



Guidance for Suitability Assessments

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

Acknowledgement: The Federal Select Agent Program would like to thank members of the Federal Experts Security Advisory Panel for their assistance in drafting this guidance document.

Revisions: This is a living document subject to on-going improvement. Feedback or suggestions for improvement are welcomed. Comments may be submitted to the Federal Select Agent Program at:

CDC: LRSAT@cdc.gov

APHIS: ASAP@aphis.usda.gov

Introduction

Section 11(f) (1) of the select agent regulations (Part 331 of Title 7, Part 121 of Title 9, and Part 73 of Title 42 of the Code of Federal Regulations) provides that the security plan for an entity possessing Tier 1 biological select agents and toxins (Tier 1 BSAT) must describe procedures for conducting a pre-access suitability assessment of persons who will have access to Tier 1 BSAT. Section 11 (f)(4)(i) provides that an entity with Tier 1 BSAT must prescribe procedures that will limit access to Tier 1 BSAT only to those individuals who are approved by the HHS Secretary or Administrator, following a security risk assessment by the Attorney General, have had an entity-conducted pre-access suitability assessment, and are subject to the entity's procedures for ongoing suitability assessment.

The purpose of this guidance document is to assist entities in the development of a site-specific suitability assessment program to enhance personnel security for individuals with access to Tier 1 BSAT. The information presented here consists of recommendations that an entity may consider in the development and implementation of personnel suitability assessments for access to Tier 1 BSAT. *A registered entity is neither required to use nor is limited to any example procedures or forms provided in this document.*

We recognize that an entity may already have established procedures that evaluate the suitability of personnel prior to their employment and/or access to Tier 1 BSAT in accordance with institutional policy, and federal, state and local laws. An entity may choose to tailor such existing procedures in a site-specific manner to meet the requirements of the select agent regulations. The guidance provided in this document is not intended to be used to assess a person's eligibility for employment by an entity; rather the guidance provides options that an entity may consider in the development of a personnel suitability assessment program.

The guidance contained in this document is not intended to and does not supersede state or local laws. Those sections of the select agent regulations which require an entity to include in its written security plan a pre-access suitability assessment and an on-going assessment of individuals with access to Tier 1 BSAT do not preempt federal, state or local employment or privacy laws. In the development and implementation of a plan for pre-access suitability assessment and the on-going assessment of suitability of individuals with access to Tier 1 BSAT, an entity must ensure that it is compliant with all federal, state and local employment and privacy laws.

Pre-Access Suitability Assessment Program

In order to ensure that personnel who will have access to Tier 1 BSAT are suitable for such access it is important to remember that while academic credentials and prior experience may qualify an individual to perform or support scientific research, their scientific ability may not equal suitability. Entity leadership needs to look beyond an individual's resume/curriculum vitae and security risk assessment (SRA) determination to assess whether an individual possesses attributes that support public safety and the security requirements of work with Tier 1 BSAT. An entity's pre-access suitability assessment should form the basis for determining whether an individual is suitable for access to Tier 1 BSAT. Chapter 2 of this document discusses entity resources and personnel responsibilities for the

development of a Tier 1 BSAT suitability assessment program. Chapter 3 of this document describes a sample pre-access suitability assessment program.

On-going Suitability Assessment Program

The purpose of the on-going assessment of an employee's suitability is to ensure that an individual with access to Tier 1 BSAT continues to merit access. It is necessary for an entity to remain engaged and to regularly check current information to ensure continued employee suitability for access to Tier 1 BSAT. Chapter 4 of this document describes a sample of an on-going suitability assessment program.

Transitioning of Individuals with Access to Tier 1 BSAT on the Effective Date of the Regulations into an On-going Suitability Program

Individuals having approved access to Tier 1 BSAT prior to the effective date of the security provisions (180 days after the publication of the select agent regulations) are not required to have a pre-access suitability assessment. An entity has discretion as to the procedures used to transition individuals, currently listed on the entity's registration as having access to Tier 1 BSAT, into an on-going suitability assessment program. Chapter 5 of this document discusses the transitioning of individuals with current access to Tier 1 BSAT into an on-going suitability program.

An entity must maintain records related to personnel suitability programs in accordance with Section 17 (Records) of the select agent regulations.

Denial, Termination or Suspension of Individual's Access to Tier 1 BSAT

Chapter 6 of this document addresses the denial, termination or suspension of an individual's access to Tier 1 BSAT.

