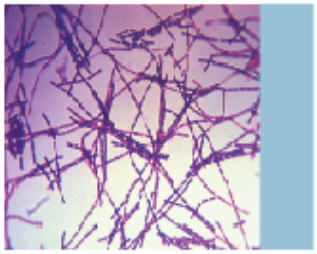
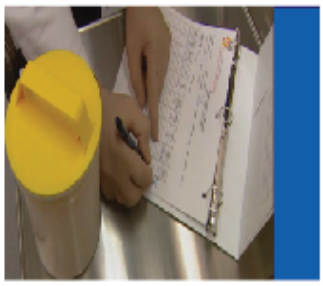




Security Guidance for Select Agent or Toxin Facilities

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

01 October 2012

Centers for Disease Control and Prevention (CDC)
Division of Select Agents and Toxins
Animal and Plant Health Inspection Service (APHIS)
Agriculture Select Agent Program

Preface

Intent: The intent of this document is to provide practices and procedures that entities may consider in developing and implementing the written security plan required by the select agent regulations (7 CFR part 331, 9 CFR part 121, and 42 CFR part 73). The ideas and suggestions provided in this document do not constitute or establish minimum acceptable standards that automatically meet the requirements of section 11 (Security) of the select agent regulations.

This guidance document supersedes the "Select Agents and Toxins Security Information Document", dated March 8, 2007.

Key changes from the last version:

- Additional guidance is provided for entities registered for Tier 1 biological agents and toxins.
- Additional guidance is provided on what measures should be considered to achieve "graded" security.
- A section that addresses security program management considerations and requirements.
- The concepts of "risk" and "risk management" are updated to reflect current generally accepted security standards.
- The section that addresses "Information Security" has been removed and has become its own guidance document.
- Addition of new appendices covering Intrusion Detection Systems (IDS) and access control.

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

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 pose to animals 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 is (1) sufficient to safeguard the select agent or toxin against unauthorized access, theft, loss, or release; and (2) designed according to a site-specific risk assessment, providing graded protection (*See section 11 (Security) of the select agent regulations).*[3]

The purpose of this document is to assist the entity in developing and implementing its site-specific security plan. This document is organized by security function/system with the regulatory citation at the end of the section heading. We have addressed any additional Tier 1 BSAT specific requirements at the end of the section. As used in this document, the word "must" means a regulatory requirement. The use of the word "should" or "consider" is a suggested method to meet that requirement based on generally recognized security "best practices." We recognize that implementation is performance based and that an entity finds other ways to meet the regulatory requirement.

This document addresses the 2012 amendments to the select agent regulations with regard to security with one exception. Entities with Tier 1 BSAT have additional pre-access suitably and ongoing suitability assessment requirements which are addressed in the "Guidance for Suitability Assessments" available at www.selectagents.gov.

Key considerations in developing an effective security system:

- It results from collaboration between scientific and security personnel.
- It is built upon well documented operational processes. Security should re-enforce existing processes. In order to do that, existing processes must be defined.
- It accounts for and secures all biological select agents or toxins from creation or acquisition to destruction.
- It complements other plans such as safety, disaster recovery, continuity of operations and others.
- It does not violate any laws. This includes the Americans with Disabilities Act, OSHA safety standards, and local building and fire codes.
- Personnel are trained so every person understands his or her responsibility.
- It accounts for the primary and secondary impacts of a threat's action, to include impacts they have beyond the entity.
- 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.

---

[1] Section 351A(e)(1) of the Public Health Service Act (42 USC 262a(e)(1).
[2] Section 8401(e)(1) of the Agriculture Bioterrorism Protection Act of 2002 (7 USC 8401) .
[3] For the 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.

Table of Contents

Considerations when performing a risk assessment and developing a site specific security plan (Section 11(b)) 1

Security Program Development and Management (Section 11) 5

Physical Security ((Section 11(c)(1) and 11(d)(3)) 8

Personnel Security (Section 10) 14

Operational Security (Section 11(d)(3)) 15

Inventory Control Measures (Sections 11(c)(1) and(2) and 17) 16

Understanding and Complying with Security Procedures/Training (Sections 15, 11(f) and 11(d)(7))19

Inspection of Suspicious Packages (Section 11(d)(4)) 20

Shipping (Section 11(c)(10)) 21

Intra-entity Transfers (Section 11(d)(5)) 22

Reporting requirements (Section 11(c)(8) and 11(d)(7)) 23

References 24

Appendices 25

Appendix I: Sample Scenario Diagram 26

Appendix II: Risk Assessment Methods 28

Appendix III: Comparison of Access Control Devices and Systems Which are Used to Control Access to Select Agents and Toxins 29

Appendix IV: Tier 1 Barrier Scenarios 30

Appendix V: Intrusion Detection Systems 31

Appendix VI: Example of a Select Agent Inventory Form that Captures the Requirements Listed in Section 17 32

Appendix VII: Example of a Toxin Inventory Form that Captures the Requirements Listed in Section 17 33

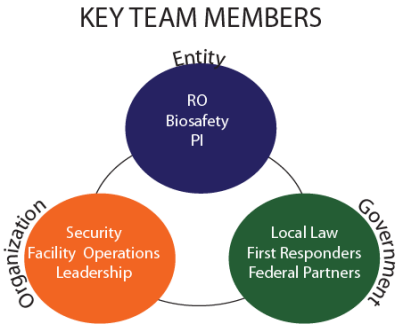
Appendix VIII: Suspicious Package 34

Appendix IX: Example of an Intra-Entity Transfer Form that Captures the Requirements Listed in Section 17 35

Appendix X: Shared areas where Tier 1 BSAT are used or stored 36

Considerations when performing a risk assessment and developing a site specific security plan (Section 11(b))

Entities should consider forming a team of both entity subject matter experts (SMEs), supporting SMEs 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 organization and governmental members as well.



Entity personnel should provide:

- Standard Operating Procedures (SOPs), policies and other organizational controls which can re-enforce or be affected by security measures.
- Public health consequences of the select agent and toxin.
- Operational requirements.
- Value of the select agent or toxin work to the organization.
- Knowledge of current security systems.

Facility and support personnel should provide:

- Facility wide security measures.
- Personnel hiring practices (background checks, reference checks, education verifications).
- Planned upgrades to the facility.
- Constraints which affect security (fire code, ordinances, federal laws).

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

- 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 development of the plan. The team should meet annually as part of the security plan review.

Entities Registered for Tier 1 BSAT must have the following additional requirements (Section 11(f)(2))

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, relevant information which may affect the security plan. They are also required to describe procedures on how the RO coordinates efforts with the entity's safety and security professionals to ensure security of Tier 1 select agents and toxins and share information as appropriate.

Specific considerations with the Site Specific Risk Assessment and Graded Security (Section 11(b))

The cornerstone of a good security plan is a 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, of those 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 safety plan.

"Risk" comes from the interaction of threats/hazards (T), a vulnerability (V) and a consequence (C). There are many ways to capture these interactions, including qualitative, quantitative, probabilistic, and others. However, any assessment which captures and relates these interactions is sufficient. There are tools available to assist the entities at http://www.selectagents.gov/.

Below is a discussion of threat, vulnerability and consequence.

1. Understanding and Assessing Threats. A threat is a person or organizations whose actions may cause the theft or release of a select agent or toxin. The threat can be an insider with approved access or an outsider. The threat may target the agent directly (theft), may cause damage to the entity as the result of their action (Animal Rights Terrorists damaging containment), may act on their own or may collude with others. Threats can be captured as a 'probability of attack.' Threats are generally determined 3 different ways. Resources that are useful when determining threats include:
    a. Expert opinions. Entities are encouraged to reach out to law enforcement and other experts to determine threats.
    b. A modeled threat (Design Basis Threat or DBT). An expert or group of experts model 'threats' in general. This is most common in federal and state facilities; however, the capability may be present in large entities.
    c. Historical data, including statistics on past local events (crimes), terrorist events worldwide, social sciences research into terrorists' behavior, official accounts, and/or terrorists 'own writings about motivation and intent.

