Select Agent Program Workshop

November 2012

Agricultural Select Agent Program (USDA/APHIS)

CDC Select Agent Program (HHS/CDC)

Bioterrorism Risk Assessment Group (FBI/CJIS)

Information Systems Security Control

Robert L. Rice
Security Manager

U.S. Department of Agriculture
Animal and Plant Health Inspection Service
Veterinary Services
Agricultural Select Agent Program

November 16, 2012
Atlanta, GA

Agenda

- ❑ Background for Change
- ❑ Key Points
- ❑ Previous Rule Provisions
- ❑ Game Changer
- ❑ The New Look
- ❑ “Cyber-security” or “Information Systems”
- ❑ What Information Should be Controlled?
- ❑ The Responsible Official- What to Consider?
- ❑ What is a deficiency?
- ❑ Review Material and Tools
- ❑ Questions

Background for Change

- Executive Order 13486, Strengthening Laboratory Biosecurity in the United States, Working Group, July 2009: Chapter 4- Physical Security.
- BMBL, 5th Edition, December 2009: Section VI- Principles of Laboratory Biosecurity (new).
  - Information Security
- Responsible Research with Biological Select Agents and Toxins, National Research Council, 2009: Chapter 2.
- Executive Order 13546, Optimizing the Security of Biological Select Agents and Toxins in the United States, July 8, 2010.
  - Federal Experts Security Advisory Panel
    - Recommendations for standards in "cyber-security", November 2, 2010, as amended

Key Points

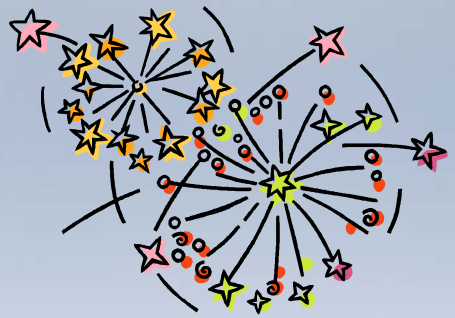
- Information systems control applies to all select agents and toxins.
- Information systems control is found in Section 11- Security.
  - Sections 11(c) and (c)(1) remain unchanged
  - Must be in the site-specific Security Plan
  - Requires written procedures equal to Physical Security and Inventory control
- Information systems control is part of Section 14- Incident Response.
  - Section 14(b) remains unchanged

Key Points

- Information systems control is part of Section 15- Training.
  - Section 15(a) remains unchanged
- Information systems control is part of Section 17- Records.
  - Section 17(b) remains unchanged
- Regulated Community manages the disposition of Biological Select Agent and Toxin (BSAT) information that is under their control.
- Application will vary from entity to entity.
- No “right” or “wrong” on how an entity implements its information systems program.

Previous Rule Provisions

- Section 11(c)- The security plan must:
  - (c)(1)- Describe procedures for physical security, inventory control, and information systems control
- Section 14(b)- The incident response plan must fully describe the entities response procedures for…..security breaches (including information systems);……
- Section 15(a)- …..under this part must provide information and training on biosafety and security *[information systems inclusive]*….
- Section 17(b)- The individual or entity must implement a system to ensure that all records and databases….are accurate, have controlled access……



SECTION 11(c)(9)

