Select Agents and Toxins
Security Information Document

7 CFR Part 331.11, 9 CFR Part 121.11, 42 CFR Part 73.11

Prepared by

U.S. Department of Health and Human Services (HHS)
Centers for Disease Control and Prevention (CDC)
Division of Select Agents and Toxins
Atlanta, GA

U.S. Department of Agriculture
Animal and Plant Health Inspection Service (APHIS)
Agriculture Select Agent Program
Riverdale, MD

March 8, 2007

Preface

Intent: The intent of this document is to provide possible practices and procedures that entities may use to assist them in developing and implementing the written security plan required by the select agent regulations. However, the ideas and suggestions provided in this document do not constitute or establish minimum acceptable standards that would automatically meet the requirements of title 7 of the *Code of Federal Regulations* (CFR) part 331.11, 9 CFR 121.11, or 42 CFR 73.11.

Revisions: This is a living document subject to ongoing improvement. Feedback or suggestions for improvement from Registered Select Agent entities are welcomed. Submit comments directly to the Select Agent Program at:

CDC: LRSAT@cdc.gov

APHIS: Agricultural.Select.Agent.Program@aphis.usda.gov

Table of Contents

Appendices

SELECT AGENTS AND TOXINS SECURITY INFORMATION DOCUMENT
7 CFR PART 331.11, 9 CFR PART 121.11, 42 CFR PART 73.11

I. Written Security Plan (Section 11 (a))

"An individual or entity required to register under this part must develop and implement a written Security Plan. The Security Plan must be sufficient to safeguard the select agent or toxin against unauthorized access, theft, loss, or release."

All select agent entities must develop and implement a written security plan that meets the provisions outlined in this section of the regulation.

II. Site-Specific Risk Assessment (Section 11 (b))

"The Security Plan must be designed according to a site-specific risk assessment and must provide graded protection in accordance with the risk of the select agent or toxin, given its intended use."

The entity must conduct a site-specific risk assessment. The site-specific risk assessment includes:

1. Agent-specific risk assessment (determine risk(s) of select agent or toxin based on intended use)
2. Threat assessment (insider, outsider, anyone desiring to do harm, natural and man made disasters)
3. Vulnerability assessment (security weakness or deficiency at the entity)
4. Graded protection determination (mitigation with a security system(s) approach based on conclusions reached after the agent, threat, and vulnerability assessments have been conducted)

Note: The following assessments can be conducted from an overall perspective or by listing each agent, threat, and vulnerability and evaluating them individually.

Agent-Specific Risk Assessment (APHIS)

Based on the agents in the entity's inventory and their intended use, there are three categories that define the risk associated with agents.

- Low Risk: Agents include emerging pathogens that could be engineered for mass dissemination in the future due to availability, ease of production, or potential for high socio-economic and/or public health impact to American agriculture.

- Moderate risk: Transmissible diseases which are considered to be of socio-economic and/or public health importance within countries and which are significant in the international trade of animals, animal products and plants.
- High risk: Transmissible diseases which have the potential for very serious and rapid spread (irrespective of national borders), are of serious socio-economic or public health consequences, and are of major importance in the international trade of animal, animal products, and plants.

Agent-Specific Risk Assessment (HHS and Overlap Agents)

Based on the agents in the entity's inventory and their intended use, there are four categories that define the risk associated with agents.

- *Low risk* includes agents that are handled in a diagnostic, nonpropagative manner (e.g., single specimen, no culture).
- *Moderate risk* includes agents that are handled in a diagnostic, propagative manner. This level includes only the amounts necessary for experiments at hand (e.g., specimen cultured for diagnostic purposes or produced only in amounts required for the research or experiments being conducted).
- *High risk* includes agents that are handled in large or highly pure quantities such as liters or grams. It would also include those agents and toxins used in restricted experiments or experiments that may increase virulence, and also includes high-risk use (e.g., centrifugation).
- *Highest risk* is a placeholder for smallpox only.

Note: The agent-specific risk categories are based on the concept that all agents and toxins do not pose the same risk or require the same level of protection.

Threat Assessment

Definition: A threat is defined as the capability of an adversary, coupled with intentions, to undertake malevolent action, or forces capable of damaging the operation.

- Could be an insider with authorized access
- Could be an outsider with limited access and system knowledge
- Could be anyone desiring to do harm (i.e., violent acts, anger, hatred, terrorist activity, civil disturbances, special interest groups, attack at gun point, etc.)

Also:

Hurricanes
Severe thunderstorms
Tornadoes
Floods
Bomb threats
Communications failure
Electrical power failure
Fire
HAZMAT incident
Biological and chemical agents
Information technology hacking

Consider: The insider must always be considered a threat.

> Example: In 2004 Robert Hanssen had worked for the FBI for 35 years before his arrest for selling secrets to Russia and the former Soviet Union. Although one would think this is an isolated case, it is not. Cases such as Mr. Hanssen's have occurred at least 15 times since 1985.

Considering all the threats listed above (man, nature, incident), the probability of their occurring may be assessed as low, moderate, or high.

Considering all the threats listed above (man, nature, incident), the consequences, should they occur may be assessed as low, moderate, or high.

Probability and consequences may vary due to the type of threat.

Vulnerability Assessment

Definition: Identified security weaknesses or deficiencies at a facility

- *Low level* means the threats identified at the entity have little or no probability for harm
- *Moderate level* means the threats identified at the entity have some probability for harm
- *High level* means the threats identified at the entity are likely to cause harm

Based on the security weaknesses and deficiencies identified at each facility and the corrective measures considered, the overall vulnerability may be assessed as low, moderate, or high.

