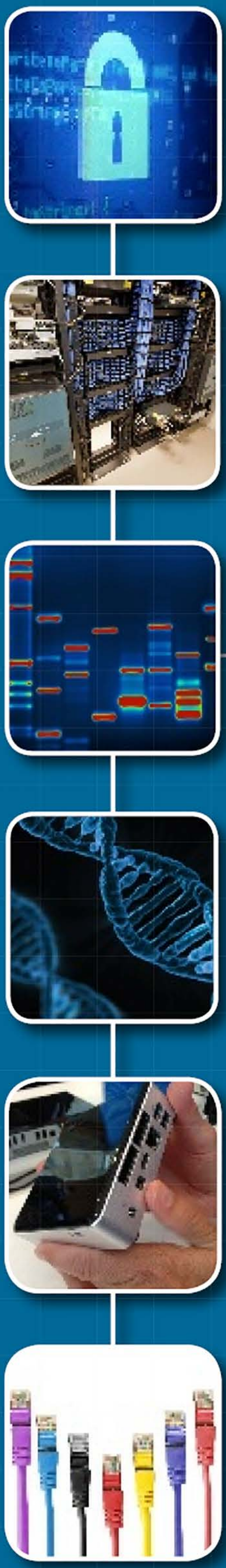

INFORMATION SYSTEMS SECURITY CONTROLS GUIDANCE

42 CFR § 73.11, 7 CFR § 331.11, and 9 CFR § 121.11

MARCH 2017

Centers for Disease
Control and Prevention
Division of Select
Agents and Toxins

Animal and Plant Health
Inspection Service (APHIS)
Division of Agricultural Select
Agents and Toxins

Table of Contents

Changes/Highlights

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

CDC: LRSAT@cdc.gov
APHIS: DASAT@usda.gov

Revision History:
October 12, 2012: Initial posting
February 12, 2014 (Revision 1): The revisions are primarily changes to correct editorial errors from previous version.
May 2017: Revised to accommodate the new language to regulations.

Introduction

The select agent regulations require a registered entity to develop and implement a written security plan that:

- Describes procedures for information system control. (*See* section 11(c)(1))
- Contains provisions for information security (*See* section 11(c)(9))

The purpose of this guidance document is to assist the regulated community in addressing the information systems control and information security provisions of the select agent regulations. The entity must provide the policies and procedures for information system security controls or reference the organizational policies and procedures in the Security plan as required by Section 11 (42 CFR § 73.11, 7 CFR § 331.11, and 9 CFR § 121.11) of the select agent regulations.

BSAT security information includes at a minimum:

- The use of Inventory access logs
- The use of Passwords
- The procedures in place for adhering to the use of Access control systems
- The implementation of Security, Biosafety, and Incident Response plans

Entity record information includes:

- The use and security of entry access logbooks
- Rosters of individuals approved for access to BSAT

Information systems security control is comprised of the processes and practices of technologies designed to protect networks, computers, programs and data from unwanted, and most importantly, deliberate intrusions. Elements of information systems security control include:

- Identifying isolated and networked systems
- Application security

- Information security, including hard copy
- Network security (network and isolated)
- Mitigating insider vulnerabilities
- Incident response
- Training

A complete program should include aspects of what's applicable to BSAT security information and access to BSAT registered space.

Information Systems Security Control

Most entities registered with FSAP have an Information Technology (IT) department that provides the foundation of information systems security. The RO should work with the IT department to ensure that their information systems are compliant with Section 11(c)(9) of the select agent regulations, as well as all other applicable parts of the select agent regulations.

Network Security – Section 11(c)(9)(i)

Section 11(c)(9)(i) requires the registered entity to "ensure that all external connections to systems which manage security for the registered space are isolated or have controls that permit only authorized and authenticated users." There are several methods for securing the network from intrusion. The entity should work with the IT department to ensure that specific provisions are in place for registered spaces. The entity may use one or more of the following to meet the requirements:

Logical Network Separation

Logical network separation means that all of the end points (computers, servers, etc.) are contained within the same local area network.

- Wireless Network – A computer network not connected by cables of any kind to create secure connection between different equipment locations.
- Segregated Network – A network of computers that is split into subnetworks to contain a local network and is not visible from the outside.
- Encrypted VPN (Virtual Private Network) – A web of computers that are linked together and able to share files and resources that is encrypted so that they can access the internet without compromising security.
- LAN (Local Area Network) or VLAN (Virtual Local Area Network) – A broadcast domain within a switched network. Devices in this network setup can communicate with one another without a router.