2. Understanding and Assessing Natural Hazards. For a tool to help you to determine if you are in a risk area for natural hazards, see the Incident Response Guide at www.selectagents.gov. As with threats, entities should assess the impacts of the hazard to the select agent or toxin as well as the entity as whole.

3. Understanding and Assessing Vulnerabilities. Vulnerability is the relative susceptibility of select agents or toxins to a threat or natural hazard. Vulnerabilities are where a threat capability can be applied which results in the theft or release or the agent. Vulnerabilities are where a natural hazard can impact the select agent or toxin. Vulnerabilities are often captured as "probability of effectiveness" (PE) of a particular system. There are many ways to determine vulnerability that

range from 'discussion' to 'mathematical simulation' depending on the information available. Below are some best practices in conducting vulnerability assessment:

a. Exercises/after action reviews
b. Assessments by subject matter experts (SMEs)
c. Scenarios and path development with SMEs and entity members (see **Appendix I**)
d. Modeling (primarily with natural hazards)
e. Simulations (primarily with natural hazards)

4. Understanding and Assessing 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:
   a. The communicability of the agent
   b. The agent's mortality and morbidity
   c. Present availability of known countermeasures to the agent or toxin
   d. 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 handled in a propagative manner 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 what a threat "could" do to make an agent more virulent. Current characteristics are sufficient for this assessment.

5. Assessing Risk. As long as the interactions of threat, vulnerability and consequence are related in the risk assessment, it will be sufficient. 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 **Appendix II** for Risk Analysis Methods from the National Academies of Science and examples of qualitative risk assessment. For guidance on mitigating the impacts of a natural hazard, see the Incident Response Guide at www.selectagents.gov.

Communicate the risk:

After the risk assessment is completed, key entity leadership (such as the Principal Investigator (PI), RO, Alternate Responsible Official (ARO), Security Staff, Institutional Biosafety Committee, and Laboratory Management) should determine if the current risk level is acceptable. If the risk level is deemed unacceptable, then the entity is obligated to 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. The entity can:

- Employ additional security measures.
- Change the work with the select agent or toxin.
- Decrease the quantity of toxin on hand, possessing only the amounts necessary for the work.
- Change how the select agent or toxin is stored (i.e., not lyophilized).
- If the 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 at least yearly or as the threat changes.

Security Program Development and Management (Section 11)

A security program implements risk management goals. Security program management consists of the plans, policies, people, processes/procedures and performance assessments that support the security system.

Plans (Section 11(a) and (b))

Entities are required to develop and implement a written site-specific security plan. A security plan is a documented systematic design for implementing security goals. It is a blue print for how an entity secures its select agents and toxins. It establishes the performance goals for the system and metrics for performance. As stated in the select agent regulations (section 11 (b)), "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.

Plans also include agreements or arrangements with extra-entity organizations such as with local law enforcement.

Reviews, Evaluating Effectiveness: The select agent regulations require that the security plan be reviewed on an annual basis. A security plan should be reviewed after any security incident, as well as after drills and exercises, and revised as needed (Section 11(h)).

Entities Registered for Tier 1 BSAT should have the following enhancements:

An effective security program for Tier 1 BSAT should include roles and responsibilities for security management, and the possible designation of a Security Officer to manage the entity's security. It 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 (i.e., a 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 (i.e., alarm).
- How the entity screens visitors.
- A documented security awareness training program for, at a minimum, all employees listed the entity's approved registration that include regular insider threat awareness briefings on how to identify and report suspicious behaviors that occur inside the laboratory or storage area.

Policies

Entities should consider establishing specific policies which support their plan. Security policies, for purposes of this document, are documented strategies, principles, or rules which the entity follows to manage its security risks. They are a clear means of establishing behavioral expectations. They cover the spectrum from directives to standard operating procedures. As part of security program management, the entity should consider formally documenting security policies covering all operational controls (See p. 16: Inventory Control Measures).

- Background checks and other personnel security measures. If practical, these policies should be vetted through the entity's legal and human resources department. Additional guidance on suitability assessment can be found at www.selectagents.gov.

People

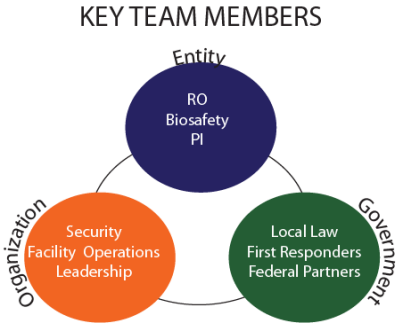
Entities should consider who will implement the plan. People are the core of any security system. The security program should define an individual's roles and responsibilities in the system and solicit their input for improvements.

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

- 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.

Entities Registered for Tier 1 BSAT must have the following enhancements:

Entities registered to possess Tier 1 BSAT must include in their security plan a component for all professionals involved in BSAT safety and security at an entity to share relevant information with the RO in order to coordinate their efforts. (Section 11(f)(2))



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.

Processes and Procedures

Processes and procedures are how people implement the leadership's plan. They are more than standard operating procedures (SOPs) and policies; they are how well the SOPs are implemented, followed, and supervised.

Entities should consider integrating security processes and procedures into existing safety, incident response and other plans and policies. Security procedures should never be done in a vacuum. Security procedures should complement existing biosafety policies. When developing a security policy, consider having the Biosafety Officer, facility manager, and organizational leadership participate in development of the policies. Entities should consider the security impacts of:

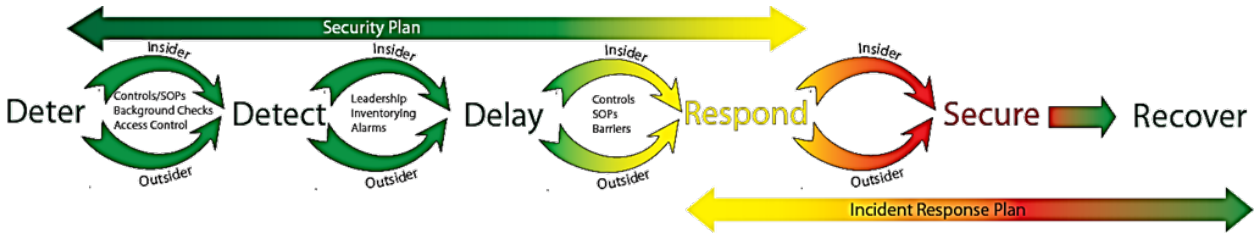
- Safety SOPs.
- Hiring policies (including background checks).
- Inventory access policies.
- After hours work policies.

Performance Assessment

Entities should consider assessing the performance of their security systems measures as part of the annual review of the plan. Entity leadership or security team should define the performance requirements of the security system, assess how well it is performing and determine how to improve it. This includes:

- Testing the system.
- Audits.
- Adjusting the system based on changes to threats, vulnerabilities or consequences.
- Adjusting the system based upon exercise or events to address new changes.
- Providing resources based on requirements.

Physical Security ((Section 11(c)(1) and 11(d)(3))



The Security Plan must 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; creating sufficient time, between detection of an attack and the time when the attack becomes successful, for response force to arrive. It should include:

- Security barriers which both deter intrusion and deny access (except by approved personnel) to the areas containing select agents and toxins. This may be perimeter fences, walls, locked doors and security windows. This can also be a trained person (i.e., security guard, trained laboratorians, or escorts).
- Safety measures and other environmental factors which increase security. An access or locking system which denies access to the select agent or toxin. This may include mechanical locks, card key access systems or biometrics. Consider 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, is secured at the same level.
- A procedure or process to keep the number of nuisance alarms to a minimum.