Graded Protection (mitigation measures)

Considerations:

The site-specific risk assessment should determine what graded security measures are needed.

The entity needs to consider the number of lockable (secure) barriers that exist starting from the point where select agents and toxins are possessed, used, or transferred, and working outward from that point. In concept, the more barriers that exist, the higher the level of security. These measures can be accomplished using various combinations such as locks, card keys, biometric readers, intrusion detection systems, etc.

Entity Security Conference:

After the agent, threat, and vulnerability assessments are completed, the relevant staff members at the entity (such as the Principal Investigator (PI), Responsible Official, Alternate Responsible Official, Security Staff, Institutional Biosafety Committee, and Laboratory Management) should recommend security measures to be implemented to prevent the theft, loss, and release of select agents and toxins.

Note: The written security plan must contain language relating to the site-specific risk assessment, conclusions reached from those assessments, and security measures that were implemented as a result of those conclusions.

III. Physical Security, Inventory Control, and Information Systems Control (Section 11 (c)(1))

Physical Security: The security plan must describe what physical security measures are in place and their applications. Some examples include guard service; gated entry; barriers; lock boxes; locked storage units; locked entrances to where select agents and toxins are possessed, used, or transferred; barricades; fencing; key and card access; biometric readers and intrusion detection systems. (This list is not exhaustive.)

Operational Security: This includes the training of staff personnel, escort procedures, identification of suspicious persons or activities, inspection of packages, key and access card control management, and related policies and procedures.

Inventory Control: Each entity is required to keep a current and up-to-date inventory. How that inventory is conducted and maintained must be documented in the entity's security plan and must be consistent with the

requirements found in Section 17. The select agents and toxins in the entity inventory must be labeled and identified in a way that leaves no question that what is in stock is accurately reflected in the inventory records. Section 17 gives examples of GenBank Accession Numbers and strain designations as a detailed means of identification. All inventory control records must be safeguarded to prevent alterations and be retained for 3 years. See Appendices A, B, and C.

Information Systems: The security plan must describe security for the entity's information system(s). Questions to consider:

- Is the operating system connected to the Internet?
- What operating systems are in use?
- Are back-up systems utilized?
- Are computer systems internally networked?
- Is there an active system in place to prevent cyber attacks?
- Is there a firewall in place?
- How often are passwords changed?
- Can passwords be reused?
- Is anti-virus software used?
- Are there restrictions on Internet browsing?
- Are e-mail servers protected by a restricted download policy?

(The above list is not exhaustive.) See Appendix D.

Key points: For those laboratories that have key card access, it is important to remember that staff personnel who program these cards can also program access to select agent handling areas. Additionally, locksmiths also have the capability to duplicate keys and gain access. When keys are used, a key control program must be in place.

Secure management controls (for example, locked file cabinets and dedicated file rooms) must be in place for entities that choose to manually store select agent and toxin information such as hard copies and log books. Documents on file that contain access information (ability to gain access to select agent and toxins) must be under the control of a security risk assessment (SRA) approved individual. All other files and correspondence should be in a secure area where it is reviewed and discussed on a "need to know" basis. Access logs need to be reviewed by the Responsible Official regularly to ensure there has been no unauthorized access.

IV. Access Control (Section 10 (b), Section 11 (c)(2), and Section 17 (a)(4))

Access Definition: An individual will be deemed to have access at any point in time if the individual has possession of a select agent or toxin (e.g., ability to carry, possess, use, transfer, or manipulate) or the ability to gain possession of a select agent or toxin.

Access Control: The security plan must describe how access is controlled at the entity. Examples of controls are locks (keyed, combination, punch code), access cards, escort by SRA-approved individuals, and biometrics. (This list is not exhaustive.)

Recording Access: The regulations require a log of individuals entering select agent labs. If an electronic log is utilized, the database controlling access should be capable of printing hard copies. The name, date, and time must be recorded along with the name of SRA-approved individual providing escort (if applicable). Entry records must be safeguarded to prevent alterations and be retained for 3 years.

V. Routine Cleaning, Maintenance, and Repairs (Section 11 (c)(3))

Maintenance and Cleaning: The security plan must state how cleaning and repairs will be accomplished in areas where select agents and toxins are possessed, used, or transferred. Since cleaning and maintenance staffs usually do not have SRA approval, an SRA-approved escort must be provided when select agents and toxins are possessed, used, or transferred.

Provisions for maintenance, cleaning, and repair personnel: In allowing maintenance, cleaning, or repair personnel (whether in-house or contract services) into a select agent area, including into storage areas, an entity should: 1) use only SRA-approved individuals; or 2) provide an SRA-approved individual as an escort at all times for the non-SRA-approved personnel while the non-SRA-approved personnel are in, or have access to, a select agent area; or 3) if the non-SRA-approved individual will not be escorted, install additional security countermeasures (beyond the basic locked freezer/refrigerator/incubator or lock boxes) to prohibit access to the select agents or toxins by non-SRA-approved individuals; or 4) remove the select agents or toxins to a different area that is appropriately registered. If additional countermeasures are used, they may include, but are not limited to, an additional lock and key, cipher lock, or tamper alarms interfaced with the facility intrusion detection system. Section 17 (Records) requires that select agent area access logs must be in place to record the name and date/time of entry into the select agent activity area, including the name of an escort, if applicable.

VI. Unauthorized or Suspicious Persons (Section 11 (c)(4))

Definitions:

Unauthorized person: One who is not SRA approved.

Suspicious person: Any individual not associated with the entity that has no valid reason to be in the areas where select agent or toxins are possessed, used, or transferred. Suspicious persons are generally not known to laboratory staff and generally have no means of identification or credentials.