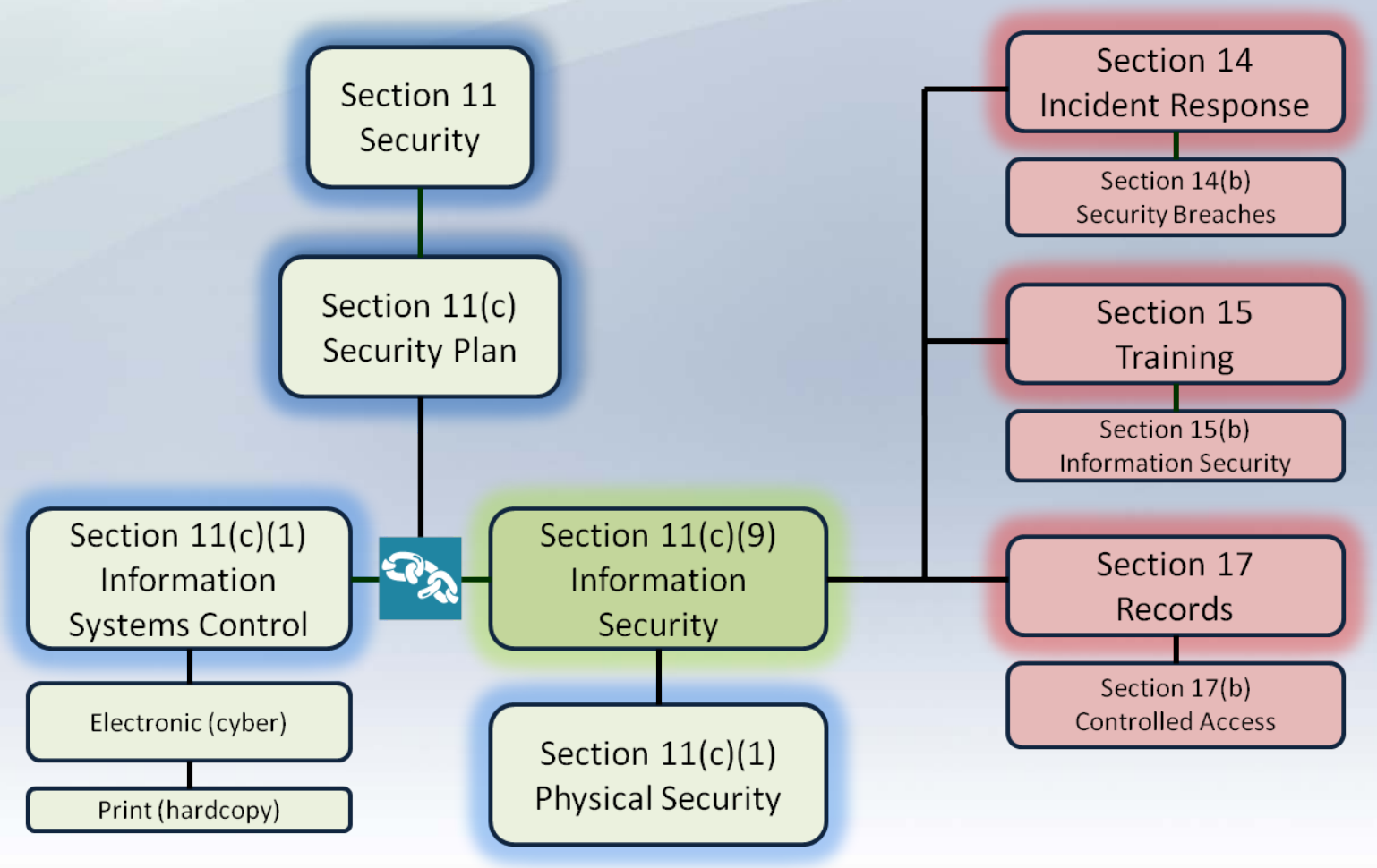
Game Changer

- New Security Plan provision [E.O. 13546].
- Connects "Information Systems Control" with "Information Security".
- Section 11(c)(9)- Contain provisions for information security that:
  - (i) Ensure that all external connections to systems which manage security for registered space are isolated or have controls that permit only authorized and authenticated users;
  - (ii) Ensure that authorized and authenticated users are only granted access to select agent and toxin related information, files, equipment (e.g. servers or mass storage devices), and applications…….;

Game Changer

- (iii) Ensure that controls are in place that are designed to prevent malicious code (such as, but not limited to, computer viruses, worms, spyware) from compromising the confidentiality, integrity, or availability of information systems which manage access to spaces…..;
- (iv) Establish a robust configuration management practice for information systems to include regular patching and updates to operating systems and individual applications;
- (v) Establish procedures that provide back-up security measures in the event that access control systems, surveillance devices, and/or systems that manage the requirements of Section 17 *[records]* are rendered inoperable.

The New Look


Section 11
Security
Section 11(c)
Security Plan
Section 11(c)(1)
Information
Systems Control
Electronic (cyber)
Print (hardcopy)
Section 11(c)(9)
Information
Security
Section 11(c)(1)
Physical Security
Section 14
Incident Response
Section 14(b)
Security Breaches
Section 15
Training
Section 15(b)
Information Security
Section 17
Records
Section 17(b)
Controlled Access

“Cyber-security” or “Information Systems”

- Select Agent and Toxin Regulations.
  - Information systems include:
    - Electronic [cyber]
    - Print [hardcopy application]
- Term “cyber-security” is not used in the regulations.
  - Misleading
  - Accounts for only one means of recording and storing information
- Entity applications.
  - Electronic for everything
  - Strictly hardcopy
  - Combination

What Information Should be Controlled?