The physical security system must control access to the select agents and toxins. An individual will be deemed to have access at any point in time if the individual has possession of a select agent or toxin (e.g., ability to carry, possess, use, transfer, or manipulate) or the ability to gain possession of a select agent or toxin (section 10(b) of the select agent regulations). Based on the site-specific risk assessment, the entity should control access to the facility and to registered areas within the facility beyond the registered area, limiting access to the select agents and toxins to only those individuals with access approvals from the HHS Secretary or Administrator.

The entity must:

Create an Access Control System (Section 11 (c)(2) and 11(d)(1): Create a system which limits access to select agents and toxins to those approved by the HHS Secretary or APHIS Administrator. This should:

- Include provisions to limit unescorted/unrestricted access to the registered areas to those who have been approved by the HHS Secretary or 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.
- Access logs should be reviewed and updated regularly.

- 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.
- **Appendix III** addresses access control measures and security risk assessment (SRA) requirements in detail.

Access considerations for autoclaves

Individuals loading an autoclave with select agents or toxins must be approved for access by the HHS Secretary or Administrator and, if a Tier 1 BSAT, have undergone pre-access suitability and are subject to ongoing suitability assessment. They should check the autoclave to ensure it is loaded properly and comes up to temperature and pressure within guidelines. Once that is complete, the person does not have to remain for the full cycle.

Individuals unloading the autoclave may not require additional personnel security measures. At the end of the cycle, the person removing material from the autoclave should verify the cycle completed within normal parameters. If it has, the person removing the material does not require an SRA nor has additional suitability requirements. However, if the run was not completed with normal parameters, the personnel security requirements remain. RO should be notified and the material removed by an individual approved for access by the HHS Secretary or Administrator and, if a Tier 1 BSAT agent, undergone pre-access suitability and are subject to ongoing assessment.

Provide provisions for escorts (Section 11(d)(2)): The security plan must contain provisions which allow non-approved persons access only when escorted by an approved person. The escort must be dedicated (no other duties during the time he or she is serving as an escort) to observing the escorted person and must understand what to observe for (i.e., accessing select agents and toxins). Non-approved persons are not allowed to put "hands on" or have access to an agent, even if escorted by an approved person.

Record Access (Section 17(a)(4)): An access log to record information for all entries, including the name of the individual, the name of the escort (if applicable), and date and time of entry must be maintained. If an electronic log is utilized, the database controlling access must be capable of maintaining three years of access information. Entry records must be safeguarded to prevent alterations and be retained for 3 years (Section 17(c) of the select agent regulations).

Control Access of Support Personnel for Maintenance, Cleaning, and Repair (Section 11(c)(3)): The security plan must state how cleaning, maintenance and repairs will be accomplished in areas where select agents and toxins are possessed or used. In allowing maintenance, cleaning, or repair personnel (whether in-house or contract services) into a registered area, an entity should: 1) use only approved individuals; or 2) provide an 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, if applicable.

Prevent Sharing Access Credentials (Section 11(d)(6)): 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 approved person's access card
- Sharing a key card, password or badge.

Sharing access makes accountability very challenging. When access is captured electronically and personnel "piggyback" or "tailgate," their access is not recorded, creating vulnerabilities.

Reporting and Removing Unauthorized or Suspicious Persons (Section 11 (d)(4) and 11(d)(6)): An "unauthorized person" is one who 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, challenging and removing unauthorized and suspicious persons. It must also require follow-up actions such as reporting the information to the RO, the RO providing an incident report to entity security personnel, and possibly contacting local law enforcement agencies and the Federal Select Agent Program as appropriate.

Unauthorized and suspicious persons attempting to gain entry into registered areas without proper credentials should be identified, challenged and removed immediately and the RO notified. It is important for an entity to train laboratory personnel on what to do when a suspected unauthorized person attempts to access registered areas.

The entity should consider:

- Integrating an access control measure (i.e., card key) into an alarm system which 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 which clearly identifies who does and does not have access to select agents and toxins and training on how to remove unauthorized personnel (e.g., procedures for notification of security personnel and/or local law enforcement).

Address the Loss and Compromise of Access Credentials (Section 11(d)(7)): The security plan must include the reporting mechanisms for loss or compromise of keys and access cards and how they will be replaced. To be effective this requires prompt and immediate attention to ensure there is no compromise of security. The entity must:

- Require the immediate notification if a key or access card is lost.
- Evaluate whether locking mechanisms need to be replaced if keys are lost.
- Describing the procedure for deactivating access for a lost or stolen access card and how entry logs will be checked.
- Describe, in cases where a badge system is used, the means of disseminating information concerning the loss of a badge in order that all personnel know the badge may have been compromised.

Address Procedures for Personnel Changes (Section 11(c)(5)): The security plan must describe the procedures for changing access after personnel changes in order to prevent access by personnel who have previous 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 when people leave or change duties.

Separate storage or laboratories that contain select agents and toxins from public areas of a building (Section 11(d)(8)): The storage or laboratories that contain select agents and toxins must not be publicly accessible. Public areas are, as the name suggest, places where the general public may congregate or transit in the vicinity of registered spaces.

Entities Registered for Tier 1 BSAT must have the following enhancements:

Three Barriers (Tier 1 only) [Section 11(f)(4)(iv)]
For entities registered to Tier 1 BSAT, the select agent regulations require three barriers (section 11(f)(4)(iv). A barrier is a physical structure that is designed to prevent access by unauthorized persons. Cameras, security lighting and IDS are not considered security barriers because while they may monitor access, they cannot, by themselves, prevent access. These security barriers must be identified on the entity's registration and discussed in the security plan (Sections 5A and 6A of APHIS/CDC Form 1).

Examples include:

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

Personnel who are trained to identify and respond to suspicious activities can be a security barrier. Persons who receive 'insider threat,' 'suspicious person' training or similar training along with response procedures (i.e., calling security, 911, etc.) are considered 'trained personnel.' Therefore, when they are physically present, they are considered security barriers. This information must be included in the required annual refresher training in accordance with section 15 (b) of the Select Agent Regulation.

Each security barrier must add to the delay in reaching the secured areas where select agents and toxins are used or stored. Most security barriers, in and of themselves, do provide additional delay to forced entry. Entities should also consider the delay they have on covert entry (e.g., faked badges, etc.).

All access points, including emergency exits, must be secured. This means that 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 tamper-evident tape on containers used for long term storage.

The final security barrier must limit access to the select agents and toxins to personnel approved for access by the HHS Secretary or Administrator. Also, per CFR Section 11(f) (4) (i), 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 assessment. Access records can be used to show that only approved personnel have accessed the final barrier (and the name of the escort if required). See **Appendix IV** for additional barrier scenarios.

Intrusion Detection System (Tier 1 only) [Section 11(f)(4)(v)]
All areas that reasonably afford access to the registered suite/room must be protected by an intrusion detection system (IDS) unless the registered area is physically occupied. An IDS is a system that 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. See **Appendix V** for detailed discussion of different types of IDS systems.

Personnel monitoring the IDS must be capable of evaluating and interpreting the alarm and alerting the designated security response force or law enforcement. This may be personnel employed by the entity (an alarm or security operations center), contracted alarm company, local law enforcement or a military police unit. Depending on the system, it may also be dedicated entity personnel.

If the entity contracts monitoring of its IDS from a service provider and local law enforcement respond, the entity should consider coordination with local law enforcement to assist local law enforcement 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 that possess select agents and toxins are encouraged to discuss the consequence of theft of a select agent or toxin with local law enforcement so law enforcement can appreciate the seriousness of the threat. From an entity's viewpoint, it is important that local law enforcement understand that an alarm at an entity housing select agents and toxins should not be regarded as a "typical" property crime.