Unauthorized and Suspicious Persons: A good training and indoctrination program is essential in communicating the procedures for removing unauthorized or suspicious individuals at the entity. Individuals attempting to gain entry into restricted areas without proper credentials shall be challenged and removed immediately. In addition, any suspicious activity or behavior displayed by individuals working with select agents and toxins must be reported to the Responsible Official. The security plan must describe these processes along with the required follow-up actions such as filing an incident report, reporting the information to the Responsible Official, and possibly contacting local law enforcement agencies. This list is not inclusive of all follow-up actions.

VII. Loss or Compromise of Keys, Passwords, Combinations Changing Access Numbers or Locks Following Staff Changes (Section 11 (c)(5))

Addressing Loss and Compromise: The security plan must document the reporting mechanisms for loss of keys and access cards and how they will be replaced. This requires prompt and immediate attention to ensure there is no compromise of security. The entity needs to evaluate whether or not locking mechanisms need to be replaced if keys are used. When an access card has been lost or stolen, the security plan needs to describe the procedure for deactivating access. The security plan must also describe the procedures to follow when a compromise in security has been discovered. Immediate action must be taken to evaluate whether or not locks, keys, access cards, or passwords need to be replaced or changed.

Staff Changes: The security plan must describe the procedures for staff changes and the actions required to change access, passwords, and locks.

VIII. Reporting Unauthorized or Suspicious Persons or Activities
Loss, Theft or Release of Select Agents or Toxins
Alteration of Inventory Records (Section 11 (c)(6))

Unauthorized Persons: Excluding the provisions outlined in Section 11 (c)(3) and Section 11 (d)(2), unauthorized persons are not allowed in rooms where select agents and toxins are possessed, used, or transferred. The security plan must describe the process for reporting and removing unauthorized persons. Should an unauthorized person appear in a restricted area, the written procedures must be followed. Such action should include removing the individual immediately from the space and reporting the incident to the Responsible Official.

Suspicious Persons: Entities using ID cards are advised to have all staff members prominently display their ID badges and cards at all times. ID cards are one means that staff members identify personnel who do not belong in restricted areas. When ID cards are not used, the entity needs to describe in its written security plan the means by which staff members can identify suspicious persons, visitors, and guests. Staff members should also be trained to look for any unusual behavior or suspicious activity displayed by personnel having access to select agents and toxins and follow the procedures outlined in the entity's security plan. Some examples would include a security alert protocol, contacting the Responsible Official, or contacting local law enforcement. (This list is not exhaustive.)

Loss, Theft, or Release of a Select Agent or Toxin: APHIS/CDC Form 3 on the APHIS/CDC select agent home page must be used. As soon as loss or theft or release occurs, the Responsible Official must be notified immediately. The instructions are included on APHIS/CDC Form 3 and must be followed. The Security Plan should make reference to APHIS/CDC Form 3 and describe the required contact and reporting information. Particular attention must be paid to the immediate reporting requirements to APHIS and CDC (as appropriate).

IX. Understanding and Complying with Security Procedures (Section 11 (c)(7) and Section 15)

Security Risk Assessments: Once security risk assessments have been approved, it is important that individuals working with select agents and toxins understand and follow all the security protocols established by the entity. The security plan needs to describe how this information is communicated and understood. This information can be validated by training followed by a test or quiz (also required in training regulations, Section 15). Additionally, the supervisor can validate the training conducted and the level of understanding demonstrated.

X. Access Approval (Section 11 (d)(1))

Access must be approved: The security plan must state clearly that access to select agents and toxins can only be granted to individuals who are SRA approved and who appear on the most current APHIS/CDC Form 1, Section 4B.

XI. Unescorted Access for Cleaning, Maintenance, and Repair Personnel (Section 11 (d)(2))

Provisions for cleaning, maintenance, and repair personnel: When cleaning, maintenance, or repair personnel (either in-house staff or contracted workers) need access to select agent areas (including storage areas), an entity should: 1) use only SRA-approved individuals; or 2) provide an SRA-approved individual as an escort at all times for the non-SRA-approved personnel while the non-SRA-approved personnel are in, or have access to, a select agent area; or 3) if the non-SRA-approved individual will not be escorted, install additional security countermeasures (beyond the basic locked freezer/refrigerator/incubator or lock boxes) to prohibit access to the select agents or toxins by non-SRA-approved individuals; or 4) remove the select agents or toxins to a different area that is appropriately registered. If additional countermeasures are used, they may include, but are not limited to, an additional lock and key, cipher lock, or tamper alarms interfaced with the facility intrusion detection system. Section 17 (Records) requires that select agent area access logs must be in place to record the name, date, and time of entry into the select agent activity area, including the name of an escort, if applicable.

Note: An entity also must provide biosafety information and training to each individual who does have an SRA approval before he/she works in or visits areas where select agents and toxins are possessed, used, or transferred. The training should be tailored to address the risks posed by the select agents and toxins present as well as any particular needs of the individual or the work required.

XII. Means of Securing Select Agents and Toxins (Section 11 (d)(3))

Means of Securing Select Agents: Select agents and toxins must be secured against unauthorized access. There are many ways this can be accomplished. Some examples include, but are not limited to, padlocks, lock boxes, card access, biometric readers, and intrusion detection systems. The methods used to secure select agents and toxins against unauthorized access must be addressed in the written security plan. If keys are used, a key control plan needs to be in place to safeguard the keys and who has access to them. If key cards are used, a plan should be in place to monitor creation and change of reader access.

When padlocks and hasps are used, the entity should consider using padlocks and hasps that are made of case-hardened steel. Case-hardened steel is more resistant to cutting and repeated smashing. Additionally, a padlock and hasp should be installed by a skilled maintenance person.