Table of Contents

Definitions	6
Chapter One: The Potential for Insider Threat and Need for the Suitability Assessment of Personnel	8
Chapter Two: Roles and Responsibilities.....	10
Chapter Three: Pre-Access Suitability Assessment {Section 11(f)(1)}.....	14
Chapter Four: Ongoing Suitability Assessment	21
Chapter Five: Transition of Individuals with Access to Tier 1 BSAT at the Effective Date of the Regulations	28
Chapter Six: Denial, Termination or Suspension of an Individual’s Access to Tier 1 BSAT	29
References.....	31
Appendices	32
Appendix I. Example of an Entity’s Pre-access Suitability Process	33
Appendix II. Options for Obtaining Criminal Records.....	34
Appendix III. Example Questions for Use in Reference Interviews	36
Appendix IV. Visitors for short term training with Tier 1 BSAT	37
Appendix V. Example of self and peer reporting process flow.....	38

Definitions

Access to Tier 1 BSAT: An individual will be deemed to have access to a Tier 1 BSAT at any point in time if the individual has possession of a Tier 1 BSAT (e.g., ability to carry, use, or manipulate) or the ability to gain possession of a Tier 1 BSAT (See section 10(b) of the select agent regulations).

Bioterrorism Security Risk Assessment Form (FD-961 Form): The FBI's Application for Security Risk Assessment that assists the Federal Bureau of Investigation (FBI), Criminal Justice Information Services Division (CJIS) to perform an electronic records check to determine if an individual who has been identified by a registered entity as having a legitimate need to access select agents or toxins exhibits one of the statutory restrictors which would either prohibit or restrict access.

Entity: As used in this document, the term "entity" refers to any government agency (federal, state, or local), academic institution, corporation, company, partnership, society, association, firm, sole proprietorship, or other legal entity that is registered with the Federal Select Agent Program.

Entity Leadership: Entity leadership includes all entity officials who have responsibilities for science, safety, and security at an institution. These officials may include Vice Presidents of Research, Deans, Chief Executive Officers (CEOs), Institutional Officials, Department Chairs, Ranking Officials, Owners/Controllers, etc.

Federal Select Agent Program: The joint management of Centers for Disease Control and Prevention's Division of Select Agents and Toxins and the Animal and Plant Health Inspection Service's Agricultural Select Agent Program of the select agent regulations.

Human Resources (HR): The division of an organization that is focused on activities relating to employees. These activities normally include recruiting and hiring of new employees, orientation and training of current employees, employee benefits, and retention.

On-going Suitability Assessment: After the initial pre-access suitability assessment, a standardized procedure to determine if an individual displays behaviors determined by the entity that would increase the risk of a theft, loss, or release of a select agent or toxin.

Personnel Suitability: Personnel with access to select agents or toxins should not display behaviors determined by the entity that would increase the risk of a theft, loss, or release of a select agent or toxin.

Pre-Access Suitability Assessment: The evaluation of an individual using a standardized procedure to determine if the individual displays behaviors determined by the entity that would increase the risk of a theft, loss, or release of a select agent or toxin.

Principal Investigator (PI): The individual who is designated by the entity to direct a project or program and who is responsible for the scientific and technical direction of that project or program.

Responsible Official (RO): The individual designated by an entity with the authority and control to ensure compliance with the select agent regulations. The regulatory requirements for Responsible Officials are given in Section 9 of the regulations.

Security Risk Assessment (SRA): Electronic records check performed by CJIS to determine if an individual who has been identified by a registered entity as having a legitimate need to access select agents or toxins exhibits one of the statutory restrictors which would either prohibit or restrict access (**Table 1**).

Select Agent Regulations: Part 331 of title 7, Part 121 of title 9, and Part 73 of title 42 of the Code of Federal Regulations (CFR)

Select Agents and Toxins: Biological select agents or toxins listed in sections 3 and 4 of the select agent regulations.

Suitability Assessment Program: A combination of pre-access and on-going suitability practices, in conjunction with comprehensive and consistent review mechanisms, determining the reliability of personnel for access to Tier 1 BSAT, and allowing individuals to report risks and threats to safety and security concerning Tier 1 BSAT to entity leadership.

Tier 1 BSAT: A subset of select agents or toxins designated in the select agent regulations as “Tier 1” because these agents and toxins present the greatest risk of deliberate misuse with the most significant potential for mass casualties or deleterious effects on the economy, critical infrastructure, or public confidence.

“Whole Person” Assessment: A balanced assessment of an individual, establishing a behavioral baseline in the environment in which that person works, lives and socializes, along with mitigating circumstances, and discerning overall qualities of credibility and suitability.