Physical Network Separation

A physically separated network is not connected to the internet and is physically isolated by purpose-built hardware and software security barriers.

Access Authentication – Section 11(c)(9)(ii)

Section 11(c)(9)(ii) requires the entity to "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 as necessary to fulfill their roles and responsibilities, and that access is modified when the user's roles and responsibilities change or when their access to select agents and toxins is suspended or revoked."

The entity must ensure that:

- Only authenticated users are granted access to BSAT related information.
- Authenticated and authorized users only have access to BSAT related information that is specifically related to the work that they do.
- All BSAT related information and information storage (files, computers, hard drives, and other storage devices) are accessible only by authenticated and authorized users.
- Access is modified in in the event that a user's role changes or when access to BSAT is suspended or revoked.

Things that generally meet these requirement include:

- Domain passwords (Microsoft login)
- Work station passwords
- Two-factor identification (CAC/PIV + __)
- Fingerprint or other biometric security features

Application Systems Security Controls – Section 11(c)(9)(iii)

Countermeasures taken regarding application security ensure security of software, hardware, and procedural methods to protect systems from external threats. For example, the most basic software countermeasure is a firewall that limits the execution of files by specific installed programs. Similarly, the router is a hardware countermeasure that can prevent the IP address of an individual computer from being visible on the internet. Other countermeasures include encryption, antivirus programs, spyware detection, and biometric authentication systems.

Section 11(c)(9)(iii) requires the entity to "ensure that controls are in place that are designed to prevent malicious code (such as, but not limited to, computer virus, worms, spyware) from compromising the confidentiality, integrity, or availability of information systems which manage access to spaces registered under this part or records in §73.17."

Antivirus

Antivirus software detects and removes computer viruses and other types of malware including:

- Browser hijackers
- Ransomware
- Key loggers
- Backdoors
- Rootkits
- Trojan horses
- Worms
- Adware
- Spyware

Commonly available antivirus software like McAfee, Semantic, and Avira are typically sufficient for most registered entities, though more robust systems may be required. Consult the IT department to ensure a robust antivirus system has been installed and implemented throughout the network.

Firewalls

The most common way to meet this requirement is to set up a firewall at some level of the network (computer, department, institution, etc.). Typically, Microsoft's firewall is enough to meet the SAR requirements. There are several types of firewalls that can meet this requirement. Work with the IT department to determine the best solution for the entity's specific network conditions. Some examples include:

- Packet Filtering Firewalls – monitor outgoing and incoming information based on the source and destination.
- Stateful Inspection Firewalls – monitor active network connections to determine what network packets are allowed through.
- Application-Proxy Gateway Firewalls – run a firewall system between network and proxy that acts as a gateway for packets to get through to the network.

Patching – Section 11(c)(9)(iv)

Section 11(c)(9)(iv) of the regulations require the entity to "establish a robust configuration management practice for information systems to include regular patching and updates made to operating systems and individual applications."

Patching is the process of installing pieces of software designed to update an existing program. These are often used to fix security vulnerabilities.

Microsoft updates typically occur overnight on Tuesdays. The following day is often called "Exploit Wednesday" because this is when systems are most likely to experience vulnerabilities. Thus, the IT department should push these regular updates on Wednesday after vulnerabilities have already been addressed to minimize security vulnerabilities.

Backups – Section 11(c)(9)(v)

Section 11(c)(9)(v) of the select agent regulations require the entity to "establish procedures that provide backup security measures in the event that access control systems, surveillance devices, and/or systems that manage the requirements of section 17 of this part are rendered inoperable."

Events such as security breaches, natural disasters, or equipment failure can sometimes result in systems or machines becoming inoperable. The entity is still responsible for any information that may get lost, so a backup system must be in place for the purposes of disaster recovery. There are many backup systems that will restore data after a data loss event. The IT department may set up an imaging system, an incremental style repository, a differential backup, a continuous data protection, among other solutions. The best solution depends on the size and nature of the entity and the IT department that manages the backup system.

Hardware/Downloadable Devices (Peripherals)/Data storage

The entity must ensure that proper protocols are in place to secure such devices (such as docking stations for laptops), re-emphasizing login/logout practices and safeguarding passwords. For example, if a PI uses a laptop between workstations or worksites which contain any elements of BSAT security information, the PI must follow proper laptop security procedures. Such protocols may include:

- Computers should be located within controlled space since the room will already have some level of physical security.
- Users should physically secure the device and password/encrypt the laptop if it contains BSAT security information of any kind. This practice should be extended to desktops if a PI has an office outside the BSAT registered space.
- An entity should be wary of the inherent insecurity of tablet devices that have information storage and Wi-Fi capabilities, especially if they cannot be encrypted.