Site-specific risk assessment conducted by the entity may determine a need for a higher level of protection to secure select agents and toxins against unauthorized access. This is what is meant by "equivalent or even a greater level of protection."

XIII. Inspection of Packages (Section 11 (d)(4))

Definition of Suspicious Package: Any package or item that enters or leaves the select agent handling area that does not appear to be consistent with what is expected during normal daily operations.

Some indicators to watch for:

- Misspelled words
- Address to title only or incorrect title
- Badly taped or sealed
- Lopsided or uneven
- Rigid or bulky
- Oily stains, discolorations, or crystallization on the wrapper
- Excessive tape or string
- Protruding wires
- Housekeeping cart, tool boxes, unauthorized removal of lab equipment

Inspection of Packages: This applies to suspicious packages and items entering or being removed from rooms where select agents are handled (select agent lab, shipping and receiving area). Suspicious packages should be inspected by visual or noninvasive techniques before they are brought into, or removed from, the area where select agents or toxins are possessed, used, or transferred. The security plan must describe how the entity will meet the inspection of packages requirement. The guidelines for recognizing suspicious packages are provided in Appendix H and can be found on the U.S. Postal Service and CDC Web sites.

XIV. Intra-entity Transfers (Section 11 (d)(5))

Intra-entity Transfer Definition: A transfer that takes place between two SRA-approved individuals at the same registered entity (usually from one PI to another). An intra-entity transfer can also be a PI transferring an outgoing shipment to an SRA-approved individual in the shipping department.

Intra-entity Transfers: Entities that conduct intra-entity transfers must have, in their security plan, a description of how these transfers will take place, including chain of custody.

An intra-entity transfer occurs when a select agent or toxin is transferred from one PI to another PI within the same entity under the same registration. An intra-entity transfer can also take place when select agents and toxins transferred from one SRA-approved person in one department to another SRA-approved person in

another department. An example is the PI packaging a select agent and taking it to an SRA-approved individual in the shipping department. An example of an intra-entity transfer form can be found in Appendix E.

Transfers accompanied by a chain of custody ensure that select agents will not be left unattended. If intra-entity transfers do not apply, the security plan should state so. An example of chain of custody forms can be found in Appendices F (HHS) and G (APHIS).

XV. Sharing Access (Section 11 (d)(6))

Piggybacking and Tailgating Definition: Gaining entry into a registered area using another individual's means of access, such as a key, personal Identification number, or access card.

Sharing Access Prohibited: The security plan must state that any person accessing select agents and toxins will not share their unique means of access (such as key cards and passwords) with any person. Piggybacking or tailgating on another SRA-approved access card or other means of access is strictly prohibited. When personnel piggyback or tailgate, their access is not recorded into the electronic data base. This practice results in inaccurate access logs and may promote an opportunity for theft. For those entities that use nonelectronic access control, the security plan must describe the key control program and how the security of the program is maintained. Access cards are occasionally left at home; the security plan should have a means to address this.

Annual training can be used to convey this information to the select agent program staff (Section 15(a)).

XVI. Reporting Requirements to the Entity's Responsible Official (Sections 11 (d)(7)(i) through (v))

The following must be reported to the Responsible Official:

- Any loss or compromise of keys, passwords, and combinations
- Any suspicious persons or activities
- Any loss or theft of select agents or toxins
- Any release of a select agent or toxin
- Any sign that inventory or use records for select agents or toxins have been altered or otherwise compromised

Other scenarios may also need to be reported. Since these reporting requirements relate to extremely important issues within the select agent program, it is important that they be reported immediately.

Once reported, the Responsible Official must take the appropriate action for handling the issue. This includes making required notifications and completing the required forms such as APHIS/CDC Form 3.

XVII. Public Access Areas (Section 11 (d)(8))

The area(s) where select agents and toxins are possessed, used, or transferred must be separated from public access areas. Examples include cafeterias, clinics, restrooms, and libraries. (This list is not exhaustive.)

XVIII. Select Agent Reference Document (Section 11 (e))

In developing a Security Plan, an entity or individual should consider the document entitled *Laboratory Security and Emergency Response Guidance for Laboratories Working with Select Agents*, published in Morbidity and Mortality Weekly Report, December 6, 2002; 51:RR-19:1-6. The document is available on the Internet at http://www.cdc.gov/mmwr. This reference closely parallels some of the language implemented in the regulations. It has good information on risk assessments, security plans, access control, accountability, transfers, and emergency response reporting (now called incident response).

XIX. Drills and Exercises (Section 11 (f))

Reviews, Evaluating Effectiveness: The biosafety, incident response, and security plans require an annual review as well as drills and exercises to test the effectiveness of all three plans.

Revision of the Security Plan: The security plan must be revised after any drill or exercise, after any incident, and as necessary to address new issues as they become known. This would also include any remodeling that would affect security as well as any changes to the information technology (data) systems.

XX. Retention of Records (Section 17 (c))

Records are required to be retained for three years and include the following: Inventory, transfers, theft, loss release, responsible official's records, security, biosafety, incident response, and training. Documents on file that contain access information (ability to gain access to select agent and toxins) must be under the control of an SRA-approved individual. All other files and correspondence should be in a secure area where it is reviewed and discussed only on a "need-to-know" basis.

Security cameras that record activity within the select agent rooms and related areas are security monitoring devices. Digital and analog recordings from these devices are considered records and, whenever feasible, entities should keep these records for a minimum of 45 days. These recordings are not required to be retained for 3 years.

APPENDIX A

Select Agent Inventory Requirements and Example Document. Reference is Section 17 (a)(1)(i-v) and (a)(6).

