



SECURITY PLAN GUIDANCE

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

FEBRUARY 2020



**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

Contents

| | |
|--|----|
| Changes and Highlights | 2 |
| Introduction..... | 3 |
| Section 11(a) – Creating a Site-Specific Written Security Plan..... | 4 |
| Security Plan Roles and Responsibilities | 4 |
| Section 11(b) – Site-Specific Risk Assessment..... | 7 |
| Section 11(c) – Planning Requirements..... | 11 |
| Access Control | 11 |
| Unauthorized or Suspicious Persons | 14 |
| Access Approval..... | 14 |
| RO Reporting | 14 |
| Information Systems Security Controls..... | 16 |
| Shipping and Transfers | 16 |
| Section 11(d) – Security Requirements | 18 |
| Storage..... | 18 |
| Section 11(e) – Inventory Audits | 18 |
| Section 11(f) – Tier 1 Security..... | 20 |
| Section 11(h) – Review and Revision..... | 23 |
| Appendix I: Risk Assessment Methods..... | 24 |
| Appendix II: Access Control Devices..... | 26 |
| Appendix III: Intrusion Detection Systems | 27 |
| Appendix IV: Intra-Entity Transfer Template..... | 28 |
| Appendix V: Scenarios (Non-Tier 1 Barriers and Access Controls):..... | 29 |
| Example Select Agent or Toxin Inventory Form that Captures the Section 17 Requirements | 31 |
| Inventory Audit Conditions | 32 |

Changes and 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 (FSAP) at:

CDC: LRSAT@cdc.gov

APHIS: DASAT@usda.gov

Revision History:

October 12, 2012: Initial posting

April 11, 2013: The revisions are primarily changes to correct editorial errors from previous version. July 3, 2013: Appendix added to document.

September 2017: Added Tier 1 requirements.

February 2020 (Revision 4): Revised Inventory language to match Inventory Guidance and to correct editorial errors from previous version.

Introduction

Section 11 of the select agent regulations ([42 CFR § 73.11](#), [7 CFR § 331.11](#), and [9 CFR § 121.11](#)) requires a registered entity to develop and implement a written security plan that is:

1. Sufficient to safeguard the select agents or toxins against unauthorized access, theft, loss, or release, and
2. Designed according to a site-specific risk assessment, providing graded protection.

The purpose of this guidance document is to assist an entity in developing and implementing its site-specific security plan. As used in this document, the word “must” means a regulatory requirement. The use of either “should” or “consider” signifies a suggested method that has requirements based on generally recognized security “best practices.” Implementation is performance-based and entities may find other ways to meet a regulatory requirement.

This document addresses the select agent regulations (SAR) with regard to security with one exception: Entities with Tier 1 BSAT have pre-access suitability and ongoing suitability assessment requirements which are addressed in the [Guidance for Suitability Assessments](#).

Section 11(a) – Creating a Site-Specific Written Security Plan

Section 11(a) of the select agent regulations require entities to develop and implement a written site-specific security plan. A security plan is a documented, systematic set of policies and procedures to achieve security goals that protect BSAT from theft, loss, or release. Plans may also include agreements or arrangements with extra-entity organizations, such as local law enforcement. Plans may be a single document, or incorporate other documents, policies, and procedures that work to achieve those security goals.

Entities should establish specific policies that support their plan. Security policies should document strategies, principles, and rules which the entity follows to manage its security risks. Effective policies provide a clear means of establishing behavioral expectations and cover the spectrum from directives, to standard operating procedures (SOPs). As part of security program management, the entity should consider formally documenting security policies covering all operational controls.

Background checks and other personnel security measures should be vetted through the entity's legal and human resources department. See the [FSAP Guidance for Suitability Assessments](#) for additional information.

An effective security plan should be based on the following principles:

- It should result from collaboration between entity management, scientific, facilities, safety and security personnel.
- It is built upon tested, well documented operational processes.
- It should account for and secure all biological select agents or toxins from creation or acquisition to destruction.
- It complements other plans such as biosafety, disaster recovery, continuity of operations, and others.
- It does not violate any laws. Laws to consider when creating the security plan include the Americans with Disabilities Act, OSHA Safety Standards, and local building and fire codes.
- The entity should provide security plan training to ensure every person understands his or her responsibilities.
- It requires reporting of all suspected security incidents and suspicious activities.
- It is reviewed at least annually and updated whenever conditions change.
- It is based on a site-specific risk assessment.

Security Plan Roles and Responsibilities

The security program should define each individual's roles and responsibilities and solicit their input for improvements.

An entity should be aware of, and collaborate with, the personnel responsible for and/or impacting security. This may include:

- Responsible Official (RO)/Alternate Responsible Official (ARO)
- Facility key control and/or access control personnel
- Alarm companies

- Campus security personnel
- Security personnel who observe video
- Local law enforcement or other response forces
- FBI – Weapons of Mass Destruction (WMD) coordinator

Key Entity Leadership

Certain parties should be involved in the process of designing and implementing the security plan. These include, but are not limited to:

- Owner/Controller
- Principal Investigator (PI)
- Responsible Official (RO)
- Alternate Responsible Official (ARO)
- Human Resources
- Biosafety staff
- Security staff
- Institutional Biosafety Committee
- Laboratory Management

Security Plan Team

Each person brings an important perspective as a subject matter expert (SME) in their own specialty. This group should collaborate to develop a site-specific security plan. Plans should also include agreements or arrangements with extra- entity organizations, such as local law enforcement.

Entities should form a team of entity SMEs, supporting security professionals, and stakeholders. The team should include entity professionals who are experts on the potential consequences of a theft, loss, or release of a select agent or toxin and the daily operations of the entity. Entities are also encouraged to include federal partners (i.e., the FBI) as well.

Entity personnel should provide knowledge of:

- SOPs, policies, and other organizational controls which can reinforce or be affected by security measures
- Public health consequences of the select agents and toxins
- Biosafety
- Operational requirements
- Value of the select agent or toxin work to the organization
- Knowledge of current security systems

Facility and support personnel should provide knowledge of:

- Facility wide security measures
- Personnel hiring practices (background checks, reference checks, education verification)
- Planned upgrades to the facility

- Constraints which affect security (biosafety, fire code, ordinances, federal laws)

Local, state, and federal law enforcement and security personnel members may be able to provide knowledge of:

- Known threats to the entities
- Assistance with identifying vulnerabilities
- Assistance with designing or vetting the mitigating factors
- Economic and psychological impacts of the select agents or toxins

Once the team is formed, members should be consulted on a regular basis, including during the plan development and implementation. The team should meet annually as part of the security plan review.

Section 11(b) – Site-Specific Risk Assessment

Section 11(b) of the select agent regulations states: “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.” Graded protection is a result of mitigating the hazards (threat and natural) and the vulnerabilities based on the consequences of a select agent or toxin in its current form.

The cornerstone of a good security plan is a current site-specific risk assessment. It forms the logical basis for physical and personnel security measures employed to achieve graded security. It should indicate what risks have been identified, and of those identified, which have been mitigated and any residual risks acceptable to the entity. It does not necessarily have to account for accidental hazards accounted for in a biosafety plan. **Risk** comes from the interaction of threats/hazards, vulnerabilities, and consequence (**Figure 1**).

There are many methods to capture these interactions, including qualitative, quantitative, or probabilistic analysis, among others. Any assessment that accurately captures and relates these interactions is sufficient.



Figure 1: Determining Risk

Conducting a Risk Assessment

Understand and Assess Threats

A threat is a person or organizations whose actions may cause the theft or release of a select agent or toxin. The threat may target the agent directly (e.g. theft), cause damage to the entity as the result of their action (e.g. extremists and terrorists damaging containment), and act on their own or collude with others. Threats can be captured as a ‘probability of attack.’

