation's defensive posture. This work also provides a foundation for the determination of priority technology requirements to meet the bioterrorism threat environment.

The significance of this work is in the detailed technical treatment of all of the parameters necessary for full explication of a scenario and its impact, as well as in the assessment of the provenance and uncertainty associated with the parameters used to make the calculations. These scenarios are also significant as an ensemble in that they follow a similar taxonomy, and therefore offer a more standardized means of examining and understanding the various threats and countermeasures.

SCENARIOS

The four scenarios studied were chosen as exemplars of the broad class of bioterrorism scenarios and are believed to be credible scenarios with the potential for catastrophic impact. Catastrophic impact was a key selection metric and, in this work, was defined as resulting from incidents within the United States with fatalities in excess of ten thousand people and/or economic damages reaching tens of billions of dollars. Specific adversaries were not assumed; rather, the capabilities of adversaries to acquire, prepare, and distribute agent were explored as a part of the scenario specification.

The four scenarios examined in this work include:

(b) (7)(E)



A bioterrorism taxonomy may be organized in a variety of ways: by agent, by method or location of dispersal, by type of impact (on people, on animals, etc.) or by countermeasure applicability (e.g., existence or availability of medical prophylaxis or treatment). The four scenarios considered in this work are representative of the issues and requirements associated with employment of other pathogens in bioterrorist attacks; study results highlight implications of different agents or attack approaches. For example, the end-to-end analytic framework and key findings from the smallpox scenario can be applied to other contagious biological threat agents and to pathogens capable of causing disease at low infectious doses.

SCENARIO ANALYSIS

Analysts followed a similar approach for each scenario:

- Identify and describe the attack and quantify its consequences
- Explore and document the factors and assumptions required to make quantitative estimates
- Predict the impact of response alternatives and explore the key issues associated with response alternatives.

The analytic approach for the development and assessment of these scenarios is founded on a thorough examination of the scientific literature regarding the biological threat agent and its disease-causing mechanisms. This information was then applied to a realistic characterization of the properties of the weaponized biological agent in the specific scenario and its potential health impact. Each scenario explores and documents the factors and assumptions required to make quantitative estimates, and predicts the impact of the scenario by identifying the key issues associated with response alternatives.

These scenarios are differentiated from other work in the detailed technical treatment of all of the parameters necessary for full explication of a scenario and its impact, along with an assessment of the provenance and uncertainty associated with the parameters used to make the calculations.

COUNTERMEASURE ANALYSIS

The broad functional elements that constitute a defensive architecture are similar among the scenarios. These elements include protection, surveillance, detection, rapid response, longer-term response, and restoration. An initial assessment of the effectiveness of current capabilities, policies, and practices formed the basis of the report cards that delineate the performance of the defensive system, described as pillars in the report *Biodefense for the 21st Century* (<http://www.whitehouse.gov/homeland/20040430.html>), a government document that provides a comprehensive framework for our nation's biodefense, based on the best thinking of numerous federal departments and agencies.

Analysts also examined the performance and augmentation of these systems over time to provide a temporal assessment element of the report cards, laying the foundation for future work that will improve the performance of a defensive architecture and close the gaps in knowledge.

SIGNIFICANT RESULTS FROM THE AEROSOL SCENARIOS

Aerosol scenarios have dominated the thinking of the biodefense community because of the 2001 letter attacks, the legacy of offensive weapons programs that validate the potential for catastrophic impact from aerosol releases, and the limited ability to protect against such scenarios, (b) (7)(E)

INTRODUCTION

1

A biological terrorism attack within the United States has the potential to cause countless deaths, significant economic damage, and massive psychological distress. Hoping to prevent such an attack from ever occurring, the Department of Homeland Security (DHS) is committed to fostering the development of responsive architectures that, due to a thorough and accurate understanding of how such an attack might play out, are able to thwart the attack or significantly mitigate potential attack consequences.

Because resources are limited, it is important to focus investment on attacks with the potential to produce the highest consequences. DHS Secretary Michael Chertoff emphasized this approach in his remarks to New York University's Center for Catastrophic Preparedness and Response International Center for Enterprise Preparedness on April 26, 2005, noting "As consequence increases, we respond according to the nature and credibility of the threat and any existing state of vulnerabilities. Our strategy is to manage risk in terms of these three variables: threat, vulnerability, consequence. We seek to prioritize according to these variables, and to fashion a series of preventive and protective steps that increase security at multiple levels."


Current knowledge of these three variables for biological attacks lacks the specificity needed to inform investment priorities in effective response strategies. The work described in this report was commissioned to solidify understanding of the consequences of catastrophic biological terrorism attacks, the vulnerabilities and gaps in existing response architectures, and opportunities to enhance the ability of response architectures to prevent and mitigate attacks.

