

Information Systems Security Control Guidance Document

7 CFR Part 331, 9 CFR Part 121, 42 CFR Part 73

February 12, 2014

**Animal and Plant Health Inspection Service (APHIS)
Agricultural Select Agent Services
Centers for Disease Control and Prevention (CDC)
Division of Select Agents**

Preface

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

CDC: LRSAT@cdc.gov

APHIS: ASAP@aphis.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.

Table of Contents

Introduction 5

Information Technology (IT) Security Overview 10

Network Security 11

Hardware/Downloadable Devices (Peripherals)/Data storage 13

Physical Security for IT Assets 15

Backup Security Measures 18

Risk Management and Computer Security Incident Management 20

Training 22

References 25

Appendix: Information Security Checklist..... 26

Introduction

Section 201 of the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188) (the Act)*, requires the Secretary of the Department of Health and Human Services (HHS) to, by regulation, provide for “the appropriate safeguard and security requirements for persons possessing, using or transferring a listed agent or toxin commensurate with the risk such agent or toxin poses to public health and safety including the risk of use in domestic or international terrorism”.¹ Section 212 of the Act requires the Secretary of the Department of Agriculture (USDA) to, by regulation, provide for “the appropriate safeguard and security requirements for persons possessing, using, or transferring a listed agent or toxin commensurate with the risk such agent or toxin poses to animal and plant health, and animal and plant products including the risk of use in domestic or international terrorism.”²

The select agent regulations require a registered entity to develop and implement a written security plan that (1) describes procedures for information system control, and (2) contains provisions for information security (*See sections 11(c)(1) and (c)(9) of the select agent regulations*).³

The regulated community should consider asking:

- a) Who should have access to my biological select agent and toxin (BSAT) security information?
- b) What do I need to do to ensure that BSAT security information is safeguarded?
- c) What do I need to do to ensure that BSAT security information is used for the intended purpose?
- d) What level of physical security do I need to protect BSAT security information?

BSAT security information includes at a minimum:

- a) Inventory access logs
- b) Passwords
- c) Entry access logbooks
- d) Rosters of individuals approved for access to BSAT
- e) Access control systems
- f) Security system infrastructure, including floor plans, on-site guard, CCTV, intrusion detection systems, etc.
- g) Security Plans
- h) Incident Response Plans

¹ Section 351A(e)(1) of the Public Health Service Act (42 USC 262a(e)(1)).

² Section 212(e)(1) of the Agriculture Bioterrorism Protection Act of 2002 (7 USC 8401).

³ For purposes of this document, section 11 refers to section 11 (Security) of 7 CFR part 331, 9 CFR part 121, and 42 CFR part 73.

Since the regulated community is in control of their information, each of these questions will pose a different approach because no two institutions are the same. The first step is to decide what and how much BSAT security information you are willing to make available to personnel inside and/or outside of your organization. Entities should treat information systems security with equal respect to that of physical security. A complete program should include aspects of what's applicable to BSAT security information and access to BSAT registered space.

The protection of BSAT security information is an important component in the prevention of the misuse, either accidentally or intentionally, of BSAT.⁴ The Federal Select Agent Program⁵ has established regulatory language to ensure that information related to BSAT is safeguarded and access to that information is limited to authorized and authenticated users. The select agent regulations that address information systems control are located in section 11(c)(1);section 11(c)(9) specifically states that an entity's security plan must contain provisions for information security that:

- a) Ensure that all external connections to systems which manage security for the registered space are isolated or have controls that permit and monitor only authorized and authenticated users (11(c)(9)(i));
- b) 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 (11(c)(9)(ii));
- c) Ensure that controls are in place that are designed to prevent malicious code (e.g., computer viruses, worms, and spyware) from compromising the confidentiality, integrity, or availability of information systems which manage access to registered spaces in section 11 or records in section 17 (11(c)(9)(iii));
- d) Establish a robust configuration management practice for information systems to include regular patching and updates made to operating systems and individual applications (11(c)(9)(iv)); and
- e) 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 are rendered inoperable (11(c)(9)(v)).

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

⁴ Biosafety in Microbiological and Biomedical Laboratories, 5th Edition, Section VI- Principles of Laboratory Biosecurity, page 111, December 2009.