Threats are generally determined in 3 different ways:

- Entities are encouraged to reach out to law enforcement and other experts to understand, assess, and determine threats.
- An expert or group of experts model ‘threats’ in general, often using Design Basis Threat (DBT)¹. This capability is most common in federal and state facilities but may be available in larger entities.
- Historical data, including statistics on past local events (crimes), terrorist events worldwide, social science research into terrorists’ behavior, official accounts, and/or terrorists own writings about motivation and intent.

Insider Threats

An insider threat comes from personnel within the organization who have inside information regarding the organization’s security, data to include Select Agent and Toxin inventory, access to biocontainment and computers. The goals of such threats often involve fraud, information theft, intellectual property theft, theft and/or misuse of Select Agents and toxins, and computer system sabotage.

External Threats

An external threat originates outside of the organization. These threats may include hackers, outages, and other emergencies.

Natural Hazards

See the [Incident Response Guide](#) for resources to help you to determine if you are in a risk area for natural hazards. As with threats, entities should assess the impacts of the hazard to its people, select agent or toxin inventories as well as the entity as whole.

Understand and Assess Vulnerabilities

Vulnerability is the relative susceptibility of select agents or toxins to a threat or natural hazard. Vulnerabilities are a threat capability that can be applied which results in the theft or release of the agent or a natural hazard that can impact safety of staff and security of select agents or toxins. Vulnerabilities are often captured as “probability of effectiveness” (PE) of a particular system. Below are some best practices in conducting vulnerability assessment:

- Exercises/after action reviews
- Assessments by subject matter experts (SMEs)
- Scenarios and path development with SMEs and entity members
- Modeling (primarily with natural hazards)
- Simulations (primarily with natural hazards)

¹ A profile of the type, composition, and capabilities of an adversary.

Understand and Assess Consequence

Consequence is the impact of the theft or release of the agents. It is the impact on public, animal, or plant health and safety, and the potential for economic and psychological impacts. Entities should consider:

- The communicability of the agent.
- The agent's mortality and morbidity rates.
- Present availability of known countermeasures to the agent or toxin.
- The type of work being conducted on the select agent or toxin:
 - **Low risk** generally includes select agents or toxins that are handled in a diagnostic, non-propagative manner (e.g., single specimen, no culture). This may also include small quantities of select agents or toxins that are endemic in the environment.
 - **Moderate risk** includes select agents or toxins that are propagated or in amounts greater than a diagnostic sample. This risk level includes activities that work only with 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 select agents or toxins that are handled in large or highly purified quantities. It would also include those select agents or toxins used in higher risk procedures such as aerosolization, centrifugation, animal inoculation, or restricted experiments (as defined by section 13 of the select agent regulations).

Key point: Unless there is sufficient data available to project a particular threat's capability to enhance an agent, entities do not have to consider hypothetical threats that would make an agent more virulent. Current characteristics are sufficient for this assessment.

Assess Risk

A sufficient risk assessment should reflect the interactions of threat, vulnerability and consequence. In implementing a risk assessment, threat, vulnerability, and consequence may be captured as discrete variables, dependent variables (i.e., probability), or other methods. Also, entities may use a quantitative or qualitative means depending on the amount of information available. See [Risk Analysis Methods](#) for more information and examples of qualitative risk assessment. For guidance on mitigating the impacts of a natural hazard, see the [Incident Response Guide](#).

Communicating Risks

After the risk assessment is completed, the [key entity leadership](#) should determine if the current risk level is acceptable. If the risk level is deemed unacceptable, then the entity should develop a means to mitigate the risk. Some common risk mitigation measures are given below. It should be noted that any activity involving a select agent or toxin will involve some level of unmitigated risk. The only way to eliminate risk completely would be to not undertake this work.

Manage the risk: Mitigation measures

If the risk is not acceptable, the entity has multiple paths to mitigate the risks. Options include:

- Employ additional security measures.
- Change the work with the select agent or toxin to reduce risk.

- Decrease the quantity of toxin on hand, possessing only the amounts necessary for the work.
- Change how the select agent or toxin is stored (e.g., not lyophilized).
- When a toxin is a by-product of a larger process, immediately autoclave the agent or destroy the toxin.
- Document any risks which have not been mitigated and why.

Document and Update the Risk Assessment

The entity should document the risk assessment and review it as threats change. The security plan should be updated to reflect the changes based on the risk assessment, as should any drills and exercises that are impacted by the change.

Section 11(c) – Planning Requirements

Section 11(c)(1) of the select agent regulations requires the security plan to describe procedures for physical security, inventory control, and information systems control. These descriptions should reflect the policies implemented at the entity. This section explains different methods for ensuring that the entity's security plan complies with the regulations.

Effective inventory control measures for select agents and toxins can deter and detect a variety of insider threats. How the inventory audits are conducted and inventory is maintained must be described in the entity's security plan and inventory records must meet the requirements of section 17 of the select agent regulations. The security requirement includes:

- Current accounting of any animals or plants intentionally or accidentally exposed to a select agent.
- An accurate and current inventory for each select agent or toxin in long-term storage.
- Labeling and identifying select agents and toxins in the entity inventory in a way that leaves no question that the entity's inventory is accurately reflected in the inventory records.
- Accounting for select agents and toxins from acquisition to destruction.
- See [Inventory Audits](#) for more detailed instructions on maintaining effective inventory control.

Access Control

Section 11(c)(2) – Provisions for Access and Safeguarding

Section 11(c)(2) of the select agent regulations require the security plan to describe how the select agent or toxin is physically secured against unauthorized access. The security plan is performance based and should complement the Incident Response Plan and Biosafety Plan. An effective physical security plan deters, detects, delays, and responds to threats identified by the site-specific risk assessment. A successful security plan creates sufficient time between detection and the completion of an attack for response force to arrive. The physical security plan should include:

- Security barriers that both deter intrusion and deny access (except by access approved personnel) to the areas containing select agents and toxins:
 - Perimeter fences
 - Walls
 - Locked doors
 - Security windows
 - Trained person (e.g., security guard, trained laboratorians, or escorts)
- Biosafety measures and other environmental factors that increase security such as:
 - Access or locking system which denies access to BSAT, e.g. mechanical locks, card key access systems or biometrics
 - Tamper-evident devices for select agents and toxins held in long-term storage
- A balanced approach so that all access points, including windows and emergency exits, are secured at the same level
- A procedure or process to keep the number of alarms to a minimum

Create a system that limits access to select agents and toxins to those approved by the HHS Secretary or APHIS Administrator for access to select agents and toxins. The access control system should:

- Include provisions to limit unescorted/unrestricted access to the registered areas to those who have been approved by the HHS Secretary or APHIS Administrator to have access to select agents and toxins.
- Include provisions for the safeguarding of animals and plants exposed to or infected with select agents.
- Regularly review and update access logs.
- Be modified when access requirements change or be responsive to changes in personnel's access requirements during personnel changes.

Remain flexible enough so non-approved personnel can be escorted if needed. See [Non-Tier 1 Barrier Scenarios](#) for a visual representation of adequate physical security barriers. See [Intrusion Detection Systems](#) for a chart that defines and explains the use of various IDS options.

Section 11(c)(3) – Provisions for Cleaning, Maintenance, and Repairs

The security plan must state how cleaning, maintenance, and repairs will be accomplished in areas where BSAT are stored or used. When allowing maintenance, cleaning, or repair personnel (whether in-house or contract services) into a registered area, an entity should practice one or more of the following:

- 1) Use only access approved individuals.
- 2) Provide an access approved individual as an escort to the non-approved individual.
- 3) If the non-approved individual will not be escorted, install additional security measures (e.g., additional lock and key, cipher lock, or tamper alarms interfaced with the facility intrusion detection system) to prohibit access to select agents and toxins by non-approved individual; or
- 4) Remove the select agent or toxin to a different area that is appropriately registered.

Section 17 (Records) of the select agent regulations requires that access logs must be in place to record the name and date/time of entry into the registered area, including the name of an escort.