- Select agent name and characteristics (strain, GenBank Accession number, etc.)
- Quantity acquired (containers, vials, tubes, etc.)
- Date of acquisition and source
- Where stored (building, room, freezer)
- When moved from storage and by whom
- When returned to storage and by whom
- Select agent used and purpose of use
- Date destroyed
- Discrepancies

APPENDIX A, continued

EXAMPLE OF A SELECT AGENT INVENTORY FORM THAT CAPTURES THE REQUIREMENTS LISTED IN
Section 17 (a)(1)(i-v) and (a)(6)

SELECT AGENT NAME: TYPE: STRAIN DESIGNATION:
GENBANK ACCESSION NUMBER:

QUANTITY ACQUIRED: DATE OF ACQUISITION: SOURCE OF ACQUISITION:

WHERE STORED:
BUILDING: ROOM: FREEZER:

INVENTORY OF USAGE

DATE REMOVED FROM STORAGE	QUANTITY REMOVED	REMOVED BY	PURPOSE OF USE	DATE RETURNED TO STORAGE	QUANTITY RETURNED	RETURNED BY	DATE DESTROYED	QUANTITY REMAINING

Comments/Discrepancies:_____
_____
_____

APPENDIX B

Toxin Inventory Requirements and Example Document. Reference is Section 17 (a)(2)(i-vi, x) and (a)(6).

- Name and characteristics
- Quantity acquired (containers, vials, tubes, etc.)
- Date of acquisition and source
- Initial quantity
- Current quantity
- Toxin used
- Purpose of use
- Quantity used
- Date used
- Used by whom
- Where stored
- When moved from storage and by whom including quantity
- When returned from storage and by whom including quantity
- A written explanation of any discrepancies

APPENDIX B, continued

EXAMPLE OF A TOXIN INVENTORY FORM THAT CAPTURES THE REQUIREMENTS LISTED IN
Section 17 (a)(2)(i-vi, x) and (a)(6)

TOXIN NAME: CHARACTERISTICS:

QUANTITY ACQUIRED: DATE OF ACQUISITION: SOURCE OF ACQUISITION:

INITIAL QUANTITY:

WHERE STORED:
BUILDING: ROOM: FREEZER:

INVENTORY OF USAGE

CURRENT QUANTITY	DATE REMOVED FROM STORAGE	QUANTITY REMOVED	REMOVED BY	USED BY	DATE RETURNED TO STORAGE	QUANTITY RETURNED	RETURNED BY	PURPOSE OF USE	DATE DESTROYED	QUANTITY REMAINING

Comments/Discrepancies:_____
_____
_____

APPENDIX C

Intra-entity Transfer Inventory Requirements and Example Document. Reference is Section 17 (a)(2)(vii and viii).

- Name of select agent or toxin
- Quantity transferred
- Date of transfer
- Sender
- Recipient

APPENDIX C, continued

EXAMPLE OF AN INTRA-ENTITY INVENTORY FORM THAT CAPTURES THE REQUIREMENTS LISTED IN
Section 17 (a)(1)(vii) and (a)(2)(viii)

INTRA-ENTITY TRANSFER INVENTORY

SELECT AGENT/TOXIN	STRAIN / CHARACTERISTICS	QUANTITY TRANSFERRED	DATE OF TRANSFER	SENDING LAB		RECEIVING LAB	
				NAME OF LAB	P. I	NAME OF LAB	P. I.

Comments:

APPENDIX D

Information Systems Control Example Document

IT Contact Name_____

Contact Office Phone _____

Contact Fax _____

Contact e-mail address_____

Fill in the information describing your Information Systems Security Program. Check all that apply:

A. Information Technology (IT) Infrastructure

Security Firewall Protection	Yes	No
Anti-Virus/Worm Protection	Yes	No
Network Password Protection	Yes	No
Desktop Password Protection	Yes	No
Certified/Accredited Systems	Yes	No
Data Classification Hierarchy	Yes	No
Security Patch Mgt. Procedures	Yes	No

B. Hardware Assets Protection

Main Computer Room Protection	Yes	No
Office Protection	Yes	No
Laboratory Protection	Yes	No
Wiring/Cable Closet Protection	Yes	No
Restricted Access Protection	Yes	No
Secured Space for Sensitive Info	Yes	No
Property Inventory Controls	Yes	No
Fire Protection and Alarms	Yes	No

C. Personnel Security

Background Check for IT Staff	Yes	No
Background Check for IT Part-Time	Yes	No
Vendor Background Check	Yes	No
Personnel Records Secured	Yes	No
Information Security Manager	Yes	No
Security Policy/Procedures	Yes	No

D. Data Protection

Data Encryption	Yes	No
Remote Access Protocols	Yes	No
Web Data Sanitized	Yes	No

Log On/Off Procedures	Yes	No
Access Denial Protocols	Yes	No
Select Agent Inventories Secured	Yes	No

Note: In using this document, a box checked "No" does not imply that the entity must make it a "Yes" in order to satisfy the provisions of the CFR for information systems control. The purpose of this document is to determine what the entity has in place.

Additional Remarks:

APPENDIX E
Intra-entity Transfer Request Example Document

Intra-entity Select Agent Transfer Request

This tracking document must have Responsible Official (RO) approval BEFORE transferring select agents from one entity lab to another.