Chapter One: The Potential for Insider Threat and Need for the Suitability Assessment of Personnel

The select agent regulatory requirements for a pre-access suitability assessment and an on-going suitability assessment are designed to reduce the risk of select agents or toxins misuse through the actions of an “insider”.

Select agents or toxins released intentionally or accidentally, can result in disease, wide-ranging and deleterious impacts on the economy, disruption to society, diminished confidence in public and private institutions, and large-scale loss of life. People or livestock can be exposed to these agents by inhalation, skin contact, or the ingestion of contaminated food, feed, crop or water. Also, plants infected with select agents or toxins could cause disruption of the domestic food supply and trade, as a result of crop contamination and/or mortality.

The October 2001 anthrax letter attacks provide an example of the costs that the select agent regulations would help prevent. The anthrax letter attacks caused 5 fatalities and 17 illnesses, disrupted business and government activities, closed substantial parts of the U.S. government, and caused widespread apprehension and changes in public behavior. Costs included more than \$23 million to decontaminate one Senate office building, approximately \$2 billion in revenues lost to the postal service and up to \$3 billion in additional costs to the postal service for decontamination and procurement of mail-sanitizing equipment. Substantial costs due to lost productivity throughout the economy and from on-going costs of the investigations into the incident are additional impacts.

The FBI Amerithrax investigation identified a U.S. scientist as the most likely perpetrator of the October 2001 anthrax attacks. This finding resulted in a renewed scrutiny of laboratory security addressing the insider threat, and emphasized concerns surrounding the potential misuse of dangerous pathogens within research settings. Subsequently, reports produced by Federal and non-Federal advisory groups identified a gap that existed in regulatory oversight at the local level between the eligibility of personnel accessing select agents and toxins, and suitability of such personnel to maintain entity safety and security standards. Reports also identified the limitations of relying on the FBI’s security risk assessment entirely for personnel security. Additionally, the Amerithrax Expert Behavioral Analysis Panel (EBAP), commissioned by the United States District Court for the District of Columbia, noted several concerning behaviors and an unwillingness on the part of supervisors and coworkers to report these behaviors to relevant authority. The EBAP report identified a need for baseline and on-going personnel suitability assessments coupled with a robust peer- and self-reporting mechanism.

With respect to select agents or toxins, the “insider threat” generally refers to an individual who has access to select agents or toxins as part of his or her job and has the potential to misuse these materials. Some examples of the “insider threat” include:

- an individual with malevolent intent who infiltrates a research facility under the guise of a legitimate researcher in order to steal, release or divert select agents or toxins;
- an individual with access to select agents or toxins who is coerced or manipulated into providing access or expertise to unauthorized individuals with malevolent intent;

- an individual whose job duties require legitimate access to select agents or toxins but who may misuse, release or divert select agents or toxins as a result of a significant life changing event.

The current mechanism utilized by the Federal Select Agent Program for determining whether an individual will be approved for access to select agents or toxins is the SRA conducted by the CJIS. The SRA process is an electronic database check to identify any of 9 “prohibitors” and 3 potential “restrictors”, outlined in **Table 1**. However, the SRA is not a comprehensive “background investigation” and should not be regarded as a substitute for the suitability assessment discussed in this guidance.

Table 1. Restricted categories under 18 USC § 175b
• Individual is under indictment for a crime punishable by imprisonment for a term exceeding 1 year
• Individual has been convicted in any court of a crime punishable by imprisonment for a term exceeding 1 year
• Individual is a fugitive from justice
• Individual is an unlawful user of any controlled substance (as defined in section 102 of the Controlled Substances Act (21 USC 802))
• Individual is an alien illegally or unlawfully in the U.S.
• Individual has been adjudicated as a mental defective or has been committed to any mental institution
• Individual is an alien (other than an alien lawfully admitted for permanent residence) who is a national of a country as to which the Secretary of State, pursuant to section 6(j) of the Export Administration Act of 1979 (50 App. U.S.C. 2405 (j)), section 620A of chapter 1 of part M of the Foreign Assistance Act of 1961 (22 U.S.C. 2371), or section 40 (d) of chapter 3 of the Arms Export Control Act (22 U.S.C. 2780 (d)), has made a determination (that remains in effect) that such country has repeatedly provided support for acts of international terrorism
• Individual has been discharged from the Armed Services of the U.S. under dishonorable conditions
• Individual who is a member of, acts for or on behalf of, or operates subject to the direction or control of, a terrorist organization as defined in section 212(a)(3)(B)(vi) of the Immigration and Nationality Act (8 USC 1182 (a)(3)(B)(vi))
The Federal Select Agent Program may limit or deny access to individuals reasonably suspected by any Federal law enforcement or intelligence agency of:
• Committing a crime specified in 18 USC §2332b(g)(5) (Acts of Terrorism Transcending National Boundaries)
• Knowing involvement with an organization that engages in domestic or international terrorism (as defined in 18 USC 2331) or with any other organization that engages in intentional crimes of violence
• Being an agent of a foreign power (as defined in 50 USC 1801)

Entities are permitted and encouraged to deny or remove anyone from access to Tier 1 BSAT who has qualities or has exhibited behaviors that suggest the individual is incapable of safely working with or protecting the security of Tier 1 BSAT. This guidance addresses these aspects of suitability.