Section 11(d)(2) – Escort Provisions

The security plan must contain provisions that allow non-approved persons access to registered spaces that store BSAT only when escorted by an access approved person. The escort must be dedicated to observing the escorted person. No other duties may be performed during the time that the individual is serving as an escort. The escort must understand what to observe for (e.g., accessing select agents and toxins). Non-approved persons are not allowed to have access to an agent, even if escorted by an access approved person. The escort's responsibilities include:

- Serving as a physical barrier between the non-FSAP approved person and select agents and toxins.
- Being knowledgeable about the entity's security policies.
- Training non-FSAP approved persons on emergency protocols and risks related to the BSAT before they enter the registered space.
- Executing safety protocols as necessary.
- Receive approval for escorted access and notifying the RO when escorted entry has concluded.

See the [Security Risk Assessment FAQs](#) for more information about escort provisions.

Section 11(d)(6) – Prevent Sharing Access Credentials

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 other person. This should include how the entity prevents:

- “Piggybacking” or “tailgating” on another access approved person’s access card.
- Key card, password or badge sharing.

Challenge all individuals who tailgate or piggyback a secured access entry point.

Section 11(c)(5) – Identification, Key, Keycard, Combination, and Password Management

The security plan must describe the procedures for changing access after personnel changes in order to prevent access by personnel who have previous approved access to select agents and toxins. This can include:

- Deactivating card key access.
- Deactivating email, network, and local machine computer accounts which provide access to information.
- Surrendering key cards and badges.
- Surrendering keys and key cards when people leave or change duties.

The security plan must indicate that the following incidents must be reported to the RO:

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

Unauthorized or Suspicious Persons

Section 11(c)(4) – Reporting and Removing Unauthorized or Suspicious Persons

An “unauthorized person” is not approved to have access to select agents and toxins or is not authorized by the entity to be in a particular area or be involved in particular conduct. A “suspicious person” is any individual who has no valid reason to be in or around the areas where select agents and toxins are possessed or used.

The security plan must describe the process for identifying and removing unauthorized and suspicious persons. It must also require follow-up actions such as reporting the information to the RO; and the RO reporting the information to entity security personnel, and possibly contacting local law enforcement agencies or FSAP, as appropriate.

Unauthorized and suspicious persons attempting to gain entry into registered areas without proper credentials should be identified, challenged and removed immediately. The RO must be notified immediately (see Section 11(d)(7) for more details).

The entity should consider:

- Integrating an access control measure (e.g., card key) into an alarm system that notifies a responder when an unauthorized person attempts to gain access (similar to an IDS, but does not involve an actual break in).
- Having a badge system that clearly identifies who does and does not have approved access to select agents and toxins.
- Provide training on how to remove unauthorized personnel (e.g., procedures for notification of security personnel and/or local law enforcement).

See [RO Reporting](#) for more detailed instructions for what activities should be reported to the RO.

Access Approval

Section 11(c)(7)

Section 11(c)(7) requires the entity to ensure that all individuals with access approval from the HHS Secretary or APHIS Administrator understand and comply with the security procedures. All approved individuals should undergo training that covers general security as well as security training as it applies to their specific work. See the [Training Requirements guidance document](#) for general information on training provisions.

Section 11(d)(1)

Create a system that limits access to select agents and toxins to those approved by the HHS Secretary or APHIS Administrator for access to select agents and toxins. Individuals must have passed a security risk assessment and have approval from either the HHS Secretary or APHIS administrator before they obtain access to any select agents or toxins.

RO Reporting

Section 11(c)(8) – Suspicious Activities

The security plan must describe procedures for how the RO will be informed of suspicious activity that may be criminal in nature and related to the entity, its personnel, or its select agents and toxins. Individuals with access

to select agents and toxins must be aware of the protocol for reporting suspicious or criminal activity. The plan must also describe procedures for how the entity will notify the appropriate federal, state, or local law enforcement agencies of such activity. Identify who best can respond to the circumstances during the security portion of the risk assessment.

The security plan must include procedures for how the entity will notify the appropriate Federal, State, or local law enforcement agencies of any suspicious or criminal activity.

Suspicious activity of a criminal nature includes:

- Those activities so identified in the site-specific security risk assessment.
- Insider:
 - Attempts to create additional select agent or toxin inventory not authorized or required.
 - Attempts to conceal or hide and not report select agent or toxin inventory discrepancies.
 - Attempts to remove select agent or toxin inventory without authorization.
 - Attempts by “restricted” persons to intentionally access registered areas containing a select agent or toxin.
- Outsider:
 - Indirect threats against the entity receives by email, letter, telephone, or website postings.
 - Unauthorized attempts to purchase or transfer a select agent or toxin.
 - Attempts to coerce entity personnel into a criminal act.
 - Intimidation of entity personnel based on their scientific work (for example, eco-terrorism).
 - Requests for access to laboratories for no apparent legitimate purpose or for purposes that do not appear legitimate.
 - Unauthorized attempts to probe or gain access to proprietary information systems particularly access control systems (for example, attempts by unauthorized individuals to gain physical or electronic access to systems).
 - Theft of identification documents, identification cards, key cards, or other items required to access registered areas.
 - Personnel representing themselves as government personnel (federal, state, local) attempting to gain access to the facility or obtain sensitive information that cannot or will not present appropriate identification.
 - Use of fraudulent documents or identification to request access.

Section 11(d)(7) – Reporting to the RO

Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official:

- Any loss or compromise of keys, passwords, combination, etc.
- 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.
- Any loss of computer, hard drive or other data storage device containing information that could be used to gain access to select agents or toxins.
- Any security breach of containment laboratory containing select agents and toxins

Information Systems Security Controls

Section 11(c)(9) – Information Systems Security Controls

Please see the [Information Systems Security Controls Guidance](#) for details about meeting the requirements of this section of the regulations.

Shipping and Transfers

Section 11(c)(10) Shipping and Transfers

The security plan must contain provisions and policies for shipping, receiving, and storage of select agents and toxins. This includes procedures for receiving, monitoring, and shipping of all select agents and toxins.

With exception of exports out of the country, shipments containing select agents and toxins between entities must be authorized by FSAP, coordinated through an [APHIS/CDC Form 2](#), and tracked so the receiving entity knows when the shipment will arrive. Both the sender (unless the sender is outside of the United States) and the recipient (unless the recipient is outside the United States) of the package must be approved for access to select agent or toxins.

The individual who packages the BSAT for shipment must have an SRA approval and appropriately trained.

The package containing select agents and toxins is not considered “received” by the entity until the intended recipient takes possession of the package. The intended recipient must have SRA approval and, if the agent is Tier 1, have gone through the entity’s pre-access suitability and is subject to the entity’s ongoing assessment.

When received by the intended recipient, the shipment should immediately be secured in a registered space. Ideally, the shipment is taken to the receiving laboratory; however, the package may be temporarily stored in other registered spaces.

Shipping and receiving areas must be registered if the select agents or toxins packages are identified or accessed. For example:

- If packaging or un-packaging of a select agent or toxin is performed in these areas.
- If the plan to temporarily store identified select agents.

If select agent or toxin packages are not identified or accessed, the shipping and receiving area may not need to be registered.

The entity must also have a written contingency plan for receipt and security for unexpected shipments. An “unexpected shipment” is when an entity receives a legitimate shipment of a select agent that it had neither requested nor coordinated for. The entity must have a contingency plan to have approved personnel gain control of the unexpected shipment of BSAT without delay and secure it in a registered area.

Section 11(d)(5) – Intra-Entity Transfers

An intra-entity transfer is a physical transfer of select agents or toxins that takes place between two individual with access approval, preferably two FSAP approved PIs, at the same registered entity, and e.g., a PI removes a select agent or toxin from his long term storage and gives it to another PI at the same entity.

Entities that conduct intra-entity transfers must describe in their security plan how these transfers will take place, including chain-of-custody documents and provisions for safeguarding the select agents and toxins against theft, loss, or release. Please see the example intra-entity transfer form to see what information should be captured according to section 17 (Records) of the select agent regulations. Transfers must include a chain-of-custody document and ensure that select agents and toxins will not be left unattended. See the [Intra-Entity Transfer Template](#). The entity is not required to cover intra-entity transfers in the security plan if they do not conduct them.