Requestor: Complete block 1 and transmit to transferring lab.
Transferor: Complete block 2 and transmit form to the RO.
RO: RO assigns a tracking number and indicates approval of transfer with signature in block 3. RO returns form to transferor to initiate agent transfer.
Requestor: Complete block 4 when transfer complete and return form to RO

BLOCK 1

Requestor Name:		Signature:	Date:	Lab Location (bldg, room):
Principle Investigator:		Signature:	Date:	
Select Agent Type:				
Genus/Species:		Toxin:		
Recombinant Organism:		Recombinant Molecule:		
Intended Use:	Diagnostics ☐	Research ☐	Production ☐	Other: ☐
Material: Activated	Inactivated	Explain How:		

BLOCK 2

Transferor's Name:		Signature:	Date:	Lab Location (bldg. room):
Principle Investigator:		Signature:	Date:	
Agent Characterization:				
# Vials:	Vol or wt per vial:	Form:	Total Quantity:	

BLOCK 3

RO:	Signature:	Date:	Tracking #:

BLOCK 4

Amount per Primary Receptacle:	Number of Primary Receptacles per Container:	Number of Outer Packages:
Receipt Acknowledged by Recipient:		Date:

APPENDIX F
HHS Chain of Custody Example Document

CHAIN OF CUSTODY FOR SELECT AGENT SHIPMENTS

FORM 2 Approval Number: _____

a. Released from Inventory by: Print: Sign:	Date:	Time: AM PM
b. Accepted for Packaging and Shipping by: Print: Sign:	Date:	Time: AM PM
c. Outer Secondary Container Sealing Witnessed by: Print: Sign:	Date:	Time: AM PM
d. Packed for Shipment by: Print: Sign:	Date:	Time: AM PM
e. Package Marked and Labeled by: Print: Sign:	Date:	Time: AM PM
f. Packaged Locked/Secured by: Print: Sign:	Date:	Time: AM PM
g. Picked up at Shipping Area by Courier/Transporter: Print: Sign:	Date:	Time: AM PM
Air Waybill Number: FedEx Airborne Other_____	(circle one)	
Notes:		

APPENDIX G
APHIS Chain of Custody Example Document

Section 1

XYZ Corporation 123 Main Street Any City, USA 10101 Tel: (218) 560-8070 Fax: (218) 560-8071	Instructions: • All external (inter-entity) transfers are required to be in compliance with Section 16. An XYZ Corporation Chain of Custody Form is required to be completed, in addition to APHIS/CDC Form 2 and filed in the Chain of Custody Logbook. Receiving laboratory is required to sign and FAX Chain of Custody Form, once select agent material is received, to the XYZ Corporation. • All internal (intra-entity) XYZ Corporation transfers are required to be in compliance with Section 16 . An XYZ Corporation Chain of Custody Form is required to be completed and filed in the Chain of Custody Logbook. • Chain of Custody Form is required to be signed by the Responsible Official (RO) and Principal Investigator (PI).								
Select Agent/Toxin _____ Signature of Responsible Official _____ Signature of Principal Investigator	Transfer Use for internal and external transfers. ********** If transfer exceeds 8 actions use second form.		Received Use for internal and external transfers. ********** If transfer exceeds 8 actions use second form.		Type of Transfer Check box ☑ below and complete Section 2 for external shipping/receiving. ********** For internal transfer provide an entry of each movement in the below columns noting each location code.		Location Code ST- Storage SL- Storage to Lab LS- Lab to Storage LL- Lab to Lab O- Other (explain)	Number of Primary Containers Use for internal and external transfers. ********** If transfer exceeds 8 actions use second form.	Remarks
	Date	Time	Date	Time	Internal☑	External☑			
1)					☐	☐		☐☐☐☐☐	
2)					☐	☐		☐☐☐☐☐	
3)					☐	☐		☐☐☐☐☐	
4)					☐	☐		☐☐☐☐☐	
5)					☐	☐		☐☐☐☐☐	
6)					☐	☐		☐☐☐☐☐	
7)					☐	☐		☐☐☐☐☐	
8)					☐	☐		☐☐☐☐☐	

Section 2: External (inter-entity) Shipping and Receiving Information (Check ☑ appropriate box)

Authorization/Ship to: ☐	Received From: ☐	Authorization/Ship to: ☐	Received From: ☐	Instructions: Section 2 provides for two (2) shipping and receiving actions. Check ☑ the appropriate box beginning with the first action-shaded area.
Organization: RO Signature:_____ Date:	Organization: Signature: _____ Date:	Organization: RO Signature: _____ Date:	Organization: Signature: _____ Date:	

APPENDIX H
Suspicious Package Guidelines

UNITED STATES POSTAL SERVICE

SUSPICIOUS MAIL ALERT

If you receive a suspicious letter or package:

1 Handle with care. Don't shake or bump.

2 Isolate it immediately

3 Don't open, smell, touch or taste.

4 Treat it as suspect. Call local law enforcement authorities

If a parcel is open and/or a threat is identified . . .

For a Bomb:
Evacuate Immediately
Call Police
Contact Postal Inspectors
Call Local Fire Department/HAZMAT Unit

For Radiological:
Limit Exposure - Don't Handle
Evacuate Area
Shield Yourself From Object
Call Police
Contact Postal Inspectors
Call Local Fire Department/HAZMAT Unit

For Biological or Chemical:
Isolate - Don't Handle
Evacuate Immediate Area
Wash Your Hands With Soap and Warm Water
Call Police
Contact Postal Inspectors
Call Local Fire Department/HAZMAT Unit

This is an FBI – DHS – HHS/CDC Coordinated Document

A large number of potentially suspicious letters and packages continue to be reported to federal, state, and local law enforcement and emergency response agencies nationwide. In some instances these letters or packages may include powders, liquids, or other materials. Federal, state, and local response agencies should be mindful of the potential for small-scale exposure, which could result from material contained in threatening or suspicious packages. While this information is generally focused on the initial response to potential biological threats, all personnel responding to such incidents must be aware of the potential for exposure to hazardous chemical and/or radiological materials in addition to biological hazards. Additionally, there may be a threat posed from secondary releases or devices. Consistent with established protocols, response agencies should follow standard law enforcement procedures and hazard risk assessments in response to calls, and should pre-identify the relevant local public health points of contact to be notified in the event of a potential bioterrorism event.