⁵ The Federal Select Agent Program is the coordinated implementation of the select agent and toxin regulations by the USDA/Animal and Plant Health Inspection Service/Agricultural Select Agent Program, and the HHS/Centers for Disease Control and Prevention/Division of Select Agents and Toxins.

regulations.⁶ The application of this guidance document applies to entities that possess, use or transfer all BSAT's.

Cyber-security is the processes and practices of technologies designed to protect networks, computers, programs and data from unwanted, and most importantly, deliberate intrusions. Elements of cyber-security include:

- a) Application security
- b) Information security
- c) Network security
- d) Incident response
- e) Training

For the purpose of this guidance document "*information systems security control*" will be used instead of cyber-security, because information related to BSAT is not limited to electronic applications. Within the regulated community, BSAT security information is stored in electronic and hard copy media. Whatever approach an entity chooses regarding the management of their BSAT-related security information, the processes must be integrated into the entity's written security plans.⁷

Actions taken regarding application security, sometimes referred to as countermeasures, are used to ensure security of software, hardware and procedural methods to protect systems from external threats. For example, the most basic software countermeasure is the 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, anti-virus programs, spyware detection and biometric authentication systems.

The regulated community must take a broad view on how to safeguard information beyond the "cyber" world. Safeguarding BSAT security information can take many forms, but generally can be characterized in two ways:

- a) Information security
- b) Physical security for Information Technology (IT) assets

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, recording or destruction of data. Information security is concerned with the *confidentiality, integrity* and *availability* of data regardless of the form (i.e., electronic (cyber) or print (hardcopy)). In this day and age, information security is usually directed toward the cyber world with less emphasis on

⁶ 7 CFR 331.11(c)(1), (d)(7)(v) and (c)(9), 9 CFR 121.11(c)(1), (d)(7)(v), and (c)(9) and 42 CFR 73.11(c)(1), (d)(7)(v) and (c)(9).

⁷ Section 11(c)(1)

printed material. Nevertheless, the safeguarding of this information, whatever the medium is critical in protecting BSAT from misuse.

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. Each entity should consider assessing who is an authorized individual within the scope of the regulations, inside and outside the institution, and determine whether the system(s) used for the conveyance of legitimate research has adequate controls in place (11(c)(9)(ii)).

Integrity means that data cannot be modified undetectably. Section 11(d)(7)(v) requires the reporting to the Responsible Official (RO) of any sign that inventory or use records for BSAT have been altered or otherwise compromised. The regulated community should consider factoring in who has the ability and capability of accessing and manipulating the data (11(c)(9)(iii)). This could be a systems administrator with access rights to the entire network, or a support technician assigned to the entity's select agent program. It could be as simple as a Principal Investigator (PI) keeping his/her records on a non-networked computer.

Availability, for the purpose of this guidance document, is research information that must be available when needed. This means that the computing systems used to store and process information, the security controls used to protect it, and the communication channels used to access it must be functioning properly. This includes the application of strong passwords, firewalls, anti-virus software and regular patching and updates to operating systems. For availability to be successful these applications must be functioning properly with on-going maintenance (11(c)(9)(iv)).

Physical security for IT assets means physically protecting data and means to access data apart from protecting it electronically. Examples of physical attacks include "dumpster diving" to search for improperly discarded sensitive information and deliberate document stealing.

The regulated community should consider maintaining awareness of what informational "waste" is being disposed of through normal business activity in and around their BSAT registered space. Responsible individuals should ensure that items like computer disks, BSAT research notes that are no longer useful, and documents that contain sensitive information, or other computer hardware are properly destroyed before being discarded. On the more extreme side, the simple act of stealing the information by unauthorized people, inside or outside the organization, should be factored into an entity's information systems security control policies and procedures. This is equally important where hardcopy BSAT security information is stored in a PI's office that is not inside the BSAT registered space. Physical security for IT assets can be easily added to an entity's written security plan as required in sections 11(c)(1) and 17(b) (Records) of the select agent regulations.

Some common practices that the regulated community can adopt, or re-emphasize during information security training, are:

- a) the destruction, such as shredding, of paper documents and computer disks; and,
- b) purging electronic storage media before disposal.