Response Time (Tier 1 only) [Section 11(f)(4)(viii)]
The entity must determine the response time and describe the provisions or procedures for the response force in the security plan. Response time is the elapsed time, measured under typical conditions, from the time the response force is notified to the time the response force arrives at the entity.

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

A reasonable target for response time is 15 minutes. This is based on Department of Defense adopted standards for protecting high consequence assets. Entities have two options to meet the requirement. The first is to determine that the response time for the response force is less than 15 minutes. This can be achieved in multiple ways. For example, an entity can:

- Enter into a formal agreement with local law enforcement.
- Discuss 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).
- Conduct an exercise with local responders.

The second is to calculate the delay time provided by entity security barriers and compare it to the expected response time of the response force. This is a matter of getting the typical response times from the responding personnel and comparing it to the delay times determined through scenarios. If the delay times are greater than the response time under typical conditions, it will meet the standard. Because the delay time is threat dependent, entities are strongly encouraged to coordinate with local law enforcement and/or federal partners to assist with threat capabilities. 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.

Though not required, entities should consider the effect of natural hazards and other factors when addressing response times. For example, an earthquake may trigger the alarm but may also impact local law enforcement's capabilities to respond to alarms. A mandatory evacuation for hurricane may prevent the response force from arriving. A tornado may both cut the power to the IDS triggering an alarm but may also block the roads. Entities are strongly encouraged to address these matters in their incident response plans.

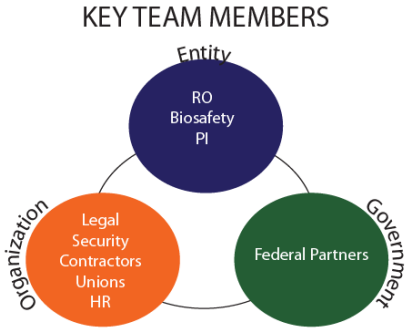
Key points: If local law enforcement is the response force, it is critical they understand that an IDS which is triggered at an entity registered with the Federal Select Agent Program is not a typical property crime. Some police do not respond to property crimes; others only respond as they get time. You would want your entity to be a 'higher' priority response.

Access control power failures and personnel changes (Tier 1 only) [Section 11(f)(4)(vii)]
For powered access control systems, the entity must describe procedures to ensure that security is maintained in the event of the failure of the access control system due to power disruption. This may include locks "failing secure" (locked), personnel/guard forces, backup generators or other similar features. For example, if power is lost and the door locks (even if they can be opened only from the inside), then it meets this requirement. If power is lost and door unlocks (it can be open from the outside), then it does not "fail secure."

Depending on access controls, the entity may also want to consider changing alarm codes when personnel change. Former employees with the capability to deactivate the IDS may pose vulnerability.

Personnel Security (Section 10)

Personnel security measures are key to mitigating the 'insider' risk. A good personnel security program re-enforces honesty and integrity while identifying those who may pose unacceptable risks.



In some cases, an entity's personnel security is already in place but outside the control of the RO. This is acceptable and often times a much more effective means of conducting personnel security. The RO, however, must be aware of these procedures.

The security plan should describe what personnel security measures are in place. These measures should assess the workers based on their level of responsibilities within the entity. Personnel security measures should be based on insider threats from the site specific security risk assessment.

Personnel Suitability Assessments (Tier 1 BSAT only) [[Section 11(f)(1) and 11(f)(3)] Personnel with access to Tier 1 BSAT must have additional pre-access suitably and ongoing assessment requirements. See the "Guidance for Suitability Assessments" on www.selectagents.gov for additional information.

Security Risk Assessment (Section 10)
A SRA is the method used by the Federal Bureau of Investigation to identify whether an individual is within any of the prohibited or restrictive categories specified in section 10 of the select agent regulations.

Additional Personnel Security Considerations
Based on the site specific risk assessment, the entity may determine risks that are best managed through additional personnel security measures. These are at the discretion of the entity and subject to many local, state and federal laws. Also, entities should keep in mind parts of a typical background check may already be in place for non-security reasons. For example, verification of a person's educational background and contacting a person's references may be accomplished as part of the hiring process.

The registered entity may also consider continuing evaluation. Some approaches may include:

- Self-reporting (an environment which encourages honesty and self-help).
- Peer reporting (an environment where team members help each other).
- Supervisor observation (to make sure people perform in approved manner).
- Periodic rescreening including the SRA and other background screens.

Suspicious activity or behavior to consider includes:

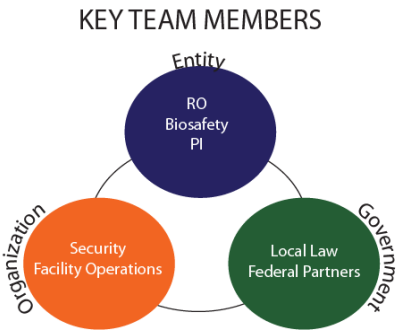
- Personnel who deliberately or routinely violate security or safety procedures.
- Personnel who threaten or support those who threaten to do harm to other people.
- Personnel who do not properly account for material.
- Personnel who work after hours without authorization or apparent reason.
- Personnel displaying nervous or evasive behavior when accounting for material.

This goes beyond laboratorians and includes support staff with access to select agents and toxins.

Operational Security (Section 11(d)(3))

Operational Security: Effective operational security builds on existing operational procedures but mitigates threats based on site-specific risk assessments. Operational security is controls and procedural measures which are put in place or modified to control access to access to select agents and toxins; they prevent the unauthorized access, theft or loss a select agent or toxin. The entity may choose to consider:

- Limiting duty hours/after hour operations.
- Training personnel on their responsibilities for securing select agents and toxins.
- Badging procedures, including displaying badges at all times unless in personal protective equipment.
- Removing signs that indicate where the select agents and toxins are stored (unless required by law, regulation, or as part of a biosafety program).
- Two personnel present while working in with select agents and toxins or review of security video by laboratorians or other trained personnel.
- Screening of visitors, packages, vehicles, etc. as part of allowing them access.
- Requiring that individuals refrain from sharing information about the entity's security.



Entities should assess lack of adherence to operational security measures because this is a key alert to potential insider threat activity.

Work hours (Tier 1 BSAT only) [Section 11 (f)(4)(ii)]:
Entities registered to possess Tier 1 BSAT are required to have procedures that limit access to laboratory and storage facilities outside of normal business hours to only those specifically approved by the RO or designee(s).

This requirement is not intended to limit work, only to make an entity aware of the work that is occurring. If the RO is aware and access is limited (card-key limitations, key control), then it is sufficient to meet the regulatory requirement. If any person on the registration can access Tier 1 BSAT after hours on their own, it is not. These procedures must also be addressed in the security plan.

Screening (Tier 1 BSAT only) [Section 11 (f)(4)(iii)]:
Entities registered to possess Tier 1 BSAT are required to have procedures for screening visitors, their property, and vehicles at the entry and exit points to the areas registered for Tier 1 BSAT, or at other designated points of entry to the building, facility, or compound based on the entity's site-specific risk assessment.

Screening consists of confirming a person's need to visit and his/her identity prior to allowing access to areas registered for Tier 1 BSAT. The method and detail is determined by the site-specific risk assessment. Screening can be done by any trained person at any point prior to accessing the area registered for Tier 1 BSAT.

Entities are also required to document in the security plan their procedures for visitors and property screening. These procedures should be based on the site-specific security risk assessment along with applicable laws.

Inventory Control Measures (Sections 11(c)(1) and(2) and 17)

Effective inventory control measures for select agents and toxins in long term storage can be a very effective way to 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 or infected with a select agent.
- An accurate and current inventory for each select agent or toxin held 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 acquisition to destruction.
- Accounting for select agents and toxins as they are withdrawn from long term storage and returned to storage.