The following guidelines are recommendations for local responders, based on existing procedures (including recommendations from the International Association of Fire Chiefs). This document provides information on the initial response to a suspicious letter/container, while other follow-on response plans, such as portions of the National Response Plan (NRP), may be utilized if a threat is deemed credible. In general, these potential threats or incidents fall into one of five general scenarios. They are as follows:

1. Letter/container with unknown powder-like substance and threatening communication (with or without illness):

Since there is an articulated threat, it is likely that the substance was intentionally introduced into the package in an effort to validate that threat. An articulated threat itself (with or without the presence of a suspicious substance) is a federal crime and may also constitute a violation under state and local statutes. The local Federal Bureau of Investigation (FBI) Weapons of Mass Destruction (WMD) Coordinator and/or FBI Joint Terrorism Task Force (JTTF), a certified HAZMAT unit, local law enforcement, and the local public health department should be notified. The role of Incident Commander (IC) will be assumed by the appropriate authority, as designated by state or local law. In many cases, the IC will be the most senior public safety officer (most likely the fire department chief or deputy chief, however, in many circumstances it may be a local sheriff or senior local or state police official). As such, it is the responsibility of the IC to establish the Incident Command System (ICS) and to ensure that notifications of the above-mentioned responders have been made or are in the process of being made. As the referenced agencies arrive, the IC will evolve into a Unified Command, as necessary.

Information on Initial Responses to a Suspicious Letter / Container
With a Potential Biological Threat

At this stage, and later again as necessary, the FBI will conduct a timely WMD threat assessment with local law enforcement/fire/HAZMAT personnel. Depending on the nature of the threat, this assessment may include relevant interagency partners. This process utilizes coordination from FBI Headquarters elements

to conduct an initial assessment of the credibility of the threat and provide technical support to responders who are on-scene. In coordination with recommendations from the threat assessment process and the unified command on-scene, an appropriately trained HAZMAT unit should screen evidence for the presence of chemicals and radiological material and double-bag in clear sealed bags (where possible), consistent with chain-of-custody requirements. Before packaging and when possible, photographs of the letter/container should be taken and relevant information should be documented, in coordination with the FBI WMD Coordinator. Under NO CIRCUMSTANCES should an unprotected responder, such as a law enforcement officer, attempt to package an unknown substance.

If this incident involves an unopened container such as a box, it must be evaluated by a certified bomb technician/explosives ordinance disposal personnel prior to being handled by HAZMAT. Any such letters/packages must also be evaluated by the HAZMAT unit for only a broad class of radiological and chemical threats prior to being released to law enforcement personnel for transport. This is required by the laboratory in an effort to protect the staff members who will ultimately be opening the container and performing definitive biological testing and/or forensic examinations.

The FBI, or the responding law enforcement agency, will ensure that a certified HAZMAT team has performed necessary field safety screening before transporting to an appropriate laboratory. This field safety screening should be clearly documented and limited to screening for pH (for liquids), radioactivity, volatile organic compounds, flammable materials, and oxidizing agents. Definitive analysis will only be performed by the appropriate laboratory.

A chain-of-custody form must be initiated along with an incident report. The FBI will then coordinate delivery of the evidence to the designated Laboratory Response Network (LRN) laboratory for further testing and analysis.

If individuals immediately present with illness in this scenario, the public health departments will have an increased role in the initial response. These issues are further addressed in the 'Critical Response Issues for Scenario #1' included below.

If the FBI Headquarters-led threat credibility assessment process deems the threat to be credible, the FBI will immediately notify the Centers for Disease Control and Prevention (CDC), the Department of Homeland Security Operations Center (HSOC), and other appropriate federal agencies. Appropriate response guidelines to a credible threat will be utilized from the NRP, including the Biological Annex and Terrorism Incident Law Enforcement and Investigation Annex. Depending on the nature and scale of the incident, the Department of Homeland Security (DHS) may choose to help coordinate response activities based on NRP procedures which, at a minimum, may include coordinating a joint public affairs statement.

2. Letter/container with a threat but no visible powder or substances present:

Merely threatening the use of a chemical or biological agent *is* a violation of federal law and merits investigation. As in scenario #1, all of the responders should be notified. Although no powder may be visible to the eye, there could be trace amounts of material present that could represent a health risk and also provide critical forensic evidence required for further investigation and prosecution. Therefore, the information in Scenario #1 also applies to responses to a letter/container containing a threat with no visible powder or substance.

3. Letter/container with unknown powder, no articulated threat, and no illness:

As there is no threat and no one is ill, it must be determined if there is a logical explanation for the presence of this substance. For example, HAZMAT teams have responded to a number of letters that contained crushed samples from vitamin and pain-relief companies. If a reasonable and defendable explanation can

be given as to the source of the substance, that there is no articulated threat, and that no one is ill, then no further actions are necessary.

If, however, a reasonable source cannot be determined or there is any uncertainty, the steps outlined in scenario #1 must be conducted.