If the entity is unclear on how to do this or does not have the means, then the RO should consider contacting their IT department or leadership for assistance. Proper access control to BSAT registered space⁸ can mitigate the threat of information theft by ensuring that only authorized individuals can enter the space, or that escort procedures are implemented for those that are not authorized.

In summary, information systems control as required by section 11 of the select agent regulations includes both BSAT security information and the physical infrastructure provided to protect this information. This also extends to discouraging sharing an individual's unique means of accessing BSAT such as passwords, as required in section 11(d)(6).

⁸ Sections 11(d)(1) and (d)(2)

Information Technology (IT) Security Overview

IT is a collection of computer hardware/software, information systems, and programming languages. The regulated community uses IT in a wide variety of applications such as:

- a) Storing personnel security risk assessment information;
- b) Storing BSAT research information and inventory records;
- c) Management and control of physical security access control and monitoring devices.

Essentially, the computer is the central node that makes everything work. As such, IT has its own uniqueness in that threats to these systems are far less obvious, and perhaps ignored through complacency or viewed as a nuisance.⁹ Unlike securing (physical) BSAT registered space and the building in which they are located, IT security requires constant systems monitoring. As such, both IT security and physical security are important.

An entity's IT security should focus on:

- a) Network security
- b) Hardware/Downloadable devices/Data storage
- c) Physical security

⁹ National Institute of Standards and Technology, Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST 800-14, September 1996.

Network Security

Large and small institutions have some level of IT infrastructure. These range from large and/or complex organizations with robust systems and support to smaller and more focused organizations that use a closed (isolated) network or stand alone system requiring, in some cases, external contracted support to maintain them. The regulated community with robust systems and support should not rely solely on their IT departments in maintaining information security control for their BSAT program. For entities with BSAT security information incorporated as part of an organization's overall IT infrastructure, this information and supporting infrastructure is subject to the overall IT policies and procedures of the organization. IT departments are designed to support the collective IT systems infrastructure and not necessarily to the specific entity's BSAT program, albeit located somewhere in the systems infrastructure. For these large organizational units, the RO should consider ensuring that their IT departments are performing regular patching and updates to operating systems and individual applications (11(c)(9)(iv)). This should also include the IT department's systems administrator who has complete access rights, or a designated systems administrator or support technician with specific access rights to BSAT security information are authorized or authenticated (11(c)(9)(ii)). While there is no regulatory requirement for an entire IT system support staff to be approved for access to BSAT, the RO needs assurances from their IT departments that those individuals understand the sensitivity of the information associated with their BSAT activity. A possible solution to this is to designate a liaison between the entity BSAT program and the IT department.

Effective IT security should be considered to include procedures, such as, but not limited to:

- a) Authenticating the user (one-factor authentication (i.e., username and strong password))
- b) Enhanced background screening for primary systems administrator or equivalent
- c) Network firewalls
- d) Anti-virus software or intrusion prevention system¹⁰
- e) Internet security software package
- f) Encryption between hosts
- g) Secured zone (where the computers and servers are housed such as LAN closets, computer rooms)

One of the most complex decisions that an RO faces with respect to staff providing support to an entity's BSAT-related security information systems is: "Should these individuals have an FBI security risk assessment?" In considering this issue, the RO should remember that the FBI security risk assessment is required for those individuals with unescorted access to the BSAT, not to BSAT information *per se*. If the BSAT access control system at an entity is

¹⁰ Not to be confused with building security intrusion detection system.

designed so that an IT support person would be able to gain access to BSAT through manipulation of the IT system, then these individuals should be submitted for approval to access BSAT and undergo a security risk assessment.