An inventory audit is an examination of a portion of the inventory or collection sufficient to verify inventory controls are effective. This guidance does not apply to inventories conducted in accordance with Section 17 for further information on long term storage inventories (S*ee* the "Guidance on the Inventory of Select Agents and Toxins" which can be found at www.selectagents.gov). This only applies to audits required by section 11. Entities must conduct complete inventory audits of affected select agents and toxins in long-term storage when any of the following occur:

- Upon the physical relocation of a collection or inventory containing select agents and toxins. This includes moving a collection or inventory into a new facility or into a new storage location within the same facility.
- Upon the departure or arrival of a principal investigator for select agents or toxins under the control of that principal investigator; or
- In the event of a theft or loss of a select agent or toxin, all select agents and toxins under the control of the principal investigator that suffered the theft or loss.

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

1) The timing of the inventory audit. See recommended objectives below.
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.

The Federal Select Agent Program recommends the following objectives:

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-

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.

Records of audit must be kept in accordance with section 73.17 (c). The changes to the inventory must be recorded in accordance with section 73.17 (a) as well.

Inventory control measures may include storage in tamper-evident storage containers. They are especially useful when the material is in storage without being accessed for a long period of time (archival collections, while laboratories are under renovation). The material should be inventoried initially then the material is sealed in the container. The entity can check the 'seal' for evidence of tampering instead of inventorying the entire container. Note: as a practical matter, an entity will either have to retain the record of the initial inventory record past the minimum 3 year select agent regulatory requirement, or the entity will have to re-inventory the select agents and toxins if the record is to be destroyed on a 3 year cycle. If the inventory record of what is inside the container is lost or destroyed, the container must be re-inventoried.

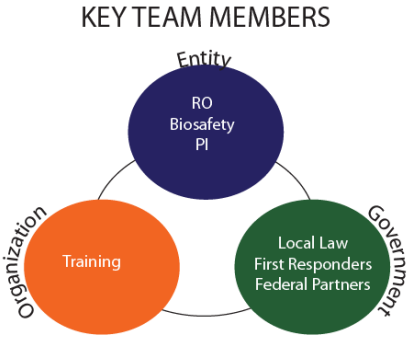
Examples of tamper evident material:

Tamper Evident Tape (useful on boxes and storage devices).	Tamper Evident Seal (useful on freezers and other locking storage devices)

See **Appendix VI** for an example of a select agent inventory form and **Appendix VII** for an example of a select toxin inventory form.

Understanding and Complying with Security Procedures/Training (Sections 15, 11(f) and 11(d)(7))

Before an individual has been granted access to select agents and toxins, it is important that the individual understands and follows all the security protocols established by the entity. Each registered entity is required to provide security training to all individuals with approved access. This security training must include both initial and annual refresher training on specific security processes and procedures which control access and prevent the theft or loss of a select agent or toxin. The training must address the particular needs of the individual, the work they will do, and the risks posed by the select agents and toxins.



Annual Insider Threat Awareness Briefings (Tier 1 BSAT only) [Section 14(b)]:
For entities with Tier 1 BSAT, training must include an annual insider threat awareness briefing. An example of insider threat awareness training can be found at www.selectagents.gov.

Annual security refresher training may include, but is not limited to:

- Identifying and removing a suspicious person.
- Identifying and reacting to a suspicious package.
- Escort Procedures.
- Entity specific security policies, including:
    1. Entry access procedures and prevention of "tailgating"
    2. Preventing the sharing of unique means of access
    3. Reporting the loss or compromise of passwords
    4. How to identify and report suspicious persons or activities
    5. Inventory documentation and records management (see "Information Systems Security Control Guidance "at www.selectagents.gov)
- Response to an alarm.
- Response to other security breaches.
- Outside threat group(s).

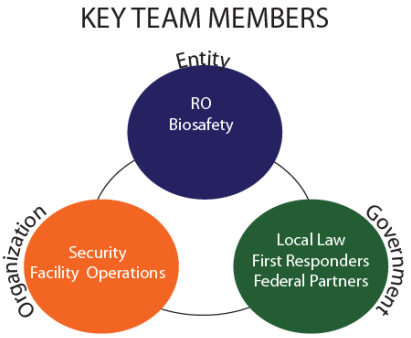
Re-training is required when the entity significantly amends its security plan. This includes processes which change how people gain access along with other significant changes to security. Significant changes may be the result of new technology (new badge reader, new IDS, new inventory control system) or new operational processes (new inventory control method, new work hour standard).

There must also be a means to verify that the employee understood the training. This may be a test or practical exercise. In the case of documentation, this can be a 'read and understood' statement.

Entities must keep records of this training and means used to verify understanding per Section17 of the select agent regulations.

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

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.

Inspection of Packages: 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 noninvasive techniques before they are brought into, or removed from the area where select agents and toxins are stored or used. Guidelines for recognizing suspicious packages are provided in **Appendix VIII.**

Shipping (Section 11(c)(10))

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.

Shipments containing select agents and toxins between entities must be authorized by the Federal Select Agent Program, and coordinated through an APHIS/CDC Form 2 and tracked so the receiving entity knows when the shipment will arrive. The package must be packaged and received by a person approved for access to select agent or toxins.

With respect to outbound shipments, the individual who packaged the BSAT for shipment must have an SRA approval. Once the select or toxin is packaged in accordance with DOT regulations and cannot be identified as a select agent or toxin, it can be passed off to a non-SRA approved person for shipping.

With respect to inbound shipments, 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 receipt must have an SRA and, if the agent is Tier 1, has gone through the entity's pre-access suitability and is subject to entitles ongoing assessment.

When received by the intended recipient, they should immediately be secured in registered space. Ideally, they are taken to the receiving laboratory. However, they may be stored in other registered space temporarily.

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 they plan to or are temporarily storing *identified* select agents and toxins packages in the area.

If select agents or toxins 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 shipment of a select agent that it had neither requested nor coordinated for, and therefore was not expecting. Upon realizing that a shipment has arrived which contains select agents and toxins, the entity must have a contingency plan to have approved personnel gain control of the shipment without delay and secure it in a registered area.

Intra-entity Transfers (Section 11(d)(5))

Intra-entity Transfer: A physical transfer of select agents or toxins that takes place between two SRA approved PIs at the same registered entity (e.g., from one PI to another).

Entities that conduct intra-entity transfers must have in their security plan a description of 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. An example: A PI removes a select agent or toxin from his long term storage and gives it to another PI. An example of an intra-entity transfer form can be found in **Appendix IX**.

Transfers accompanied by a chain-of-custody ensure that select agents and toxins will not be left unattended. If intra-entity transfers are not conducted in the entity, this is not required to be covered in the security plan.

Entities with Tier 1 BSAT must have the following enhancements to transfers (See Appendix IX for an example form)

Personnel transferring Tier 1 BSAT must ensure that individuals receiving the Tier 1 BSAT are approved by the HHS Secretary or Administrator, have gone through the entity's pre-access suitability and are subject to the entity's on going assessment.

Reporting requirements (Section 11(c)(8) and 11(d)(7))

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.

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; and describe procedures for how the entity will notify the appropriate federal, state, or local law enforcement agencies of such activity. Discussions during the risk assessment's security portion should identify who best can respond to the circumstances.

Suspicious activity of a criminal nature includes:

- Those identified in the site-specific security risk assessment.
- Insider:
  - Attempts to create additional inventory not authorized or required.
  - Attempts to "cover up" and not report inventory discrepancies.
  - Attempts to remove inventory without authorization.
  - Attempts by "restricted" persons to intentionally access registered areas containing a select agent or toxin.
- Outsider:
  - Indirect threats against the entity received by e-mail, letter, telephone, or Web site 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 (Eco-Terrorism).
  - Requests for access to laboratories for no apparent legitimate purpose, or for purposes that don't seem legitimate.
  - Unauthorized attempts to probe or gain access to proprietary information systems, particularly access control systems (e.g., 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.