- BSAT Information or BSAT Security Information.
- BSAT Information not covered.
  - Research publications; sharing
  - Working laboratory notes or lab books/journals
- BSAT Security Information requiring controlled access:
  - Inventory access logs
  - Passwords
  - Entry/Exit access logs
  - SRA rosters
  - Access control systems
  - Security system infrastructure [floor plans, IDS, guards]
  - Entity Security Plan
  - Entity Incident Response Plan

What Information Should be Controlled?

- BSAT Security Information can be characterized as:
  - Information security
    - Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, recording or destruction of data.
    - Concerned with the *confidentiality*, *integrity*, and *availability* of data regardless of the form [electronic or print].
  - Physical Security for Information Technology (IT) Assets
    - Physically protecting data
    - “Dumpster Diving”
    - Stealing

The Responsible Official- What to Consider?

- Information Security.
  - Confidentiality- Section 11(c)(9)(ii)
    - Who is an authorized individual
    - Not necessarily an SRA approved person
  - Integrity- Section 11(c)(9)(iii)
    - Who has the capability to access and manipulate data
    - IT administrators; PI's; security
  - Availability- Section 11(c)(9)(iv).
    - Are IT systems functioning properly; regular patching and updates
    - File rooms, file cabinets

The Responsible Official- What to Consider?

- Physical Security for Information Technology (IT) Assets.
  - What informational “waste” is being disposed of through normal business activity?
  - Are CD’s; BSAT research notes no longer useful; documents that contain sensitive information, such outdated inventory, SRA rosters, security plans, etc., being properly destroyed.
  - Management and control of physical security access control devices [Section 11(c)(9)(i)/(v)].
    - Who’s responsible?
    - IT information and security usually work on separate platforms

The Responsible Official- What to Consider?

- **Responsible Official Focus:**
  - Network security
  - Hardware/Downloadable devices/Data storage
  - Physical security for IT Assets

The Responsible Official- What to Consider?

- **Network security:**
  - Key Points
    - Networked or stand-alone IT application
    - Organizations with an IT department more than likely provides overall IT support [policy and procedures] to an entity's BSAT program
      - IT departments are designed to support the collective IT systems infrastructure
      - RO should not rely solely on IT department(s) in maintaining information security control for their BSAT program
      - RO should have an IT liaison to ensure that patching and updates are performed

The Responsible Official- What to Consider?

- **Network security:** *[continued]*
  - Key Points *[continued]*
    - Verify who has access rights to select agent databases and security systems
      - SRA may be required if person can gain access to BSAT through manipulation of the IT system.
    - IT departments should understand the sensitivity of the organizations BSAT program
    - Third-party contractor IT support
      - Small to moderate size BSAT entity's
      - Require the same level of attention

The Responsible Official- What to Consider?

- **Hardware/Downloadable Devices/Data Storage**:
  - Key Points
    - Entity should have protocols in place to secure desktop and laptop computers
    - Protocols for safeguarding passwords
    - Servers and mainframes are within controlled space
    - Use of encryption for computers containing BSAT security information for laptops
    - Entity should be wary of the inherent insecurity of iPads, notebooks and similar devices that have information storage and wi-fi capabilities

The Responsible Official- What to Consider?

- **Hardware/Downloadable Devices/Data Storage:** *[continued]*
  - Key Points *[continued]*
    - Have well defined policies and procedures in the entity's overall information systems security control program
    - Downloadable devices can pose an unseen threat
      - Can be hidden from sight, i.e. flash drives
      - Viewed as a non-threat, i.e. BlackBerrys/PDA's
    - Data storage devices that are used for archiving BSAT security information, even on a temporary basis, should be handled and secured as if they were paper hardcopy; i.e., stored in a secured cabinet in a location with appropriate physical security measures

The Responsible Official- What to Consider?

- **Physical Security for IT Assets:**
  - Key Points
    - Entity should place equal importance to physical security and its application to information systems control
      - Especially if servers and mainframes are remotely located
    - Physical security is more about safeguarding information by securing the space where IT devices are used for BSAT activity, including
      - File cabinets
      - Other equipment that maintain BSAT security information

The Responsible Official- What to Consider?