Information security can be more challenging to achieve at small and (perhaps) moderately sized BSAT entities because they may not have a robust security infrastructure and support network. Nonetheless, these entities must establish policies and procedures that are structured to meet their IT security needs.¹¹ These types of entities may use a simple stand-alone computer located within the BSAT registered space, use a limited networked system such as a local area network (LAN) with no internet connectivity, or an intra-net application for such use as a wide area network (WAN). Each configuration comes with risks, and, as such, requires an equivalent level of IT security for safeguarding BSAT information. For example, if a moderately sized entity has more than one research function (i.e., both non-BSAT and BSAT) and uses a local area network with a common file sharing or mainframe server, the entity should consider strong IT security protocols such that isolation (firewall, domains) of the BSAT security information from the non-BSAT information and other administrative access rights is achieved. Small organizations may not have in-house support people to service and maintain their IT infrastructure. If there is a third-party support unit for IT, the RO should consider having in place policies and procedures to address how the support is provided, under what conditions, and the extent of access to the operating systems and data (11(c)(9)(ii)). The BSAT regulation provides two means of accessing registered space 1) SRA-approved individuals, and 2) escorted individuals.¹² The entity will need to determine the best approach that will meet their IT needs.

ROs for the small and moderately sized entities should consider having clear written protocols to include the following IT security features:

- a) Strong log-on password(s) with expiration dates
- b) Firewall or unified threat management system
- c) Anti-virus software
- d) Discourage unsecured wireless connection or limit use
- e) Use a Virtual Private Network (VPN) to communicate between several offices, if applicable
- f) Use of reputable bonded third party IT support services should be considered.
- g) Secured zone (where the computers and servers are housed such as LAN closets, computer rooms)

¹¹ Sections 11(c)(1) and (c)(9).

¹² Sections.11(d)(1) and (d)(2).

Hardware/Downloadable Devices (Peripherals)/Data storage

Hardware. As part of computer security, and for the purpose of this guidance document, hardware is being referred to as the computer (e.g., desktops and laptops); their internal operating systems (hard drive); monitor; and tablet devices that have BSAT security information. It is important to the entity 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, proper handling of the laptop would be paramount. It's desirable that computers be located within controlled space since the room will already have some level of physical security. If laptops are used, 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. As part of the overall information systems security control there are peripheral devices to which the regulated community should pay attention. These peripheral devices can pose an unseen threat (insider/third party threat).

These devices include, but are not limited to:

- a) USB devices (commonly referred to as flash/thumb drives)
- b) USB patch cords with mini/micro connectors
- c) Electronic notebooks
- d) BlackBerrys
- e) PDA's
- f) Future technological development

Any devices, which can be hidden from sight or viewed as a non-threat (BlackBerrys, PDAs, etc.) pose 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. For example, a disgruntled employee could use a flash drive to download BSAT security information or even upload a malicious code designed to corrupt BSAT data or computer systems. Awareness is the operative word. Section 11(d)(7)(ii) 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 a device for recording (storing) information (data). A concern for the regulated community would be the storage of BSAT information on media that can be removed and stored separately from the recording device on, such as computer

disks, CD-Rs, flash drives, memory cards, etc. component for the purpose of archiving or maintaining a data library or personal files. If an entity utilizes 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 security.

Physical Security for IT Assets

There is a perception that there is no relationship between physical security and information systems security as not having the same level of importance or even relevant to safeguarding BSAT security information. This perception may be seen as physical security, as well as information security, is outside the control of the research activity only because “someone else is taking care of it.” On the contrary, IT systems that are designed to safeguard information and physical security of BSAT at an entity require the same level of attention by both the service provider and the RO.

If there is an “insurance plan” for information systems security control, it would be “physical security”. The regulated community should consider looking at both information systems security and physical security in order to have a complete information security program. Information security utilizes an array of software to secure data and to prevent unwanted intrusions. The physical security side is designed to augment what information security cannot do and is within the control of the entity’s RO to implement. These are:

- a) Ensure that only personnel authorized by the entity have access (this could and should include a systems administrator for IT and security services),
- b) Confirm that servers and mainframe systems that support BSAT information are in a secured location if not within the BSAT registered space,
- c) Ensure authorized user unique access to secured locations is not shared,
- d) Use of screens (sometimes referred to as anti-glare screens) to restrict viewing of computer monitors,
- e) Conduct periodic review of entry access journals and/or entry logbooks to verify that only authorized personnel are accessing space where computer systems are used (including BSAT registered space),
- f) Ensure that hardcopy records and computer discs that are no longer useful are properly destroyed; preferably by shredding.