Chapter Two: Roles and Responsibilities

This section provides guidance on the roles and responsibilities of entity leadership and personnel in the development and implementation of a suitability assessment program.

Entity leadership, including the RO, supervisors, HR, legal counsel, and security professionals should collect comprehensive information from personnel who will need access to Tier 1 BSAT, in order to assess their suitability. Self-reported information should be corroborated by a review of the records collected in conjunction with a review of professional and peer references. In some cases, collaboration with HR may provide information from a person's employment application. In other situations (e.g., students), the information will be acquired for the first time. Honesty and completeness are essential in the application process, and should be supported by policies that foster these qualities in an applicant and that promote the assessment of the individual as a "whole person."

An RO may not have all of the relevant experience and/or expertise necessary to develop and implement a suitability assessment program. Entity leadership should consider other entity resources to assist the RO in the development of a program. Examples of in-house resources may include HR, security personnel, occupational health programs, and legal counsel. The entity should consider all available resources that may be leveraged to assist the RO in the development of a comprehensive suitability assessment program.

The Federal Select Agent Program recommends that decisions of suitability for access to Tier 1 BSAT should not be evaluated or decided by a single person. Entities may consider the designation of two individuals for the purposes of evaluating and certifying a projected suitability assessment program:

- **Reviewer (REV):** An entity official whose duties include monitoring the suitability assessment program and reviewing warranted suitability actions. This person may be a security or administrative professional, legal counsel, or other person who can provide an alternate and complementary perspective on the suitability assessment program and Tier 1 BSAT access decisions to the RO. If resources do not permit the appointment of a separate reviewer, the RO may act as the REV. The REV will be able to protect and evaluate the personal information required to administer a suitability assessment program. The REV should be competent to assess personnel with respect to both pre-access and on-going suitability assessments.
- **Certifying Official (CO):** An entity official who certifies that personnel meet the established requirements of an entity-specific suitability assessment and monitoring program. The CO should have sufficient familiarity with all individuals having access to Tier 1 BSAT, and their supervisory chain, to permit a continual evaluation of their suitability, and have the authority to engage supervisors when warranted. The CO should possess human resources expertise and experience in order to collect, evaluate, and protect personal information required in the suitability assessment program. Optimally, the CO is a person outside the individual's supervisory chain, such as an HR professional, occupational health physician, Employment Assistance Program (EAP) counselor, Principal Investigator (PI) not associated with the work to

be performed, or other interested and qualified person. The CO notifies the RO on matters pertinent to personnel suitability directly.

The entity may have individuals who already perform the REV and CO duties, or have entity personnel who may have these duties added to their current responsibilities. The entity may consider convening an objective review panel to assess the suitability of individuals requesting access to Tier 1 BSAT. The addition of other members or designation of additional COs and REVs, to the suitability review panel would be at the entity's discretion.

Position Definitions & Responsibilities

Promoting a shared sense of responsibility for the safe and secure use of Tier 1 BSAT by all stakeholders will serve to strengthen the culture of reliability, safety and security at the registered entity. Suggested position definitions and responsibilities applicable to a suitability assessment program are listed below.

Entity Leadership

All entity officials who have responsibilities for science, safety, and security at an institution represent potential resources and support for the entity's select agent suitability program. These individuals have authority to designate the RO and alternate RO(s) on behalf of the entity. Entity leadership may include the Owner/Controller, CEO, Vice President for Research, Ranking Official, Department Chair or other senior leadership personnel. Entity leadership should provide support to the RO in the development and implementation of a suitability assessment program for individuals with access to Tier 1 BSAT. Entity leadership should encourage a culture of responsibility, safety and security, and should not tolerate retaliation or retribution for the legitimate reporting of information that may affect the safety and security of Tier 1 BSAT. Entity leadership should make a concerted effort to ensure the authorized need, anonymity and confidentiality of personal information when shared.