Section 11(d)(4) – Inspection of Suspicious Packages

A suspicious package is any package or item that enters or leaves registered areas that does not appear to be consistent with what is expected during normal daily operations.

The entity should consider the following indicators of suspicious packages:

- Misspelled words
- Addressed to a title only or an incorrect title
- Badly taped or sealed
- Lopsided or uneven
- Oily stains, discolorations, or crystallization on the wrapper
- Excessive tape or string
- Protruding wires
- Return address does not exist or does not make sense

The security plan must describe how the entity will inspect packages based on the site-specific risk assessment. The entity should inspect all packages and items before they are brought into or removed from areas where select agents and toxins are used or stored (registered laboratory, etc.). Suspicious packages should be inspected visually or with noninvasive techniques before they are brought into, or removed from the area where select agents and toxins are stored or used. See the [USPS guidelines for recognizing suspicious packages](#) for more detailed information.

Section 11(d) – Security Requirements

This section describes the policies and procedures that the entity must implement in order to be in compliance with the select agent regulations.

Storage

Section 11(d)(3) – Storage Control

The entity is required to “provide for the control of select agents and toxins by requiring freezers, refrigerators, cabinets, and other containers where select agents or toxins are stored to be secured against unauthorized access (e.g., card access system, lock boxes).” See [Access Control Devices](#) for more information on methods of securing BSAT against unauthorized access.

The entity can comply with this requirement in a number of ways. Typically, physical locks, key card access, biometrics, or some combination of those provide adequate storage control. Tier 1 select agents and toxins require more stringent conditions. See the Tier 1 guidance document for more information.

Section 11(d)(8) – Separate Registered Space from Public Space

The storage or laboratories that contain select agents and toxins must not be publicly accessible. Public areas are places where the general public may congregate or transit. Areas where select agents and toxins are used or stored must be registered and personnel with access to the registered space must have approval from the HHS Secretary or the APHIS administrator.

Section 11(e) – Inventory Audits

An inventory audit is an examination of a portion of the inventory or collection sufficient to verify that inventory controls are effective. **Note:** This inventory is not a part of the requirements of [section 17](#). Section 11(e) of the select agent regulations requires the entity to perform a complete inventory audit for all BSAT under the control of a PI whenever:

1. The BSAT is physically relocated to another registered space.
2. There is a change (departure or new arrival) of the PI in control of the BSAT.
3. There is a theft or loss of BSAT under the control of the PI.

Entities have discretion on how they conduct these audits. The depth of an audit should depend on the circumstances. Entities should consider the following when determining the depth of an entity audit:

1. The timing of the inventory audit.
2. The circumstances that require the inventory audit. For example, an ‘emergency’ movement to another location (freezer malfunction) may result in a focus on counting full racks and a confirmation of a targeted, smaller number of vials. In the case of a shipment to a new building or campus where there is sufficient time to plan, entities are encouraged to inventory more thoroughly.
3. The criteria used to determine which samples are audited. In the case of a large inventory, the entity may choose to focus on the most recently manipulated samples. In the case of a small inventory, the entity may choose to focus on the entire inventory.
4. Any additional storage measures. If the material is stored in tamper evident systems, the entity may choose to count the sealed containers instead of the individual vials within those containers.

5. The size of the collection being audited and the manner it is stored. Inventories which are intermixed with other samples may require a 'vial by vial' audit.

Select agent inventories should be confirmed, at a minimum, annually. For those inventories with frequent access, regardless of the number of individuals accessing, it is recommended that inventory records are confirmed semi-annually or quarterly for those specific accessed storage containers.

A suggested best practice is to have two individuals involved in confirming the inventory records to ensure counts are accurate and verified. Each individual could record their respective inventory counts on an inventory verification worksheet with initials or signatures indicating the verification. If two individuals cannot be involved in the verification count, then one individual conducting the select agent inventory confirmation could conduct two counts of the inventory and record both counts on the inventory verification worksheet to provide verification of an accurate inventory count. Sealed boxes should have the security tape identification confirmed. There should be a record available of a vial-by-vial inventory being conducted at the time of the box being sealed. If there are doubts of the sealed box contents then the box should be opened and a confirmed inventory identification and count conducted and recorded. Frequency of the inventory confirmation may vary depending upon how often inventories are accessed and the manner of storage.

For those inventories that contain a mixture of varying agent identifications, or inventories with multiple individuals frequently accessing storage areas, it is recommended that quarterly inventory confirmations are conducted for those storage containers involved in such access occurrences. During the quarterly, semi-annual, or annual inventory confirmation, those containers which are accessed and having inventory added or removed should have all vials or containers in those specific storage boxes/containers counted and confirmed. The percentage of additional inventory that is to be confirmed on an annual basis will vary with the inventory size. Laboratories with large inventory volumes should confirm inventories for any storage boxes/containers accessed throughout the year. Inventory collections containing lesser quantities of material and routine access should have the entire inventory confirmed at least on an annual basis.

See the [Inventory Audit Conditions table](#) for more detailed instructions for when an inventory audit is necessary.

Maintain audit records in accordance with section 17(c). Changes to the inventory must be recorded in accordance with section 17(a) as well.

Section 11(f) – Tier 1 Security

Tier 1 select agents and toxins require additional security measures to be implemented including the addition of pre-access suitability assessments, extra access controls, and extra barriers. These extra measures are intended to safeguard Tier 1 select agents and toxins further from theft, loss, or release. The list of Tier 1 select agents and toxins includes:

- *Bacillus anthracis*
- *Bacillus cereus* Biovar *anthracis*
- Botulinum neurotoxins
- Botulinum neurotoxin producing species of *Clostridium*
- *Burkholderia mallei*
- *Burkholderia pseudomallei*
- Ebola virus
- Foot-and-mouth disease virus
- *Francisella tularensis*
- Marburg virus
- Rinderpest virus
- Variola major virus (Smallpox virus)
- Variola minor virus (Alastrim)
- *Yersinia pestis*

An effective security plan for Tier 1 BSAT describes how the requirements of the regulations are met. The security plan should also discuss who manages security control measures. This may include:

- How the entity manages access controls – This management may include keys, card keys, access logs, biometrics and other access control measures for each of the security barriers in the security plan. This may be accomplished by directly controlling or interacting with a service provider (e.g., a security guard company).
- Designating personnel to manage the entity's security systems, including intrusion detection
- How the intrusion detection alarm code is managed (who has it, when it is changed)
- How the entity tests and manages the configuration of the system
- How the entity responds to an access control or intrusion detection failure (e.g., alarm)
- How the entity screens visitors

Section 11(f)(1) – Pre-Access Suitability Assessment

The entity must develop, implement, and describe in the security plan procedures for conducting a pre-access suitability assessment of persons who will have access to a Tier 1 select agent or toxin. See the [Guidance on Suitability Assessments](#). Individuals must have a pre-access suitability assessment conducted before they are allowed access to Tier 1 select agents and toxins.

Section 11(f)(2) – Responsible Official Coordination with Other Safety and Security Professionals

Entities must describe procedures for how an entity’s Responsible Official (RO) will coordinate their efforts with the entity’s safety and security professionals to ensure security of Tier 1 select agents and toxins and share, as appropriate.

Ideally the entity’s RO, safety, and security professionals should meet on a regular or defined basis. This may be annually in conjunction with the security plan review, after a security incident, when there is a significant entity change that affects security, or in response to a threat. See **Figure 2** for an example of the personnel who should be involved in creating a security plan for entities registered to possess or use Tier 1 BSAT.