The entity should place equal importance on physical security, especially if the computer system servers and mainframes are located elsewhere in the facility or at a remote location. It is understood that an RO may not have control over this, but an RO can engage their IT departments to get clarity on how well these areas are secured and monitored. This is also an opportunity for the RO to explain to the IT systems administrator the sensitivity of the BSAT program and the requirements of the regulations that are to be met.

Physical Security Access Controls, CCTV and Intrusion Detection Systems. Security access controls (e.g., card-key, biometric, etc.) generally operate on a separate security IT platform. The majority of these systems are isolated from other information systems and databases and not connected to the internet. There may be some intranet applications where a single platform serves multiple buildings, or rooms within a single building, which is controlled and managed at a central location. Even these are isolated from each other by

the access coding of the card-key. However, like BSAT, IT information systems and databases, IT controlled security systems is an “information” database that the regulated community cannot ignore. Card-keys come in two forms: 1) a card-key that simply has the institutional logo or other graphics and is issued with an ID card; and 2) card-keys that are used as a photo-ID badge or combined with bio-metrics. Both may have personally identifiable information (PII). IT controlled security systems are designed to record entry (or exit) activity. Card-keys can contain the following information, but not limited to:

- a) control number
- b) name of the individual in possession of the card-key
- c) entry/exit rights to certain spaces, floors and doors
- d) assigned department
- e) security clearance level, if applicable

As with the IT departments, the RO should consider engaging the organization’s security department, or security service provider, to work out any physical security requirements for the BSAT registered space and establish protocols to ensure that the entity’s BSAT program is safeguarded. Physical security IT platforms must meet the *confidentiality*, *integrity* and *availability* criteria as well. Such discussions should include:

- a) Establishing a liaison between the security department/service provider and entity BSAT program.
- b) Is the security server/mainframe in a secured space with restricted access?
- c) Are security equipment closets secured with restricted access?
- d) How is stored/archived information protected?
- e) Who has access to the information?
- f) Do doors that access BSAT registered space “fail-secure” in the event of power loss?
- g) Are card-keys promptly inactivated when there are staff changes in the BSAT program?
- h) Establish protocols/agreements for routine review of entry access journals to registered BSAT space.

Much of the above is directed towards safeguarding information regarding individuals that are approved for access to BSAT and securing the space where IT devices such as desktop and laptop computers are used for BSAT activity; as well as file cabinets and other equipment that maintain BSAT security information. Protection of physical security information relies heavily on controlling entry access to the registered space.

Closed Circuit Television (CCTV) and CCTV surveillance. Some registered entities use CCTV as simple recording (informational) devices that are not monitored, but record activity in and around BSAT areas. They are usually reviewed periodically by the organization’s BSAT leadership or when there is a discovery of an incident. CCTV surveillance is a monitored, usually 24/7, application. Monitoring is performed by a trained security staff or a security service provider. More than likely the regulated community has no direct responsibility for maintaining CCTV systems, therefore an RO needs to be wary of the information being

recorded and the retention of archived information. If an entity's security staff, or CCTV support provider, is responsible for maintaining video records, the RO should work out a retention period and a security storage plan for the archived video media for the registered spaces that are being monitored. Retention of video records is not a provision of section 17(c) of the select agent regulations which require 3 year retention. However, the Federal Select Agent Program recommends a 45 day retention period for these video records. At the end of the retention period the data storage media could be destroyed.

Intrusion Detection System (IDS). As the name implies, an intrusion detection system (IDS) detects; it can also record data (information) regarding access to the BSAT registered space whether it's a single room or an entire building. An IDS for building security should not be confused with an IDS for IT systems. An IDS for building security uses an array of devices such as motion sensors, glass-break sensors and infrared sensors. In physical security, an IDS is designed as a component of a security access control system (card-key, biometrics, etc.) or stand alone as a single system for the sole purpose of monitoring access entry points or areas of buildings with vulnerabilities, such as windows, to alert a security response force. An IDS for an IT system is sometimes referred to as an intrusion prevention system (IPS) where they use anti-virus software to inhibit the action of malware. The data collected by an IDS can provide useful information to the RO when resolving incidents of unauthorized access. Handling of the data should mirror the management of data collected by a CCTV system.