References

1. Facilities Physical Security Measure Guidelines, ASIS GDL FPSM-2009
2. Pre-employment Background Screening Guidelines, ASIS GDL PBS-2009
3. UNIFIED FACILITIES CRITERIA (UFC), DoD Security Engineering Facilities Planning Manual, 11 September 2008
4. The FBI Agriculture, Chemical and Petroleum Industry Terrorism Handbook
5. Workplace Violence Prevention and Intervention. ASIS/SHRM WVP1.1-2011 (ANSI Standard)
6. Biosafety in Microbiological and Biomedical Laboratories (BMBL) 5th Edition
7. Director of Central Intelligence Directive No. 6/9 (Physical Security Standards for Sensitive Compartmented Information Facilities)
8. Review of the Department of Homeland Security's Approach to Risk Analysis (2010), National Research Council of the National Academies, The National Academies Press
9. ANSI Security Management Standard: Physical Asset Protection, ANSI/ASIS PAP.1-2012

Appendices

The appendices contain information, suggested diagrams, and examples that an entity may consider in development and implementation of a security plan. The entity is not required to use, or limited to, the information provided in the appendices.

Appendix I: Sample Scenario Diagram

Appendix II: Risk Assessment Methods

Appendix III: Comparison of Access Control Devices and Systems Which are Used to Control Access to Select Agents and Toxins

Appendix IV: Tier 1 Barrier Scenarios

Appendix V: Intrusion Detection Systems

Appendix VI: Example of a Select Agent Inventory Form that Captures the Requirements Listed in Section 17

Appendix VII: Example of a Toxin Inventory Form that Captures the Requirements Listed in Section 17

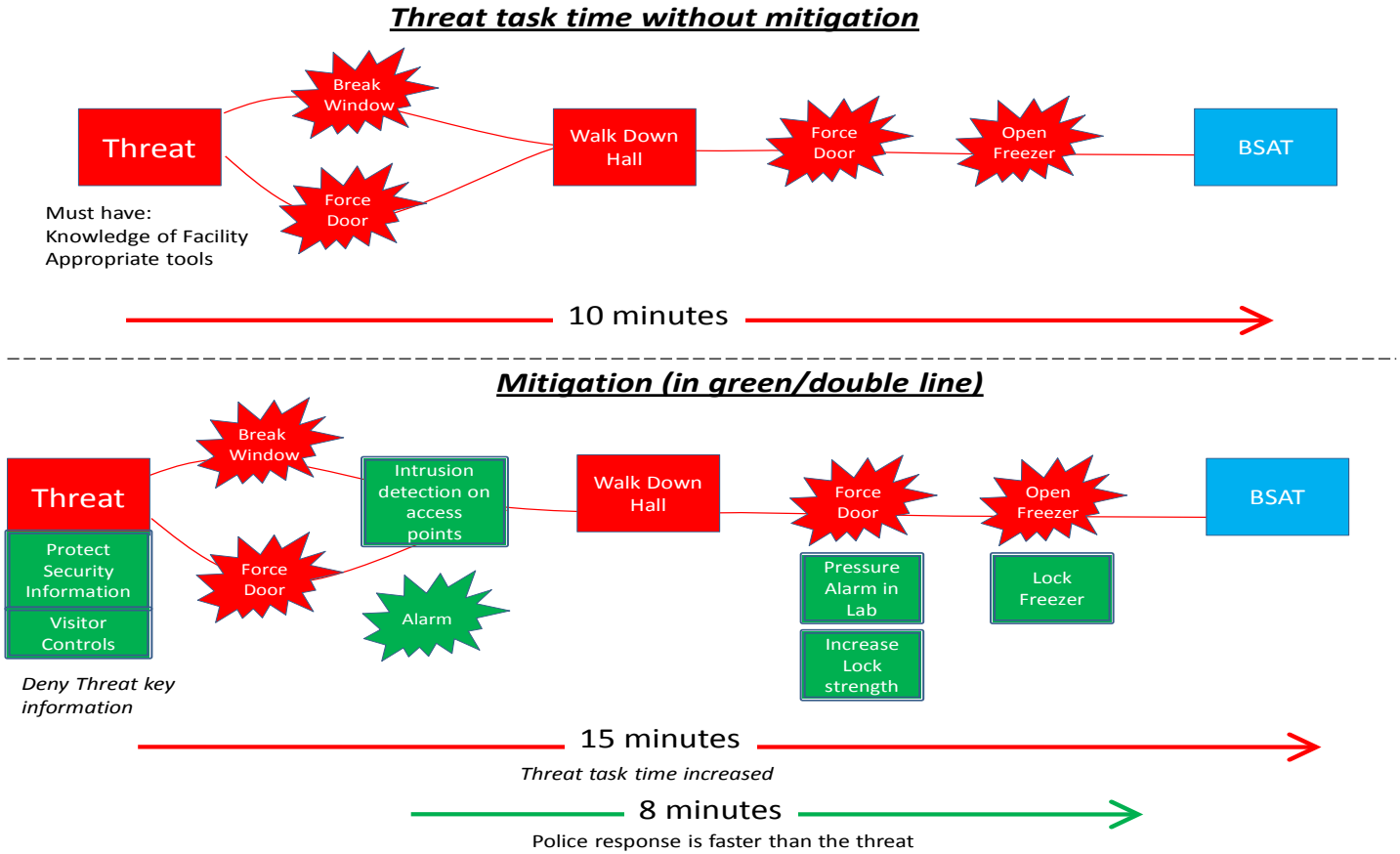
Appendix VIII: Suspicious Package

Appendix IX: Example of an Intra-Entry Inventory Form that Captures the Requirements Listed in Section 17

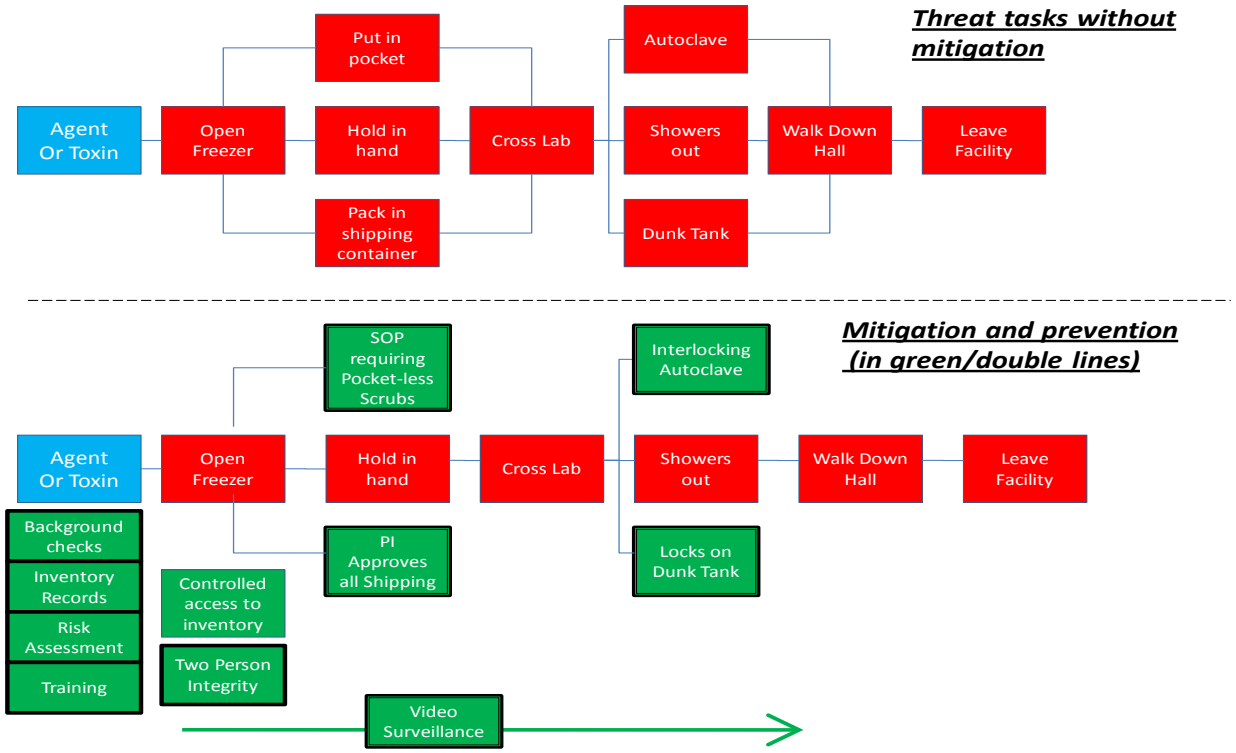
Appendix X: Shared areas where Tier 1 BSAT or Toxins are used or stored