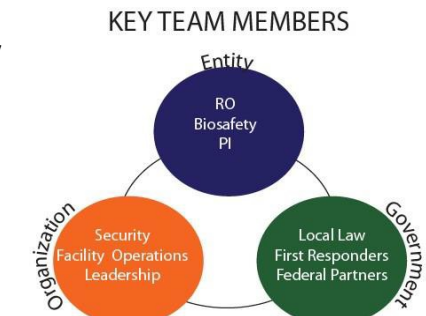


Figure 2: Tier 1 BSAT Security Plan Team

Section 11(f)(3) – Ongoing Suitability Assessments

Describe procedures for the ongoing assessment of the suitability of personnel with access to a Tier 1 select agent or toxin. See the [Guidance on Suitability Assessments](#). The procedures must include:

- Self-Reporting – Individuals should be trained on how to report any incidents or conditions that might impact their ability to safely have access to select agents and toxins and to safeguard them from theft, loss, or release.
- Peer-Reporting – Individuals should be trained on how to report incidents or conditions that might impact the ability of others to safely have access to select agents and toxins. Peer-reporting should be safe and anonymous and protect whistle-blowers from repercussion.
- Employee Training – All employees must be trained on the entity’s policies and procedures for reporting, evaluating, and corrective actions concerning suitability assessments. This type of training may include threat awareness, self- and peer-reporting, behaviors of concern, and suitability policies.
- Ongoing Suitability Monitoring – All individuals with access to Tier 1 select agents and toxins must undergo ongoing suitability monitoring. There are several ways to achieve this, including annual performance reviews, access reviews, and criminal record reviews.

Section 11(f)(4) – Security Enhancements

Entities that possess Tier 1 select agents and toxins must adhere to extra security enhancements, including access limitations, extra barriers, intrusion detection system, and visitation policies.

Section 11(f)(4)(i) requires the entity to limit access to a Tier 1 select agent or toxin to only personnel who have been approved by the HHS Secretary or APHIS Administrator, following a security risk assessment (SRA) conducted by the Attorney General, and have had an entity-conducted pre-access suitability assessment. Such individuals must also be enrolled in an ongoing suitability assessment program conducted by the entity.

- Make sure that only HHS or USDA approved individuals have access to Tier 1 BSAT.
- Conduct a pre-access suitability assessment before granting access.

- Enroll each individual to be given access to Tier 1 BSAT in an ongoing suitability assessment program.

Access Outside Normal Business Hours

Section 11(f)(4)(ii) requires the entity to limit access to registered spaces outside of normal business hours. Only individuals who have been specifically approved by the RO, or his/her designee, may be allowed to access laboratories or storage facilities containing Tier 1 select agents and toxins outside of normal business hours.

Limiting access to registered spaces outside of normal business hours does not mean that personnel cannot work outside these hours; however, they should get specific approval by the RO, or his/her designee, before doing so. The entity may choose to establish specific after-hours work policies. For example, the entity could establish a rule that states at least 2 persons should be working in the laboratory if work must be conducted after hours. This rule should consider, and implement, any necessary justification for after-hours work, such as 24 hour animal studies.

Security Barriers

Section 11(f)(4)(iv) of the select agent regulations requires a minimum of three security barriers safeguarding Tier 1 select agents and toxins against theft, loss, or release. A barrier is a physical structure designed to prevent unauthorized access. Cameras, security lighting, and IDS are not considered security barriers because, while they may monitor and detect unauthorized access, they cannot, by themselves, prevent access. These security barriers must be identified on the entity’s registration ([APHIS/CDC Form 1](#)) and described in the security plan.

Examples of Acceptable Security Barrier Implementations

| Ex. | Barrier 1 | Barrier 2 | Barrier 3 (linked to access approval) |
|-----|--------------------------|------------------------------|---|
| 1. | Guard/Perimeter Fence | Card-Key Access to floor | Key locked container with strong key control measures |
| 2. | Building Card Key Access | Limited Room card-key access | Different card-key required for room |
| 3. | Building Card Key Access | Limited Room card-key access | Card-key PIN access room |
| 4. | Building Card Key Access | Limited Room card-key access | Biometric lock system on freezer |
| 5. | Building Card Key Access | Card-key PIN access room | PIN access to freezer |
| 6. | Building Card Key Access | Limited Room card-key access | Restricted card key access to registered space |
| 7. | Floor Card Key Access | Limited Room card-key access | Restricted card key access to registered space |

Security barriers should be implemented based on a site-specific risk assessment and should ensure that the following conditions are met:

- Each security barrier must add to the delay in reaching the areas where select agents and toxins are used or stored. Most security barriers, in and of themselves, do provide additional delay to forced entry.
- All access points, including emergency exits, must be secured. If there is a card key lock on the main door, the emergency exit should be secured to prevent ingress – for example, by having no outside handle.
- One of the security barriers must be monitored in such a way as to detect circumvention of established entry control measures under all conditions. This may include video cameras, monitoring access control

logs from a card key reader or other methods of regular monitoring.

- The final security barrier must limit access to the select agents and toxins to personnel approved for access by the HHS Secretary or APHIS Administrator.
- Per section 11(f)(4)(i), the entity must ensure access to the Tier 1 BSAT is limited to those who have undergone the entity's pre-access suitability and are subject to ongoing suitability assessment. Access records can be used to show that only access approved personnel have accessed the final barrier.

Personnel who are trained to identify and respond to suspicious activities can be considered a security barrier. Persons who receive 'insider threat,' 'suspicious person' or similar training along with response procedures (i.e., calling security, 911, etc.) are considered 'trained personnel.' Therefore, when they are physically present, they may be considered a security barrier.

Intrusion Detection Systems

Section 11(f)(4)(v) requires the entity to ensure that all registered spaces containing Tier 1 select agents or toxins must be protected by an intrusion detection system (IDS) unless the area is physically occupied. An IDS consists of a sensor device which triggers an alarm when a security breach occurs notifying a response force (e.g., local police, security guard force, etc.) who have the capability to respond to the alarm and stop a threat.

Section 11(f)(4)(vi) requires that personnel monitoring the IDS must be capable of evaluating and interpreting the alarm and alerting the designated security response force or law enforcement. Some response options include:

- Personnel employed by the entity (an alarm or security operations center)
- Contracted alarm company
- Local law enforcement
- Military police unit
- Dedicated entity personnel

If the IDS is monitored by a service provider with a local law enforcement response, the entity should coordinate with local law enforcement to assist them in understanding the importance of the information from the service provider. For example, due to the volume of false alarms, local law enforcement may not treat the alarm as a serious matter. Entities are encouraged to discuss the consequence of the theft of a select agent or toxin with local law enforcement so they can understand the seriousness of the threat and also understand that an alarm at an entity housing select agent requires immediate response.

Intrusion Detection Response Times

Section (11)(f)(4)(viii) requires the entity to determine response times for security forces or the local police to Intrusion Detection Systems. The response time must not exceed 15 minutes from the time that an alarm sounds or a security incident is reported to the arrival of the responders at the first security barrier.

A response force is a force capable of interrupting a threat. It may be unarmed guards, armed guards and/or local law enforcement – though law enforcement is preferable.

The target for response time, 15 minutes or less, is based on the Department of Defense adopted standards for protecting high consequence assets. However, entities are strongly encouraged to coordinate with local law enforcement and/or federal partners to assist with threat assessment to determine the appropriate response

time. Local law enforcement, especially in areas where the response time is challenging, will often assist the entity in determining how long the barriers will delay an adversary.

There are many ways to reduce response time for the response force to less than 15 minutes. One method is to perform the following steps:

- Discuss regulatory requirements and strategies with local law enforcement.
- If you have a dedicated guard force, work with them (generally, you will meet this requirement with a dedicated guard force).
- Calculate the delay time provided by entity security barriers and compare it to the expected response time of the response force. Get the typical response times from the responding personnel and compare it to the delay times determined through scenarios.
- Conduct an exercise with local responders.

Though not required, entities should consider the effect of natural hazards, such as a hurricane or blizzard, when addressing response times.