Backup Security Measures

Backup security measures need to be in place for both information security control and physical security associated with the entity's BSAT program.¹³ This is to ensure that integrity is maintained for the information and physical security systems of the entity's BSAT program.

Backup security measures can take many forms, depending on the size and mission of the organization. For example, large organizations, in most cases, have backup power generators to support critical infrastructure such as IT based security and information systems. Having a backup power generator can solve many issues in maintaining the integrity of critical systems.

Unfortunately, not all registered entities have the luxury of power generators, nor do the regulations require entities to install one to satisfy the requirements of section 11 (c)(9)(v). This does not mean that these entities have no recourse. An RO should have alternate plans in place to mitigate the problem, such as posting guards, roving security patrols or ensuring that the access control system has a "fail-secure" feature during the period of lost power. For example, an entity that has an access control system, with no connections to an existing alternate power source, should make sure that all doors within the BSAT activity area "fail-secure." This provides an immediate lock-down of the space without sacrificing the safety of individuals in the laboratory. In the absence of a "fail-secure" system the entity should establish procedures to prevent unauthorized access until power is restored. If the RO is unsure whether their space has a "fail-secure" system, then the RO should have a discussion with their security department or security service provider to determine how the access control system functions during a power outage.

Similar precautions can be implemented for information security. For those organizations that do not have an alternate power source, the entity should consider or verify the following:

- a) BSAT security information is automatically backed up according to a predetermined schedule and the backup process should be periodically checked to ensure that the data is backed up properly.
- b) Provide backup hard-drives to critical BSAT security information systems,
- c) Use of an Uninterruptible Power Source (UPS) with sufficient power to allow for the manual saving of data and computer shutdown,
- d) BSAT laboratorians periodically save information while actively engaged in entering information into database(s),
- e) Save BSAT security information on portable media where the files are password protected and secure portable media in a lockable file cabinet,

¹³ Section 11(c)(9)(v).

- f) File cabinets that contain BSAT information should be secured in the BSAT registered space or the duty office of the laboratorian with restricted entry access.

Whatever backup security measures the entity implements, the policies and procedures need to be written into the entity's security plan as required in section 11(c)(1). Any and all computer security incident management procedures should be incorporated into the entity's written incident response plan as required in section 14 (Incident Response) of the select agent regulations which should specifically include a disaster recovery plan for BSAT security information.

Risk Management and Computer Security Incident Management

Risk Management. Information systems control is primarily linked as a component of the entity's site-specific written security plan.¹⁴ More specifically, how the entity develops its policies and procedures in safeguarding its information from unwanted intrusions must be designed according to a site-specific risk assessment.¹⁵ This would include evaluating the vulnerabilities and threats that could be directed at the entity's information systems, whether network based or stand-alone. The physical security component of information systems security control is already covered when the entity evaluated its vulnerabilities and threats towards safeguarding BSAT from theft, loss or release.^{16,17} However, unlike physical security, information systems may be attacked without any visible trace and the RO needs assurances from their IT departments or service providers that intrusion inhibitors are fully functioning.

BSAT programs associated with large institutions with a robust IT infrastructure should have thoroughly evaluated the vulnerabilities and threats to the overall information systems network and incorporated the necessary intrusion inhibitors. It's important for the RO to work with the IT department systems administrator in understanding the particular sensitivities of the BSAT program. Smaller and moderate size organizations may not have this level of support. In this case, an RO may need to work more closely with their service provider to ensure the maximum level of protection is in place to address vulnerabilities and threats.

Similar to assessing the physical security threats and vulnerabilities, information systems security can follow the same concepts by evaluating through consequence assessment, and threat/vulnerability assessment.¹⁸ Once a thorough risk assessment has been performed by the RO and subject matter experts from the IT and security departments, the RO should consider following through with:

- a) Determining the risk
- b) Communicating the risk
- c) Managing the risk

Determining the risk: What is subject to a threat?

- a) The network
- b) The computer
- c) The BSAT security information

¹⁴ Section 11(c)(1).

¹⁵ Sections 11(b) and 17(b).

¹⁶ Section 11(a).

¹⁷ See "Security Guidance for Select Agent or Toxin Facilities" available at: <http://www.selectagents.gov>.