Appendix I: Sample Scenario Diagram

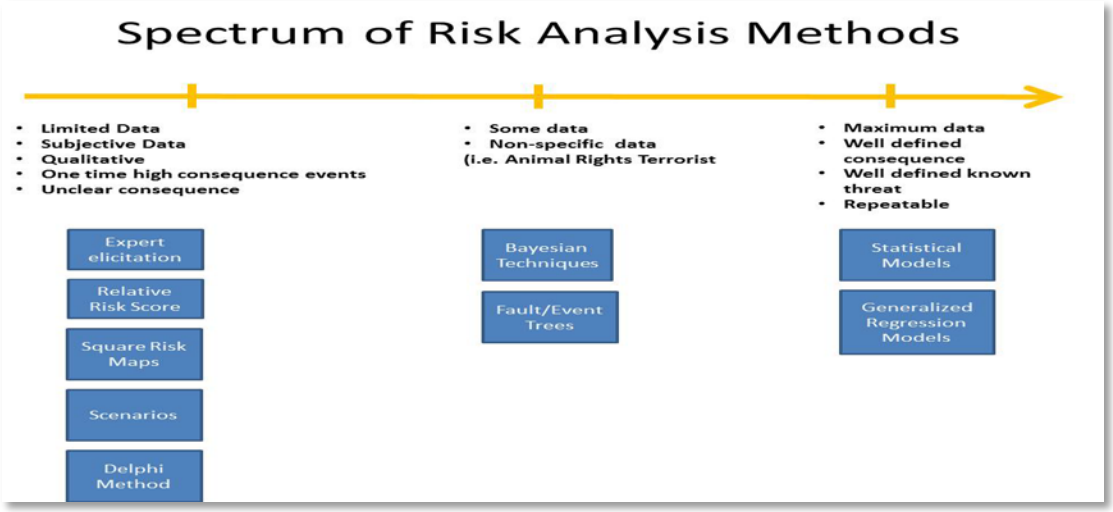
Outsider Threat (Someone without authorized access with intent and capability to steal or impact a select agent or toxin). Barriers deter but cannot be relied on to stop an outsider. The outsider cannot be stopped by locks, doors or other barriers, only delayed. The only thing that will stop an outsider is a response force.



Insider Threat (Someone with authorized access with intent and capability to steal or impact a select agent or toxin)
Unlike the Outsider, the entity can take steps to prevent certain tasks. Entities should focus on how one could get a select agent or toxin out of the registered areas without authorization and create control or measures which prevent it.



Appendix II: Risk Assessment Methods



(From National Academies of Science)

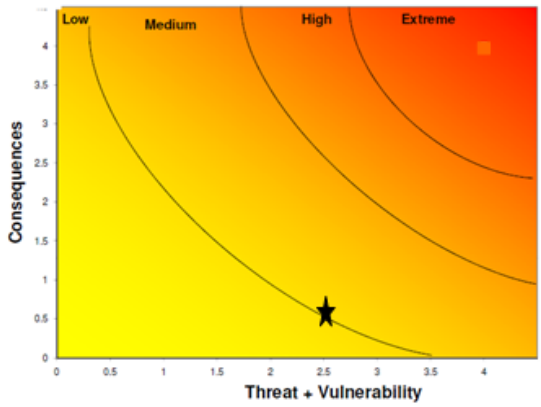
Example "Squares Risk Map" or "4 Square Risk Map"- This method assesses risk as 'low,' 'medium,' 'high' and 'extremes.' Threat and Venerability are combined into one score (one independent variable) and compared SMEs and Entity Members to consequence which is treated as independent variable.

RISK

Consequence			
Extreme	High	High	Extreme
High	Medium	High	Extreme
Medium	Medium	Medium	High
Low	Low	Medium	High
	Unlikely	Possible	Likely

Threat + Vulnerability

Example "Relative Risk Score"- This method assesses risk by numerically scoring threats and vulnerabilities. Threat and Venerability are combined into one score (one independent variable) and compared to consequence which is treated as independent variable.

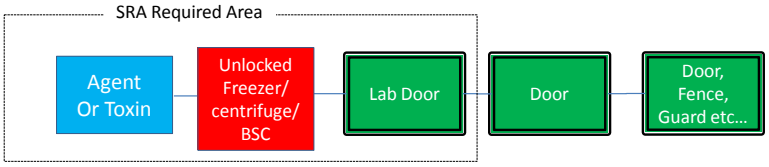


Appendix III: Comparison of Access Control Devices and Systems Which are Used to Control Access to Select Agents and Toxins

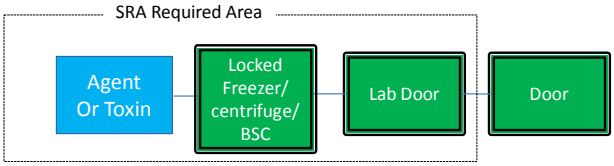
Lock Type	Physical Security Requirement	Additional SRA Requirements
Mechanical Key	• All keys must be tracked in a log. • Change locks if key is lost or compromised. • All keys must be returned when people quit or are terminated. • The entity must log access and retain for 3 years. • If the key is secured in a key box, the key box key must meet the requirements above.	• 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	• The entity must change the code or lock when personnel quit or are terminated. Changes must be reflected in a log. • The entity must change the code or lock in the event of compromise. • The entity must log access to registered areas and retain access records for 3 years.	• 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	• The entity must 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.	• All personnel with card-key which can open door (includes facility wide keys)
Card Key+ Pin	• The entity must maintain electronic logs of access for 3 years. • The access control network must meet the information security requirements.	• No additional requirement
Biometrics	• The entity must maintain electronic logs of access for 3 years. • The access control network must meet the information security requirements.	• No additional requirement
Multiple kinds of access control (i.e., Card Key and Mechanical Lock on same door)	• All the requirements for each type of access control systems when or if used.	• 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)	• Maintain electronic logs of access for 3 years. • The access control network must meet the information security requirements.	• No additional requirement
"Emergency" card key kept with First Responders	• Log of access. • Inventory of key. • Notification of the RO and Federal Select Agent Program in the event of its use.	• 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)	• Maintain electronic logs of access for 3 years. • Notification of the RO and Federal Select Agent Program in the event of its use.	• No SRA requirement for first responders