Access Control Systems

Section (11)(f)(4)(vii) requires the entity to describe procedures to ensure that security is maintained in the event of the failure of access control systems due to power disruption affecting the registered spaces.

In the event of an incident that disrupts or cuts off power to the registered space, the entity must have a plan in place to ensure that security is maintained, and three physical barriers will remain in place, until power can be restored. Some acceptable methods include:

- Fail-safe locks that are locked or remain locked when power is interrupted or there is a power outage.
- Adding personnel/guard forces at doors that acts as one of the three physical barriers but may fail and open instead of being closed/locked in the event of a power failure.
- Backup generators or batteries that will restore power to the access control systems.

For example, if power is lost and the door locks (even if it can be opened only from the inside), then it meets this requirement. If power is lost and the door unlocks (it can be opened from the outside), then it does not meet the “fail safe” requirement.

Depending upon the access control systems (ACS) and equipment, the entity should consider changing lock combinations, ACS password/PIN, intrusion detection system (IDS) password/PIN, and access approvals in which the departing personnel was assigned when they are removed from the program and/or access to Tier 1 select agents. Former employees that retain the ability to use and control the locks, ACS, and the IDS would be considered a vulnerability.

Section 11(f)(5) – Security Enhancements

Entities that possess Variola major virus, Variola minor virus ([9 C.F.R. Part 121](#)), foot-and-mouth disease virus and rinderpest virus ([42 C.F.R. Part 73](#)) must have additional security requirements as outlined in the select agent regulations.

Section 11(h) – Review and Revision

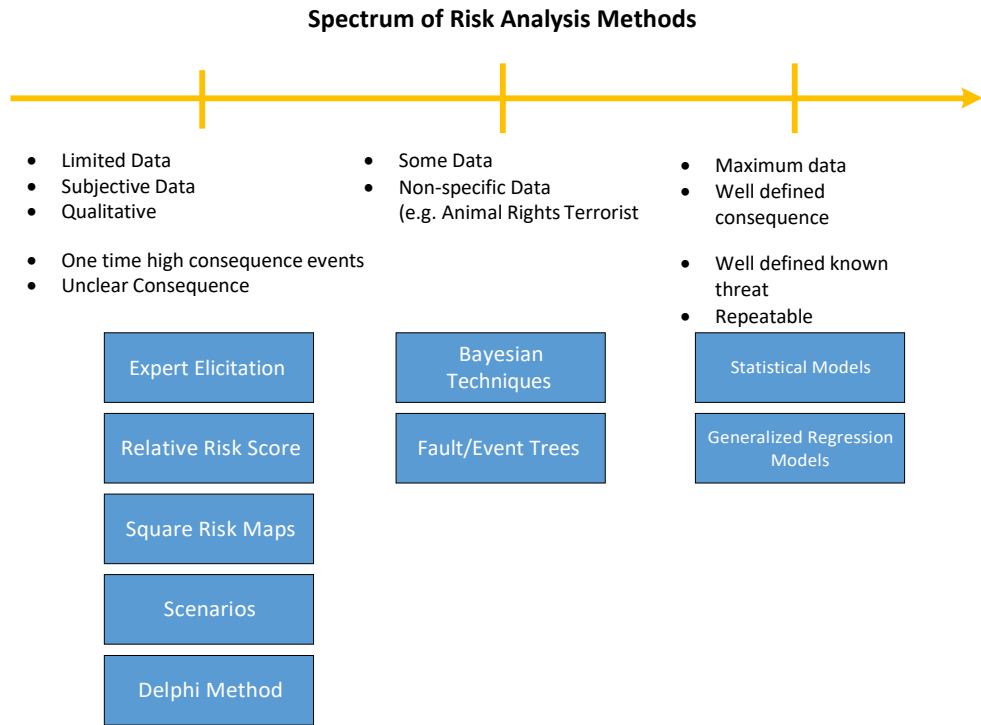
The security plan should be reviewed at least annually and revised as necessary. Some events that may necessitate the review and revision of the security document include:

- Theft, loss, or release of a select agent or toxin
- Changes to entity registration
- Changes to the registered space
- Changes to relevant entity personnel
- Any training assessments, drills, or exercises that may change along with a change to the security plan must also be updated. In addition, all drills and exercises should be documented to include How the plan was tested and evaluated (i.e. objectives and goals for the exercise or drill)
- Problems identified in corrective action
- Names of personnel who participated i.e. sign-in sheets

For more information, see the [Drills and Exercises guidance document](#).

Appendix I: Risk Assessment Methods

There are several methods for determining risk. Any recordable method is acceptable, as long as the entity determines risk as the intersection between threat, likelihood, and consequence. The National Academies of Science describes different methods of risk analysis as being on a spectrum, like those in the following table. More qualitative methods are on the left while quantitative, data-reliant methods are toward the right.



For example, the square risk map is a qualitative analysis method that relies on a common sense understanding of the combination of threat and vulnerability with the consequence of such an incident occurring.

| | | | | |
|-------------|---------|------------------------|----------|---------|
| | | RISK | | |
| Consequence | Extreme | High | High | Extreme |
| | High | Medium | High | Extreme |
| | Medium | Medium | Medium | High |
| | Low | Low | Medium | High |
| | | Unlikely | Possible | Likely |
| | | Threat + Vulnerability | | |

Figure 1: Square Risk Maps assess risk by comparing the threat and vulnerability of a situation to the consequence. The risk is assessed as Low, Medium, High, or Extreme.

Similarly, the relative risk score method numerically scores threats and vulnerabilities compared to the consequence of a given scenario and plots the risk according to a set range of risk levels.

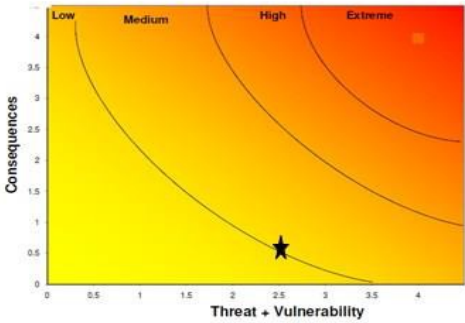


Figure 2: Example “Relative Risk Score”- This method assesses risk by numerically scoring threats and vulnerabilities compared to the consequence of a given scenario.

Appendix II: Access Control Devices

| Lock Type | Physical Security Requirement | Additional SRA Requirements |
|--|---|---|
| Mechanical Key | <ul style="list-style-type: none"> • All keys must be tracked in a log. • Change locks if key is lost or compromised. • All keys must be returned when people quit or are terminated. • Log access and retain for 3 years. • If the key is secured in a key box, the key box key must meet the requirements above. | <ul style="list-style-type: none"> • All personnel with access to the key must have SRAs. • If in a key box, all personnel with access to the key box key must have an SRA. • If there is no IDS, the following people must have SRAs: • All personnel with access to a master key. • All personnel with access to a facility or building grand master. • Entity locksmiths if they have or can make the key and the key can be traced to the door. |
| Cipher Key/Combination lock | <ul style="list-style-type: none"> • Change the code or lock when personnel quit or are terminated. Changes must be reflected in a log. • Change the code or lock in the event of compromise. • Log access to registered areas and retain access records for 3 years. | <ul style="list-style-type: none"> • All personnel with the code/combination or access to the code/combination must have SRAs. • If there is no IDS, the following people must have SRAs: • All personnel who can change the code. |
| Card Key | <ul style="list-style-type: none"> • Maintain electronic or physical logs of access to registered areas for 3 years. • The log must be capable of being printed. • The access control network must meet the information security requirements. | <ul style="list-style-type: none"> • All personnel with card-key which can open door • (includes facility wide keys) |
| Card Key+ Pin | <ul style="list-style-type: none"> • Maintain electronic logs of access for 3 years. • The access control network must meet the information security requirements. | <ul style="list-style-type: none"> • No additional requirement |
| Biometrics | <ul style="list-style-type: none"> • Maintain electronic logs of access for 3 years. • The access control network must meet the information security requirements. | <ul style="list-style-type: none"> • No additional requirement |
| Multiple kinds of access control (i.e., Card Key and Mechanical Lock on same door) | <ul style="list-style-type: none"> • All the requirements for each type of access control systems when or if used. | <ul style="list-style-type: none"> • All the SRA requirements for both systems unless use of the access control device triggers the IDS (use of a mechanical key in Card-Key door will often trigger a 'forced door' alarm. The same alarm if someone broke the door down). |
| Remote opening (e.g., someone 'buzzes' a person in) | <ul style="list-style-type: none"> • Maintain electronic logs of access for 3 years. • The access control network must meet the information security requirements. | <ul style="list-style-type: none"> • No additional requirement |
| "Emergency" card key kept with First Responders | <ul style="list-style-type: none"> • Log of access. • Inventory of key. • Notification of the RO and FSAP in the event of its use. | <ul style="list-style-type: none"> • No SRA requirement for first responders |
| Emergency mechanical key or Card-Key in Knox Box (key stored in secured 'box' only accessible to first responders) | <ul style="list-style-type: none"> • Maintain electronic logs of access for 3 years. • Notification of the RO and FSAP in the event of its use. | <ul style="list-style-type: none"> • No SRA requirement for first responders |