¹⁸ See "Security Guidance for Select Agent or Toxin Facilities" available at: <http://www.selectagents.gov>.

Communicating the risk: Key entity leadership should determine if the current risk is acceptable by considering who should have access to the BSAT information and information system control databases.

Managing the risk: Are the intrusion inhibitors offered by the service providers sufficient to safeguard the entity's BSAT information? Do I have a disaster recovery or back up plan in the event of a successful intrusion or uncontrolled emergency?

Computer Security Incident Management. The National Institute of Standards and Technology (NIST) describes a computer security incident as “resulting from a computer virus, other malicious code, or a system intruder, either an insider or an outsider”.¹⁹ Similar to responding to natural disaster incidents, computer security incident management requires a process and a team to follow the process. More than likely, the team that is formed for managing an incident for the theft, loss or release of a BSAT will be the same for an incident involving information systems related to security and BSAT. The new player would be an individual well versed in information systems technology and security.

In the event of an incident caused by an attack, the entity should have response procedures in place to recognize an event. Some attacks are detected by a sensor, a network analyst or a user reporting something unusual with the computer. Containment is critical for stopping malicious network traffic or a computer virus, the spread of which could be terminated by taking the computer(s) off-line. Cleaning of the system should be monitored by the RO, or designee, if the IT department or service provider performs these functions. This would include ensuring the destruction of any hard drives that still maintain BSAT security information including inventory records.

¹⁹ National Institute of Standards and Technology, Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST 800-14, September 1996.

Training

Each registered entity is required to provide security training to all individuals with BSAT access approval.²⁰ Security training goes beyond safeguarding BSAT from theft, loss or release and should include modules for information systems control. With the varying degree of registered entities, large and small, with research from diagnostic to commercial, information security training amounts to computer security awareness.²¹ This is no different than the training that is required for security, biosafety and incident response. In each of these applications the training includes proper planning, implementation, maintenance, and evaluation:²²

The following BSAT regulatory requirements regarding information systems security control should be included in the overall entity training program:

- a) Physical security
- b) Entry access
- c) Sharing of unique means of access
 - 1) Reporting of loss or compromise of passwords
 - 2) Reporting of suspicious person or activities
- d) Inventory control (i.e., alteration or compromise of inventory records)
- e) Information systems control
 - 1) Control of external connections to facility security systems (who's responsible)
 - 2) Only authorized and authenticated users to information, files and equipment is granted to approved personnel
 - 3) Controls are in place designed to prevent malicious code (who's responsible)

The select agent regulations do not make a distinction between an IT based information system application or a paper based (hardcopy) application. In any given scenario the regulated community uses a combination of both. Some use IT more than others, but in any event, where both are used, each should be given equal attention. It is important that the entity includes both applications in their training program when it comes to information security. Furthermore, an RO needs to involve their IT and security departments and should include these departments in providing training for their laboratory personnel on the systems that are in place.

²⁰ Section 15(a) of the select agent regulations.

²¹ National Institute of Standards and Technology, Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST 800-14, September 1996.

²² National Institute of Standards and Technology, Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST 800-14, September 1996.

NIST has identified seven steps that should be considered when developing a computer security awareness program:²³

- **Identify Program Scope, Goals and Objective-** The program should provide training to all types of people who interact with IT systems. This would include large organizational programs supplemented by a more system-specific program. *All personnel approved for access to BSAT need to be trained on the specifics of good computer security practices.*
- **Identify Training Staff-** Trainers should have sufficient knowledge of computer security issues, principles and techniques. *ROs need to engage their IT departments or service providers to assist in the specifics of computer security, in addition to educating their IT support staff on the sensitivity of the BSAT program.*
- **Identify Target Audience-** Not everyone will need the same level of training to do their jobs. *Most users are not involved in the details of all nuances of IT hardware and software. Training should focus on the specific needs of the BSAT program.*
- **Motivate Management and Employees-** It's important to gain support of management and employees. *ROs need to engage with entity management to ensure that everyone associated with their BSAT program follows established information security policies and procedures.*
- **Administer the Program-** This would include visibility of the program, selection of appropriate training methods, topics and materials. *The RO needs to ensure that the IT training material has a specific application to the entity's BSAT program information security controls.*
- **Maintain the Program-** Efforts should be made to stay ahead of changes in computer technology and security requirements. *The RO should have a continuing dialogue with their IT departments, or service provider, to ensure that their IT needs are being met and if any new changes in the IT infrastructure (i.e., patching and updates) affect their activity.*
- **Evaluate the Program-** An evaluation should attempt to determine how much information is being retained, to what extent computer security procedures are being followed, and general attitudes toward computer security. *The RO needs to monitor performance (section 9(a)(4) of the select agent regulations) regarding adherence to good computer security practices and determine whether additional training should be conducted. This includes annual refresher training as required in section 15(c) of the select agent regulations.*