4. Letter/container with no visible powder, no threat, but recipients are ill:

This scenario has the most potential for ambiguity and confusion. Those who come in contact with *Bacillus anthracis* (anthrax), or other biological pathogens/toxins, may not immediately appear symptomatic. Although no powder or substance may be available to be collected for environmental testing, public health officials may decide to utilize clinical samples from potentially exposed individuals. Additionally, in this scenario it may be difficult to determine if a letter/container is actually associated with the illness. As there is no specific threat to investigate, this is primarily a public health and medical issue; but this scenario also represents a potential criminal act that should be jointly investigated by public health and law enforcement. The initial notifications will largely be the same as scenario #1, with public health taking a primary role in the response. While the primary concern is the treatment and well-being of the recipient, public health and law enforcement should maintain close contact, while public health determines the nature of the illness and law enforcement examines any relevant intelligence. Depending on the scale and nature of the incident, if HHS/CDC is notified they will maintain close contact and coordinate with DHS. If a potential criminal nexus is identified, the FBI will conduct an initial threat assessment and initiate appropriate actions and notifications listed under scenario #1.

5. Letter/container arrives with no powder, no threat, the recipient is not ill, but the recipient is concerned about the package:

With strict regard to federal criminal statutes, no investigative actions are necessary in this matter. However, if other threat indicators are present such as excess postage, misspelled names, unusual odors/colors, etc., law enforcement and the United States Postal Inspection Service should be notified to evaluate it for potential hazards. If the assessment determines that the letter/container is "suspicious," then appropriate steps outlined in scenario #1 would be initiated.

Critical Response Issues for Scenario #1:

1. Request the assistance of the nearest certified hazardous materials response team to conduct risk assessments, field safety screening, sample (evidence) collection, decontamination, and other mitigation activities. Any sample (evidence) collection must be coordinated with law enforcement (FBI).

2. Notify appropriate law enforcement (local, state and local FBI WMD coordinator/JTTF, postal inspectors) when a potential threat is identified.

3. Do not touch, move, or open any suspicious package until an initial hazard risk assessment of the package can be performed in coordination with HAZMAT personnel and law enforcement.

4. An initial threat credibility assessment will be coordinated via the local FBI WMD Coordinator and the FBI Counterterrorism Division's Weapons of Mass Destruction Operations Unit (WMDOU). This will include the FBI Laboratory Division, Hazardous Materials Response Unit (HMRU) and other select interagency subject matter experts, tailored for the specific threat. This assessment includes an analysis of technical feasibility, operational practicability, behavioral resolve, and examination of any intelligence that might relate to the threat. If the threat is determined to be credible, other appropriate federal agencies will be notified, to include DHS and HHS/CDC. Additional information on this process is available from the NRP, including the Biological Annex and Terrorism Incident Law Enforcement and Investigation Annex.

5. Contact your local public health department (who should in turn notify state authorities and the CDC) if there is a threat of public health exposure or environmental contamination exists. HHS/CDC will then notify the HSOC, where appropriate.

6. In coordination with law enforcement, always notify the U.S. Postal Inspection Service, whenever it appears that the threat was delivered through the U.S. Postal Service. Assist with ensuring that origin and tracking information is obtained from the package (ideally, photographs of the front and back).

7. Treat the scene as a crime scene. Preserve evidence in coordination with law enforcement and ensure that materials are safely packaged. Take steps to retain enough suspicious material for:

a. Laboratory analysis;
b. Forensic examination of criminal evidence, regardless of whether the threat is ultimately determined to be accompanied by a hazardous material.

8. Transfer custody of evidence to a law enforcement officer as soon as possible. Maintain chain of custody by obtaining a record of names and signatures every time custody of a suspicious material or sample for laboratory analysis changes hands.

9. Perform basic field safety screening of the substance to rule out explosives, radiation, flammability, corrosives, and volatile organic compounds prior to transporting the materials to the appropriate LRN, as coordinated with the FBI WMD Coordinator. All field safety screening that is performed by responders should be clearly documented and shared with law enforcement and the LRN.

10. In coordination with the local FBI WMD Coordinator (and/or a responding law enforcement entity), transport samples to the designated CDC-qualified LRN facility. If field safety screening detects the presence of chemical or radiological hazards, the FBI WMD Coordinator will contact FBI Headquarters for information regarding which laboratory is appropriate to perform the analysis. This will be done as part of the threat credibility assessment process noted above (see #4).

11. In coordination with public health and law enforcement, identify and list the names and contact information for anyone who may have been exposed to the suspicious substance so that they may be contacted when the LRN test results are available or if there is other additional information. If positive results are obtained, state and local public health departments will need to contact those potentially exposed as soon as possible to provide appropriate assistance (e.g., antibiotics, education, additional testing, vaccination, surveillance/symptom reporting).

12. In coordination with the FBI, identify a single point-of-contact for incident follow-up.

13. If LRN tests identify positive results for threat agents or a threat is determined to be credible, the FBI will immediately notify the DHS and other appropriate federal agencies to initiate relevant NRP actions, as necessary. The DHS will work closely with the FBI, HHS/CDC and other agencies to ensure a coordinated response.

Note on field screening

Once activities are complete to address immediate public safety concerns, every effort must be made to preserve evidence necessary for public health and law enforcement investigations.

In situations where biological threat agents are suspected, the item(s) should be field safety screened and

immediately transported in law enforcement custody to an LRN laboratory. This should be done in coordination with the local FBI WMD Coordinator.

Field safety screening should be limited to ruling out explosive devices, radiological materials, corrosive materials and volatile organic compounds. Currently, there are no definitive field tests for identifying biological agents. Additional field testing can mislead response efforts by providing incorrect or incomplete results, and destroy limited materials critical for definitive laboratory testing required to facilitate any appropriate public health and law enforcement response.

This document is provided for information. Questions related to the content of this document can be addressed to your local FBI WMD Coordinator.