Appendix III: Intrusion Detection Systems

| Systems | Definition | Possible Uses | Questionable Uses | Dependencies |
|---------------------------------------|---|---|--|---|
| Infrared motion detector | A device that detects a change in ambient temperature (heat sensor) | -Inside registered areas -Along a hall that leads to registered areas -Doors that lead to registered areas -Storage freezers | -Areas where things are heated (warming) - Very large areas | Ensure that system is focused at key areas and not 'randomly' located throughout entity |
| Contact Switches | Devices that alarm when a circuit is broken (door or window opened) | -Inside registered areas -Along a hall that leads to registered areas -Doors that lead to registered areas -Storage freezers | Areas with glass windows or doors that provide direct access to registered area | Ensure the emergency exit has an alarm and windows have sensors |
| Broken Glass Sensors | A device that detects the sound frequencies generated by breaking glass. | -Laboratories with glass windows which provide access to registered space | -Entities where there are frequent severe storms -Entities with synthetic windows | Ensure all the doors also have a sensor. |
| Acoustic Motion Sensor (emits sounds) | An active device that detects motion by transmitting sounds that reflects off objects | -Inside registered areas -Along a hall that leads to registered areas -Doors that lead to registered areas -Storage freezers | -Animal rooms -Rooms where equipment is continuously left on or after work hours (i.e., shakers, incubators) - Very large areas | Ensure that system is focused at key areas and not 'randomly' located throughout entity |
| Acoustic Sensor (listens for sounds) | A passive device that monitors the sounds to determine when an intrusion occurs and/or to determine the nature of the intrusion | -Inside registered areas -Along a hall that leads to registered areas | -Animal rooms - Rooms where equipment is continuously left on or after work hours (i.e., shakers, incubators) -Entities without exterior sound dampening | Ensure exterior noises do not set the alarm off (i.e., animals in the laboratory next door) |

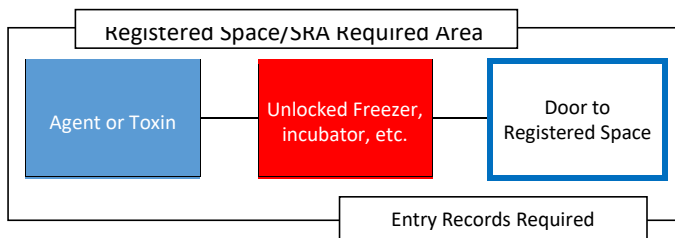
Appendix IV: Intra-Entity Transfer Template

| SELECT AGENT/TOXIN | STRAIN / CHARACTERISTICS | QUANTITY TRANSFERRED | DATE OF TRANSFER | SENDER | RECIPIENT |
|--------------------|-----------------------------|-------------------------|---------------------|--------|-----------|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

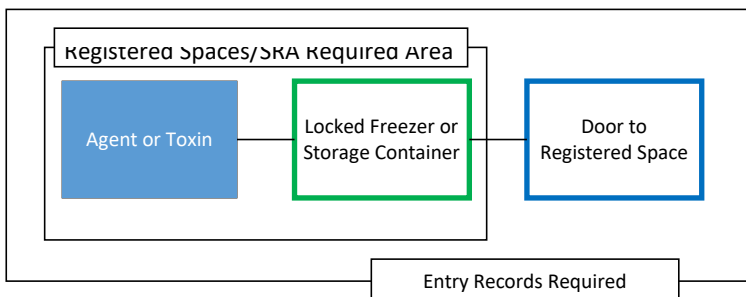
Comments:

Appendix V: Scenarios (Non-Tier 1 Barriers and Access Controls):

