

American Biological Safety Association Conference 2007- Guide to Developing a Security Plan

Robert L. Rice
Security Program Officer
Agriculture Select Agent Program

U.S. Department of Agriculture
Animal and Plant Health Inspection Service
Veterinary Services
National Center for Import and Export
Technical Trade Services Team-Select Agents

Nashville, TN

October 6, 2007

Introduction

- Overview
- Key Components
- Entity Role vs. Government Role
- Site-specific Risk Assessment
- Objectives of Security
- Physical Security vs. Operational Security
- Security Plan Development Aids
- Areas of Interest to Security
- Elements for Security Plan Development
- Incident Response Plans
- APHIS/CDC Inspection Checklists for Security
- Questions

Overview

- Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (includes the Agricultural Bioterrorism Protection Act of 2002)
- U.S. Department of Agriculture (USDA), Animal and Plant Health Inspection Service (APHIS)
 - 7 CFR Part 331
 - 9 CFR Part 121
- U.S. Department of Health and Human Services (DHHS), Centers for Disease Control and Prevention (CDC)
 - 42 CFR Part 73

Overview

- In compliance with the Bioterrorism Act of 2002 [The Act], USDA and HHS established regulations to ensure that all entities using or possessing select agents and toxins do so in a safe and secured manner to prevent unauthorized use:
 - **“Establish and enforce safeguard and security measures to prevent access to listed agents and toxins for use in domestic or international terrorism or for any other criminal purpose.”**
- CFR requires all entities that possess, use and/or transfer select agents and toxins to develop site specific written security plans.

Overview

- Security related CFR Sections:
 - Responsible Official [§331.9; §121.9; §73.9]
 - Security [§331.11; §121.11; §73.11]
 - Incident Response [§331.14; §121.14; §73.14]
 - Training [§331.15; §121.15; §73.15]
 - Records [§331.17; §121.17; §73.17]

Key Components

- Two key requirements in 7 CFR § 331.11(b), 9 CFR § 121.11(b) and 42 CFR § 73.11(b) must be addressed in order to develop a successful security plan and program:
 - **“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.”**

Entity Role vs. Government Role

- The entity is required to develop written security; biosafety; and, incident response plans that adequately describes the provisions they have in place to secure and safeguard the select agents and toxins based on a site-specific risk assessment
- The government's role is to review and approve those plans, and
- Determine whether the entity should possess, use, or transfer select agents

Site-specific Risk Assessment

■ Security Formula

□ Vulnerabilities + Threats + Mitigations = Security Infrastructure

■ Vulnerabilities

□ “soft” spots inherent in the facility

■ Threats

□ Internal or external

□ Can be natural

Site-specific Risk Assessment

■ Mitigations

- Policies and procedures that off-set vulnerabilities and threats that will maintain an adequate level of security

■ Security Infrastructure

- Security that is currently in place at the time risk assessment is performed

■ Graded Protection

- Driven by the results of the risk assessment
- Level of mitigations put into place

Objectives of Security

- The Code of Federal Regulations implies:
 - Deterrence
 - Detection
 - Delay

Physical Security vs. Operational Security

■ Physical Security

- Physical [fence, locked doors, locked freezers, guards]
- Technological [electronic, bio-metric]
- Mechanical [locks and keys]

■ Operational Security

- Human aspect
- Policy and procedures [SOP's]
- Employee awareness [training]
- Post orders
- Key and password management

Security Plan Development Aids

- Code of Federal Regulations, March 18, 2005
[7 CFR 331, 9 CFR Part 121 and 42 CFR 73]
- Select Agents and Toxins Security Information Document, March 8, 2007
- Select Agents and Toxins Security Plan Template, March 8, 2007
- APHIS/CDC Security Inspection Checklist, June 5, 2007
- <http://www.selectagents.gov>

Areas of Interest to Security

- Select Agent Activity Area(s)?
 - Single or multiple buildings
 - Laboratory specific
 - Greenhouses and propagation rooms
 - Growth Chambers
 - Shower facility
 - Anterooms
 - Local or Extended storage areas
 - Airlocks

Elements for Security Plan Development

- The three security components [§121.11(c); §331.11(c); §73.11(c)]:
 - Physical Security
 - Information Systems Control
 - Inventory Control

Elements for Security Plan Development

- Associated components that require procedures:
 - Personnel Security [§121.11(d)(1); §331.11(d)(1); §73.11(d)(1)]
 - Incident Response [§121.14; §331.14; §73.14]
 - Training [§121.15; §331.15; §73.15]
 - Records [§121.17; §331.17; §73.17]

Elements for Security Plan Development

- Physical Security
 - Perimeter of facility/site
 - Entry security
 - Interior security
 - Security planning and operation

Elements for Security Plan Development

- Information Systems Control means reviewing procedures for:
 - Non-electronic information storage such as hardcopy records
 - IT infrastructure
 - Firewalls, anti-virus, password protection
 - Hardware asset protection
 - Computer room protection, laboratory/office protection
 - Personnel security
 - Background check for primary IT systems administrators
 - Data protection
 - Data encryption

Elements for Security Plan Development

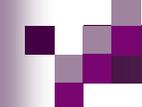
- Inventory Control means checking:
 - Inventory management
 - Inventory control manager, training
 - Inventory data management
 - Electronic data storage
 - Logbooks for accuracy
 - Tracking
 - Chain-of-custody
 - Transfer records

Incident Response Plans

■ Incident Response

□ Written plan specific to the site

- Covers incidents related to theft, loss and release
- Covers natural and man-made disasters
- Must be tested annually via drills and exercises and revised as needed



APHIS/CDC Inspection **Checklists for Security**

- Security Inspection Checklist [Section 11]
- Incident Response Checklist [Section 14]
- Training Inspection Checklist [Section 15]
- Records Inspection Checklist [Section 17]

APHIS/CDC Inspection Checklists for Security

- Special attention items:
 - Security Checklist
 - Verification of site-specific risk assessment
 - Written protocols that describe specific procedures
 - Look for logs that address conducting drills, exercises and annual reviews
 - Incident Response Checklist
 - Verify that an Incident Response Plan is in place and available to employees
 - If Plan is part of an overall entity-wide plan, check to see if select agents and toxins are specifically covered
 - Look for logs that address conducting drills, exercises and annual reviews
 - Personal Protective Equipment

APHIS/CDC Inspection Checklists for Security

- Special attention items (continued):
 - Training
 - Verify that training includes biosafety, security and incident response for authorized SA personnel
 - Training is also extended to those individuals that are not SRA-approved, but have legitimate need to enter the area where SA's are handled or stored
 - Initial training would be required anytime a new employee is hired that will be working with select agents
 - Refresher training is performed annually

APHIS/CDC Inspection Checklists for Security

- Special attention items (continued):
 - Records
 - Physically check the presence of all records
 - Match inventory records with actual inventory
 - Make sure all recording “fields” are filled in on logbooks, etc.
 - Check dates to determine 3 year retention requirements
 - Check for inventory discrepancy, theft, loss, or release records
 - Current list of SRA-approved personnel



Questions and Answers?