In addition, NIST has identified two types of audiences 1) the general user; and, 2) users that require specialized or advanced skills. Users that require specialized or advanced skills are more appropriate for entities with IT departments and systems administrators or service providers.

²³ National Institute of Standards and Technology, Introduction to Computer Security- The NIST Handbook, NIST 800-12, October 1995.

Most general users need to understand good computer security practices which should be the focus of the entity's training program, such as:

- a) Protecting the physical area and equipment (e.g., locking doors, securing file cabinets, caring for computer diskettes, USBs);
- b) Protecting passwords or other authentication data or tokens (e.g., never divulge PINs); and
- c) Reporting security violations or incidents (e.g., who to call if a computer virus is suspected).

Furthermore, general users should be instructed on the organization's policies for protecting information and computer systems and the roles and responsibilities of various organizational units with which they may have to interact.²⁴

Training should be tailored to the entity's specific needs and applications.²⁵ For example, an entity that uses an internet-based application will be different than an entity that uses a stand-alone (or intranet-based) application. Some entities may use IT databases for recordkeeping, whereas some may use hardcopy records secured in a file cabinet. Nonetheless, the entity should train personnel on the specific uniqueness of their information systems control that will satisfy sections 11(c)(1), (c)(9), 11(d)(2), (d)(6), (d)(7); and 17(b) of the select agent regulations.

²⁴ National Institute of Standards and Technology, Introduction to Computer Security- The NIST Handbook, NIST 800-12, October 1995.

²⁵ Section 15(a) of the select agent regulations.

References

1. Part 331 of title 7 of the Code of Federal Regulations (7 CFR part 331)
2. Part 121 of title 9 of the Code of Federal Regulations (9 CFR part 121)
3. Part 73 of title 42 of the Code of Federal Regulations (42 CFR part 73)
4. Biosafety in Microbiological and Biomedical Laboratories, 5th Ed. HHS Publication No. (CDC) 21-112, December 2009
5. National Institute of Standards and Technology, Introduction to Computer Security- The NIST Handbook, NIST 800-12, October 1995
6. National Institute of Standards and Technology, Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST 800-14, September 1996
7. Security Guidance for Select Agent or Toxin Facilities, which is available at <http://www.selectagents.gov/>.
8. Incident Response in Select Agent or Toxin Facilities, which is available at <http://www.selectagents.gov/>.

ADDITIONAL READING REFERENCE

National Institute of Standards and Technology, Computer Security Incident Handling Guide, Special Publication 800-61, Revision 1, March 2008

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	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Anti-Virus/Worm Protection	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Network Password Protection	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Desktop Password Protection	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Certified/Accredited Systems	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Security Patch Mgt. Procedures	<input type="checkbox"/> Yes	<input type="checkbox"/> No

B. Hardware Assets Protection

Main Computer Room Locked	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Laboratory Protection	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Wiring/Cable Closet Protection	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Restricted Access Protection	Yes	<input type="checkbox"/> No
Property Inventory Controls	Yes	<input type="checkbox"/> No
Fire Protection and Alarms	<input type="checkbox"/> Yes	<input type="checkbox"/> No

C. Personnel Security

Background Check for IT Staff	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Background Check for IT Part-Time	Yes	<input type="checkbox"/> No
Personnel Records Secured	Yes	<input type="checkbox"/> No
Information Security Manager	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Security Policy/Procedures	<input type="checkbox"/> Yes	<input type="checkbox"/> No