Appendix IV: Tier 1 Barrier Scenarios

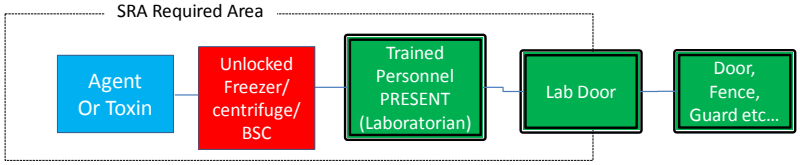
Scenario 1 (typical working facility)



Scenario 2: When in storage

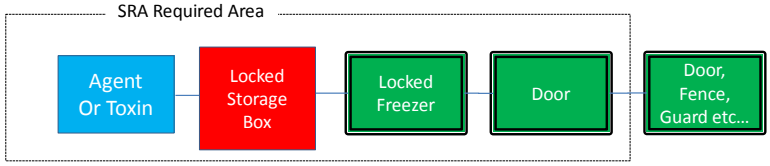


Scenario 3: If working on 'the bench'

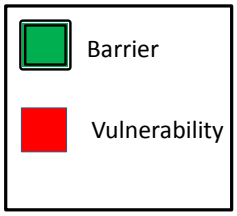


(if the person leaves, it must be returned to a secure location)

Scenario 4: Locked box



(if someone could gain possession of the locked box and depart registered area, they are considered in possession of the agent)



Appendix V: 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 VI: Example of a Select Agent Inventory Form that Captures the Requirements Listed in Section 17

SELECT AGENT NAME: TYPE: STRAIN DESIGNATION:
GENBANK ACCESSION NUMBER:

QUANTITY ACQUIRED: DATE OF ACQUISITION: SOURCE OF ACQUISITION:

WHERE STORED:
BUILDING: ROOM: FREEZER:

INVENTORY OF USAGE

DATE REMOVED FROM STORAGE	QUANTITY REMOVED	REMOVED BY	PURPOSE OF USE	DATE RETURNED TO STORAGE	QUANTITY RETURNED	RETURNED BY	DATE DESTROYED	QUANTITY REMAINING

Comments/Discrepancies:_____
_____

Appendix VII: Example of a Toxin Inventory Form that Captures the Requirements Listed in Section 17

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:_____
_____

Appendix VIII: Suspicious Package

FBI Advisory

If you receive a suspicious letter or package

What should you do?

1. **Handle with care Don't shake or bump**
2. **Isolate and look for indicators**
3. **Don't Open, Smell or Taste**
4. **Treat it as Suspect! Call 911**

If parcel is open and/or a threat is identified...

For a Bomb

Evacuate Immediately
Call 911 (Police)
Contact local FBI

For Radiological

Limit Exposure - Don't Handle
Distance (Evacuate area)
Shield yourself from object
Call 911 (Police)
Contact local FBI

For Biological or Chemical

Isolate - Don't Handle
Call 911 (Police)
Wash your hands with soap and warm water
Contact local FBI

Police Department _____

Fire Department _____

Local FBI Office _____

(Ask for the Duty Agent, Special Agent Bomb Technician, or Weapons of Mass Destruction Coordinator)

GENERAL INFORMATION BULLETIN 2000-3

Appendix IX: Example of an Intra-Entity Transfer Form that Captures the Requirements Listed in Section 17

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

Comments:

_____
_____
_____
_____
_____
_____

Appendix X: Shared areas where Tier 1 BSAT are used or stored

Security requirements for shared areas depend on access to the select agents and toxins. All personnel who have access to the Tier 1 BSAT must have gone through the entity's pre-access suitability and be enrolled in the ongoing assessment program. Beyond that, it depends on the parameters for the work or action being done. Below are six common scenarios and the corresponding personnel and physical security requirements.

1) **Actively working with Tier 1 BSAT and select agents and toxins simultaneously in the same contiguous registered area.** An entity is conducting research or diagnostic work using Tier 1 BSAT along with other work in a single registered suite.

Personnel Requirements	All people with access to the agent within the suite/shared area have gone through the entity's pre-access suitability and are subject to on-going assessment.
Physical Security Requirements	The suite/shared area meet all the physical security requirements for Tier 1. Final barrier usually the door to the suite.
Verification Check	Access logs to the suite must reflect only entity personnel who have gone through the entity's pre-access suitability and ongoing access.

2) **Storage only within a registered space.** A Tier 1 storage location or freezer location inside registered laboratory or a shared freezer inside a registered laboratory.

Personnel Requirements	All people with access to the locking storage device (i.e., freezer) have gone through the entity's pre-access suitability and on-going assessment. All people with access to the room but not to the Tier 1 BSAT do not need to be in the entity's pre-access suitability and on-going assessment program.
Physical Security Requirements	Storage location meets the security requirement for Tier 1. Final barrier is the locking mechanism of the storage device.
Verification Check	Access logs to storage device that contains Tier 1 BSAT (i.e., freezer) must reflect only entity personnel who have gone through the entity's pre-access suitability and ongoing access.

3) **Working with Tier 1 BSAT and select agents and toxins inside the same contiguous registered space separated by time.** This entails only working with Tier 1 during certain well defined times and conditions. The entity restricts access during times when Tier 1 BSAT is outside of locked storage units such as a locked freezer or a locked incubator.

Personnel Requirements	All people with access to the suite/shared area when Tier 1 BSAT is present have gone through the entity's pre-access suitability and on-going assessment.
Physical Security Requirements	The suite/shared area meet all the physical security requirements for Tier 1 BSAT. Depending on how the work is organized, the final barrier may be the door to the suite or to any freezers /devices containing Tier 1 BSAT during work with select agents and toxins.
Verification Check	Access logs to room and written procedures in the security plan that detail how access is restricted when Tier 1 BSAT are outside of locked storage.

4) **Shared Autoclave.** Using an autoclave for both Tier1 BSAT and select agents and toxins.

Personnel Requirements	For select agents and toxins, individuals operating the autoclave must be SRA approved. For Tier 1 BSAT, individuals operating the autoclave Tier 1 BSAT must be SRA approved and have gone through the entity's pre-access suitability and subject to on-going assessment.
Physical Security Requirements	For select agents and toxins, agent or toxin secured by SRA approved persons until the autoclave reaches desired operational parameters. For Tier 1 BSAT, the agent or toxin secured by individuals who is SRA approved and has gone through the entity's pre-access suitability and subject to on-going assessment. That person must remain until the autoclave reaches desired operational parameters. It is recommended that autoclaved cycles be scheduled so materials can be autoclaved without delay.
Verification Check	Autoclave records.

5) **Animals exposed to a Tier 1 BSAT-** An animal that is experimentally infected or exposed to a **Tier 1 BSAT** must be secured as a Tier 1 BSAT itself until such time as it is demonstrated to be free of that select agent.

Personnel Requirements	Individuals who exposed the animal must be SRA approved and have gone through the entity's pre-access suitability and subject to on-going assessment. Personnel who handle or care for the animal must be SRA approved and have gone through the entity's pre-access suitability and subject to on-going assessment.
Physical Security Requirements	The area where the animal is handled and housed meets all the physical security requirements for Tier 1 agents. Final barrier usually the door to the suite.
Verification Check	Access logs.

6) **Animals inoculated with a Select Toxin**

Personnel Requirements	For select toxins, persons inoculating the animals must be SRA approved. For Tier 1 select toxin, individuals who inoculated the animal must be SRA approved and have gone through the entity's pre-access suitability and subject to on-going assessment.
Physical Security Requirements	For all select toxins, room used for inoculation must be registered. Animal inoculated with select toxins are not subject to additional security requirements. However, any equipment used for inoculation of animals (syringe, aerosol chamber) must be managed as a select toxin until decontaminated. For Tier 1 select toxin, registered room must meet Tier 1 security requirements (e.g., 3 barriers, IDS).
Verification Check	Inventory Logs with respect to toxin only.