This report describes studies that examined four catastrophic bioterrorism scenarios to better understand the uncertainties and other details associated with the performance of defensive architectures and response countermeasures. Based on the quantitative assessment of the scenario impact—that is, the result of a specific scenario and a specific defensive architectural configuration and performance—gaps in knowledge and in preparedness were identified to provide information that will support enhancements in the nation's defensive posture.

SCENARIO SELECTION

The four scenarios documented in this report were chosen as exemplars of families of bioterrorism scenarios, with a focus on those credible scenarios with the largest potential for catastrophic impact. Specific adversaries were not assumed; rather, the capabilities of adversaries to acquire, prepare and distribute agent were explored as a part of the scenario specification.

Key criteria for selection and analysis of these bioterrorism reference scenarios included scenarios representative of the major classes of potential bioterrorism scenarios, credibility of the scenario, catastrophic impact resulting from the scenario, and a comprehensive, technical end-to-end assessment of the scenario. These criteria are further described below.

- (b) (7)(E)
- 

(b) (7)(E)

(b) (7)(E)

These four scenarios are generally consistent with the scenarios recommended for analysis in work performed by former Secretary of the Navy, Dr. Richard Danzig. He has noted the importance of such reference scenarios or planning cases to create a common, systematic, operational baseline within the bioterrorism defense community. Scenario analysis can establish an end-to-end operational understanding of the unfolding of a bioterrorism event and its many, interacting response elements. Danzig highlights the importance of this common operational understanding as one basis for cooperative decisions among diverse government bureaucracies.

Of course, there is great interest and concern about scenarios beyond this set of four. Assessments of other scenarios have been carried out in related work, including the case of contamination of water supplies and contamination of crops. Additional work on an expansion set of scenarios to augment this set is currently underway under DHS sponsorship.

STUDY APPROACH

The approach for each scenario was to lay out a specific scenario, explore and document the factors and assumptions required to make quantitative estimates, and predict the impact of the scenario, including key issues associated with response alternatives. The significance of this work is the detailed technical treatment of all of the parameters necessary for full explication of a scenario and its impact, along with an assessment of the provenance and uncertainty associated with the parameters used to make the calculations.

Technical teams led by a scenario Principal Investigator conducted the investigation of each scenario. Each parameter associated with specification of the scenario was documented and references and uncertainties described. Data were collected from a wide variety of sources including published and unpublished, classified and unclassified written sources, and consultation and review with knowledgeable members of the community. Workshops and review meetings with government and academic experts were held multiple times since the inception of this work in late 2003. Where possible, the lab teams also worked closely with responder communities to better characterize and analyze the response architectures now in place. These relationships have not only yielded rich information, but are already leading to incremental changes in those responses, which are providing a greater level of protection.



The broad elements that constitute a defensive architecture are similar among the scenarios. These elements include protection, surveillance, detection, rapid response, longer-term response, and restoration. An initial assessment of the effectiveness of current capabilities, policies, and practices formed the basis of the report card. Performance and augmentation of





these systems over time was also examined to provide a temporal assessment element of the report card.

REPORT ORGANIZATION

Following this introductory section, this report is organized into four sections. The following section, Section 2 includes the scenario descriptions for each of the four scenarios. The defensive architecture and its performance are described for each scenario in Section 3. Section 4 includes the gap assessment and report cards for the scenarios, while Section 5 outlines the opportunities for technology together with the need for continuing work.

(b) (6), (b) (7)(E)



- 
- 
- 
- 

SCENARIO DESCRIPTIONS

2

Section 2 presents highlights from the analyses conducted to describe how each scenario might play out, from attack preparation to recovery post epidemic. Each of these scenario descriptions includes many common basic elements:

- The preparation behind each attack
- How the agent is released
- The size of the exposed population
- The number of people infected
- The timing, size, and duration of the economic
- Aspects of the recovery from the attack

A table inserted into each subsection summarizes these attack elements.

These scenario descriptions have some distinct characteristics that set them apart from attack scenarios developed for other studies. First, they are not based on any specific notion of adversary intent or capability. Rather, they are intended to describe attacks with catastrophic outcomes that could credibly take place.

Second, although parameter ranges were considered (as shown in the summary tables), analysts identified a single value for every attack parameter. In many cases, determining this single parameter required recognizing and accounting for uncertainties and unknowns—a process that entailed extensive consultation with experts and considerable analysis. For the sake of brevity, these efforts are summarized—but not detailed—in this report. More detailed descriptions of the scenario analyses are available from the authors.

However, the importance of these detailed analyses cannot be overlooked. In fact, the significance of this report lies in the detailed technical treatment of all the parameters necessary for full explication of a scenario and its impact, as well as in the assessment of the uncertainty associated with the parameters used to make the calculations.