- **Physical Security for IT Assets:** *[continued]*
  - Key Points *[continued]*
    - Physical security IT platforms must meet the confidentiality, integrity and availability criteria as well, because:
      - IT access controlled security systems is an "information" database
    - Physical Security IT Assets requiring management controls
      - Card-key [PINS]
      - CCTV
      - IDS
      - All maintain some level of information storage

The Responsible Official- What to Consider?

- **Physical Security for IT Assets:** *[continued]*
  - Key Points *[continued]*
    - Records retention.
      - No BSAT regulation for CCTV records
      - Select Agent Program recommends 45 days
      - Security records require 3 year retention
    - RO should know who provides physical security for their BSAT program.
      - Entity security department
      - Third party support
      - Liaison

The Responsible Official- What to Consider?

- **Backup Security Measures:**
  - Is a requirement of the new regulations
    - Section 11(c)(9)(v)
    - Access control systems [physical security]
    - Records using IT databases [information security control]
  - Focus is on power outages
    - Alternate power sources, generators, not a requirement of the new regulations
    - Entity needs to determine method of providing backup security. Can take many forms:
      - Uninterrupted Power Source (UPS) with sufficient power to allow for computer shutdowns

The Responsible Official- What to Consider?

- **Backup Security Measures:** *[continued]*
  - Automatic data backup
  - Backup hard-drives
  - Save BSAT security information on CD's
  - Post security guards at critical locations
- Policy and procedures need to be covered in the Security Plan
- Response procedures need to be covered in the Incident Response Plan
  - Disaster Recovery Plan

The Responsible Official- What to Consider?

- **Risk and Incident Management:**
  - Information systems security control
    - Integral with the Security Plan
    - Site-specific
    - Subject to vulnerabilities and threat
      - Should be factored in when developing the overall vulnerability and threat analysis for the BSAT program
      - More likely insider threat
        - Easy access to databases
      - Possible external hacker

The Responsible Official- What to Consider?

- **Risk and Incident Management:** *[continued]*
  - Physical security component is (should) already be covered under the general provisions of Section 11(c)and 11 (d)
  - Information systems are constantly under attack with no obvious trace
  - Well developed incident response and disaster recovery plan
    - Incident Response- Section 14(b)

The Responsible Official- What to Consider?

- **Training:**
  - Entity is required to provide security training to all persons with BSAT access approval
  - Training goes beyond safeguarding BSAT from theft, loss or release.
    - Should have modules for information systems controls
    - Based on site-specific analysis and the entity's application of information management
  - Information systems control training is no different than that provided for security, biosafety and incident response.
    - All require planning, implementation, maintenance and evaluation.

The Responsible Official- What to Consider?

- **Training:** *[continued]*
  - As applied to the BSAT regulations, an information systems control training module should include:
    - Physical security applications
    - Entry access
    - Sharing of unique means of access
    - Inventory control

The Responsible Official- What to Consider?

- **Training:** *[continued]*
  - Information systems control
    - Control of external connections, i.e. who's responsible
    - Only authorized users to information, files and equipment is granted access
    - Controls are in place designed to prevent malicious code [who's responsible]
- Select agent regulations do not make a distinction between IT based information systems application or a paper base [hard-copy] application.

What is a Deficiency?

- No written provisions for Information Security Control in the Security Plan- Section 11(c)(1)
- Elements not covered in Section 11(c)(9)- Information Security based on a site-specific risk assessment
- No provisions for information systems security breaches per Section 14(b)- Incident Response
- No provisions regarding information systems security control in the entity's training program- Section 15(a)
- No defined system to ensure that all records and databases are accurate, have controlled access, and that their authenticity may be verified- Section 17(b).

Review Material and Tools

- Information Systems Security Control Guidance Document
- Updated Security Inspection Checklist with new Information Security criteria

QUESTIONS?

Select Agent Program Workshop

November 2012

For more information, please contact the Select Agent Program

Telephone: 301-851-3300 (APHIS) or 404-718-2000 (CDC)

E-mail: ASAP@aphis.usda.gov (APHIS) or lrsat@cdc.gov (CDC)

Web: www.selectagents.gov

The findings and conclusions in this report are those of the authors and do not necessarily represent the official position of the Select Agent Program.