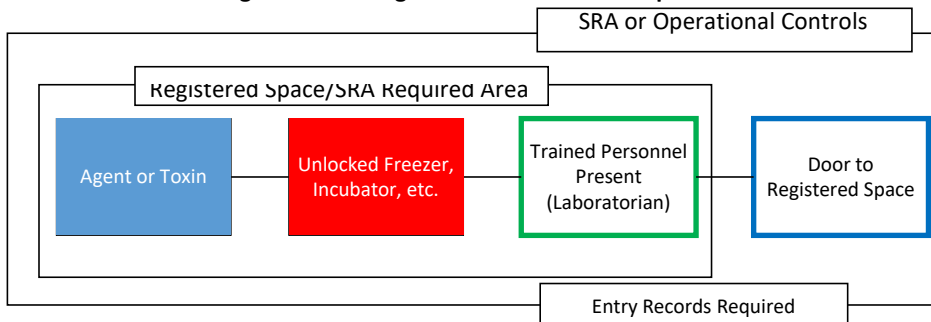
Scenario 1: Typical Working Facility



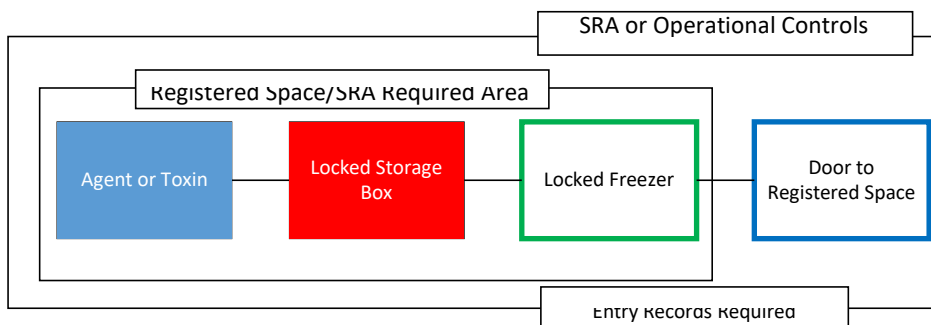
Scenario 2: Storage Only



Scenario 3: Working with Select Agent or Toxin in Shared Space



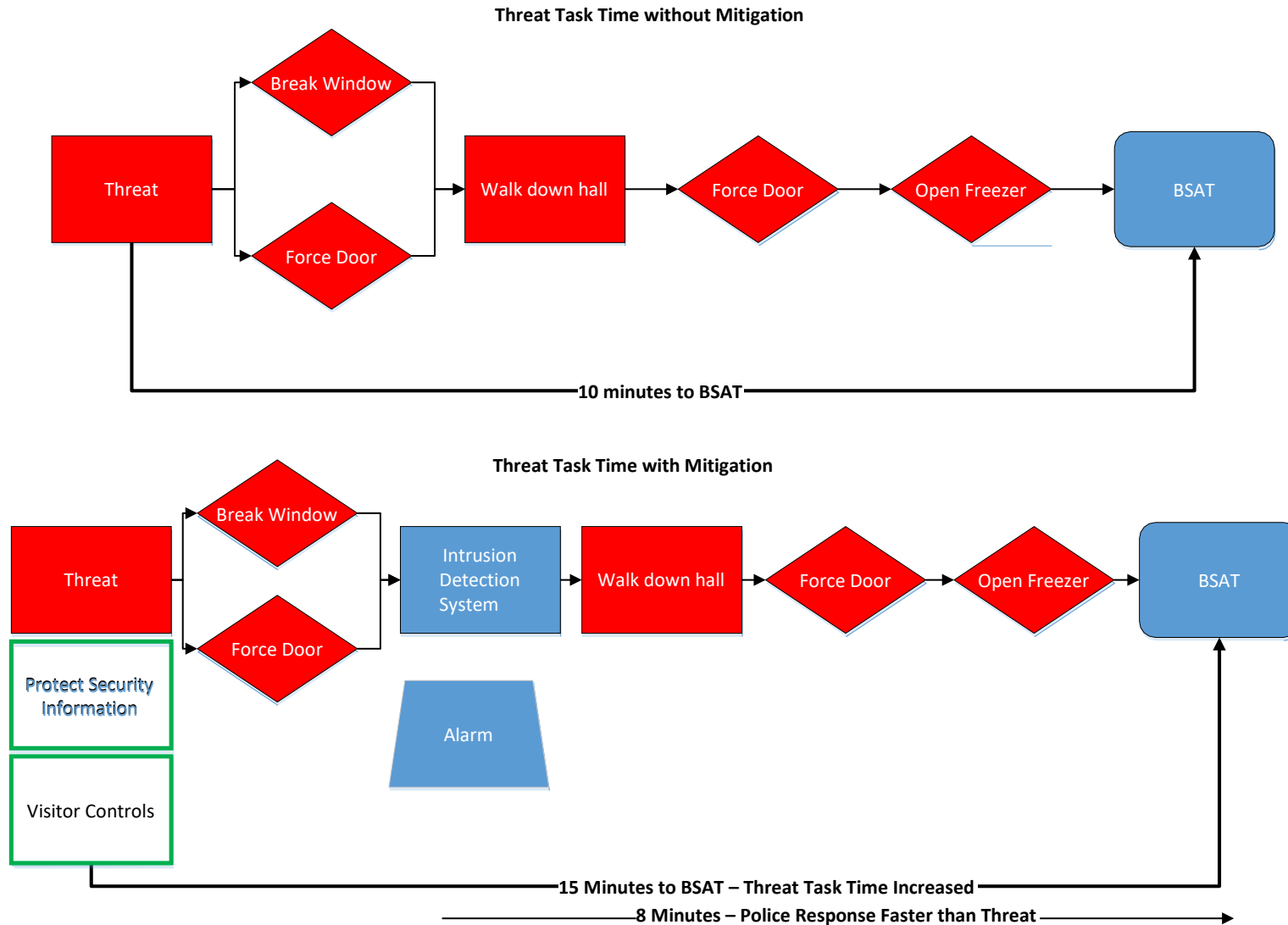
Scenario 4: Locked Box Inside Freezer



Operational controls are controls in place specifically to prevent unauthorized access to any select agent or toxin. Appropriate operational controls are based on the nature of all work in the registered area, the physical features in the area, and the entity's risk assessment.

Outsider Threat

Barriers deter but cannot be relied on to stop an outsider. The outsider cannot be stopped by locks, doors or other barriers, only delayed. The only thing that will stop an outsider is a response force.



Select Agent or Toxin Inventory Template

AGENT OR 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: _____

Inventory Audit Conditions

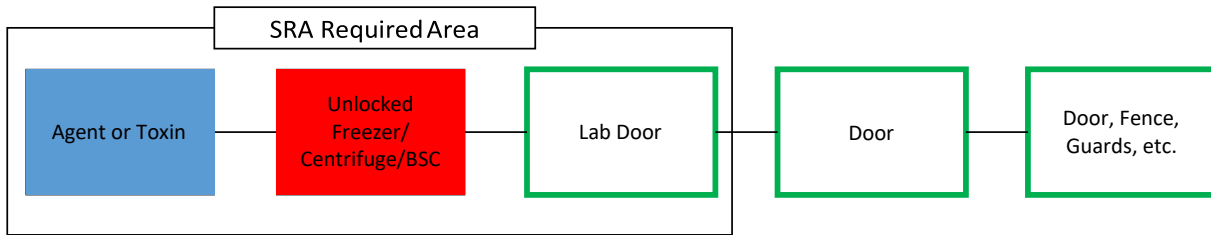
| Circumstance | Suggested audit |
|--|--|
| Emergency movement inside the same registered area | Audit not required if there is no evidence loss or theft. |
| Emergency movement to a different registered area | 100% check of sealed containers for indication of tampering. 10% of the entire inventory which is not sealed. Audit commences after the move is complete. |
| Loss | 100% of all samples in that PI's collection and/or any other inventory in shared freezer space. Audit commences immediately (within 48 hours) after the event. |
| Theft | 100% of all samples in that PI's collection and/or any other inventory in the shared freezer or space. Audit commences immediately (within 48 hours) after the event. |
| Addition or removal of a PI from the registration. Or Transfer of inventory from or to another PI. | 100% of the samples in that PI's collection. 100% check of sealed containers for indication of tampering. Audit commences as soon as possible after the arrival/removal of the investigator or as soon as practical thereafter. |
| Planned movement to a different registered area | 100% check of sealed containers for indication of tampering. 10% of the entire inventory which is not sealed. Audit commences after the move is complete. |
| Planned movement to a different registered area a different building, campus, facility. | 100% of all samples manipulated since the last inventory. 100% check of sealed containers for indication of tampering. Audit commences after the move is complete. |

Entities may also choose to consider inventory when following conditions occur:

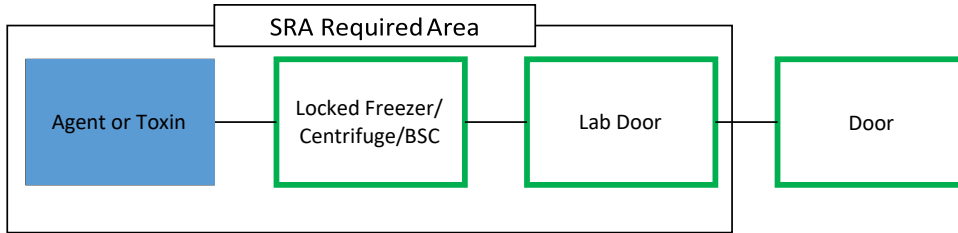
| Condition | Inventory |
|---|--|
| Laboratorian or support staff removal from registration | 10% of the samples in that PI's collection that the individual worked with. 100% check of sealed containers for indication of tampering. Audit commences as soon as practical after the person is removed. |
| Destruction of agents | 100% of the agents being destroyed. |

Tier 1 Barrier Scenarios

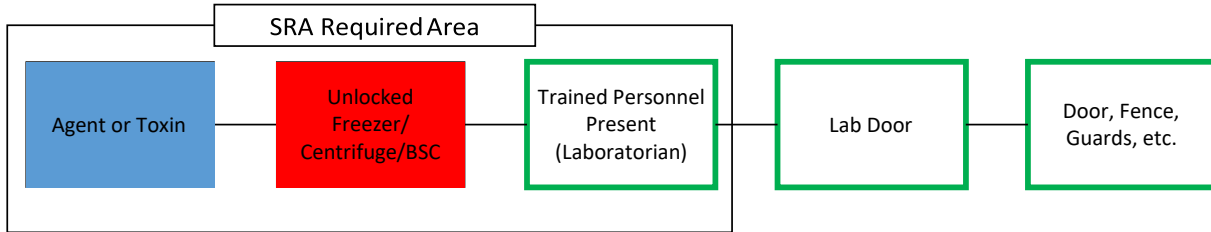
Scenario 1: Typical Working Facility



Scenario 2: When in Storage



Scenario 3: Working with Agent or Toxin



Scenario 4: Locked Box