The development of well-defined policies and procedures should be considered in the entity's overall information systems security control program.

Peripheral devices

Entities should include peripheral devices as a part of the overall information systems security control if they are used to process information required by Section 17 of the select agent rule. These devices include, but are not limited to:

- Smartphones
- USB devices (e.g. flash drives)
- USB patch cords with mini/micro connectors
- Electronic notebooks
- BlackBerrys
- PDA's
- Future technological development

Any device which can be hidden from sight or viewed as a non-threat (smartphones, flash drives, etc.) poses a security vulnerability to information systems security. The regulated community may want to include these types of devices in their information systems security protocols, or, at a minimum, include them in their information security systems training program. Risks involving peripheral devices could include but are not limited to:

- A flash drive to download BSAT security information.
- Uploaded malicious code designed to corrupt BSAT data or computer systems.
- If the network is isolated but the USB drive touches the internet, it can transmit a virus and that risk must be addressed.

Section 11(d)(7)(ii) of the select agent regulations requires procedures for reporting suspicious persons or activities. This provision is not limited to physical security and should be applied to information systems security as well.

Data storage

A data storage device is any device used for recording (storing) information (data). The entity should have written policies regarding the storage of BSAT information on media that can be removed and stored separately from the recording device such as:

- Computer disks
- CD-Rs
- Flash drives
- Memory cards

If the entity uses these means of archiving, even on a temporary basis, they should be handled and secured as if they were a paper hardcopy (i.e., stored in a secured cabinet and in a location with the appropriate physical security measures in place). Items such as these are easily concealed and could get past institution physical security.

Industrial Control Systems

An industrial control system (ICS) consists of combinations of control components like electrical, mechanical, hydraulic, and pneumatic devices that act together to achieve an industrial objective. ICS may be fully automated or may incorporate human input into the processes that the systems carry out.

Advances in technology have led to many improvements to such systems that make them perform better and more cost-efficiently. The systems are as a result safer and more reliable than ever. However, the more reliant that entities are on the functionality of these systems, the more critical it is that they ensure each system has provisions in place to ensure safety and security.

The entity must ensure that these systems are secured against intentional or unintentional interference that could impact the safety and security of BSAT through malfunction or failure of an ICS. Work with the IT department and facility departments to put provisions place to protect the entity's ICS. An ICS security management system must be a part of the information system security control plan. The plan should directly address systems like:

- Power
- Water
- Water Waste
- HVAC
- Transportation

The ICS should function inside the network and be protected by the same antivirus and firewall systems in place for the entity's computers, servers, and other equipment.

ICS Security Program Development

Incidents that impact the ICS are likely to have a physical impact (e.g. an attack on the HVAC system may shut down the air filtration system), even if the incident is the result of a virtual attack. The Information System Security Control plan should fully describe provisions put in place to mitigate virtual and physical risks to the ICS. Follow the following steps to develop the ICS component of the Information System Security Control plan.

1. Build a cross-functional team of subject matter experts.
2. Perform a risk assessment specifically for the entity's ICS. Identify risks and vulnerabilities to the system. Determine the likelihood and consequence of those risks to determine the threat level.
3. Define and fully describe policies and procedures to mitigate the risks determined in the risk assessment. These provisions should focus on preventing threats and vulnerabilities to the ICS from occurring.
4. Implement the ICS security policies and procedures.
5. Provide policy and security awareness training for ICS staff.
6. Describe how the entity will patch and update their ICS.

Appendix: Information Security Checklist

The information found in the appendix consists of information that an entity may consider in development and implementation of entity's security plan. The user is not required to use, or limited to, the information provided in the appendix.

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

Security Patch Mgt. Procedures • Yes • No

B. Hardware Assets Protection

Main Computer Room Locked • Yes • No

Laboratory Protection • Yes • No

Wiring/Cable Closet Protection • Yes • No

Restricted Access Protection • 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
Personnel Records Secured	• Yes • No
Information Security Manager	• Yes • No
Security Policy/Procedures	• Yes • No

D. Data Protection

Select Agent or Toxin Inventories

Record Secured	• Yes • No
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

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 select agent regulations for information systems control. The purpose of this document is to determine what the entity has in place.

Additional Remarks:

____

____

____

____

____

____

____

____

____

____