Entity Leadership responsibilities:

- Collaborate with the RO to develop and implement a suitability assessment program for personnel access to Tier 1 BSAT
- Provide resources for the RO to establish a suitability assessment program. This may include direct financial support or promoting connections between the RO and existing institutional resources (e.g., entity leadership, HR, security personnel, legal counsel, occupational health program, etc.)
- Support the RO in the establishment of policies and administrative procedures to execute an effective suitability assessment program. Essential program components may include:
 - a. Routine pre-access and ongoing suitability assessment protocols
 - b. Policies that allow an individual to voluntarily "opt out" of Tier 1 BSAT work (coordination with human resources, supervisors, etc.)
 - c. Policies that address the temporary or permanent denial of access to Tier 1 BSAT

- d. Policies and procedures to manage appeals of administrative actions that may result from suitability assessments
- Support efforts to protect from retribution those individuals reporting adverse or derogatory information. A plan should be implemented for appropriately handling false reports.
- Establish communication channels for the sharing of suitability program information, as appropriate, among relevant stakeholders and the RO. At a minimum, this will involve the timely communication to entity personnel – administrators, supervisors, laboratorians, security, etc. – of the development, implementation, expected support, and personnel rights and responsibilities associated with the entity’s personnel suitability program
- Promote a culture of reliability, safety and security in all matters dealing with access to Tier 1 BSAT.

Responsible Official (RO)

The RO is responsible for ensuring compliance with the select agent regulations. The RO can be the person with the authority to immediately restrict or deny access to Tier 1 BSAT based on behavioral, medical or administrative grounds, and is ultimately responsible for notifying the Federal Select Agent Program of terminations to personnel access to select agents and toxins through the submission of amendments to the entity’s registration. With available entity resources, the RO should establish and implement procedures for conducting suitability assessments for individuals requesting access to Tier 1 BSAT.

RO responsibilities:

- Ensure that the APHIS/CDC Form 1 indicates those individuals that will have access to Tier 1 BSAT
- Involvement in the development of the Tier 1 BSAT suitability assessment program and lead its implementation and administration
- Designation of a CO and a REV, or establishment of administrative mechanisms to execute these functions
- Coordination with other entity resources (e.g., safety and security personnel, legal counsel, HR) for the development, implementation and administration of the Tier 1 BSAT suitability assessment program
- Determine who should have Tier 1 BSAT access based on personnel suitability recommendations
- Ensure that access to Tier 1 BSAT is limited to individuals who have undergone a pre-access suitability assessment, are part of the entity’s on-going suitability monitoring, and have current Federal Select Agent Program approval (i.e., SRA clearance) to access select agents or toxins
- Ensure that appropriate annual training is completed and documented prior to the approval or continuance of access to Tier 1 BSAT
- Promote a culture of reliability, safety and security in all matters dealing with access to select agents and toxins

Individuals with Access to Tier 1 BSAT

Individuals with access to Tier 1 BSAT have a responsibility to monitor their own suitability, as well as the suitability of their colleagues performing duties that require access to Tier 1BSAT. It should be an entity policy that individuals advise their supervisor, CO, REV, and/or RO of any issues that could have an adverse impact on their performance, suitability, or safety while performing Tier 1 BSAT duties. It should be an entity policy that individuals advise their supervisor, RO and/or other entity officials (e.g., CO) when another individual with access to Tier 1 BSAT manifests behaviors, or otherwise appears to be involved in situations that may adversely affect the safety or security of Tier 1 BSAT.

Individual responsibilities (not intended to be comprehensive):

- Follow institutional policies and procedures for the safe and secure use of Tier 1 BSAT and comply with the select agent regulations
- Participate in and understand training associated with the suitability assessment program
- Report any situations that may affect safety and/or security of Tier 1 BSAT
- Respect the privacy and confidentiality of colleagues, and support an environment where direct or indirect retribution is not tolerated

Chapter Three: Pre-Access Suitability Assessment {Section 11(f)(1)}

Purpose

An entity registered to possess, use or transfer Tier 1 BSAT must describe procedures to evaluate a person's suitability for access to these materials in its site-specific security plan. An entity may consider the recommendations presented in this chapter to mitigate personnel security risks and to foster a culture of suitability, responsibility, safety and security for individuals with access to Tier 1 BSAT. It should be noted that the select agent regulations specifically address the suitability of an individual for access to Tier 1 BSAT, but not for employment in general. Although pre-access suitability is required specifically for applicants requesting access to Tier 1 BSAT, the regulations do not preclude the application of some pre-access suitability program for individuals with access to any select agents or toxin.

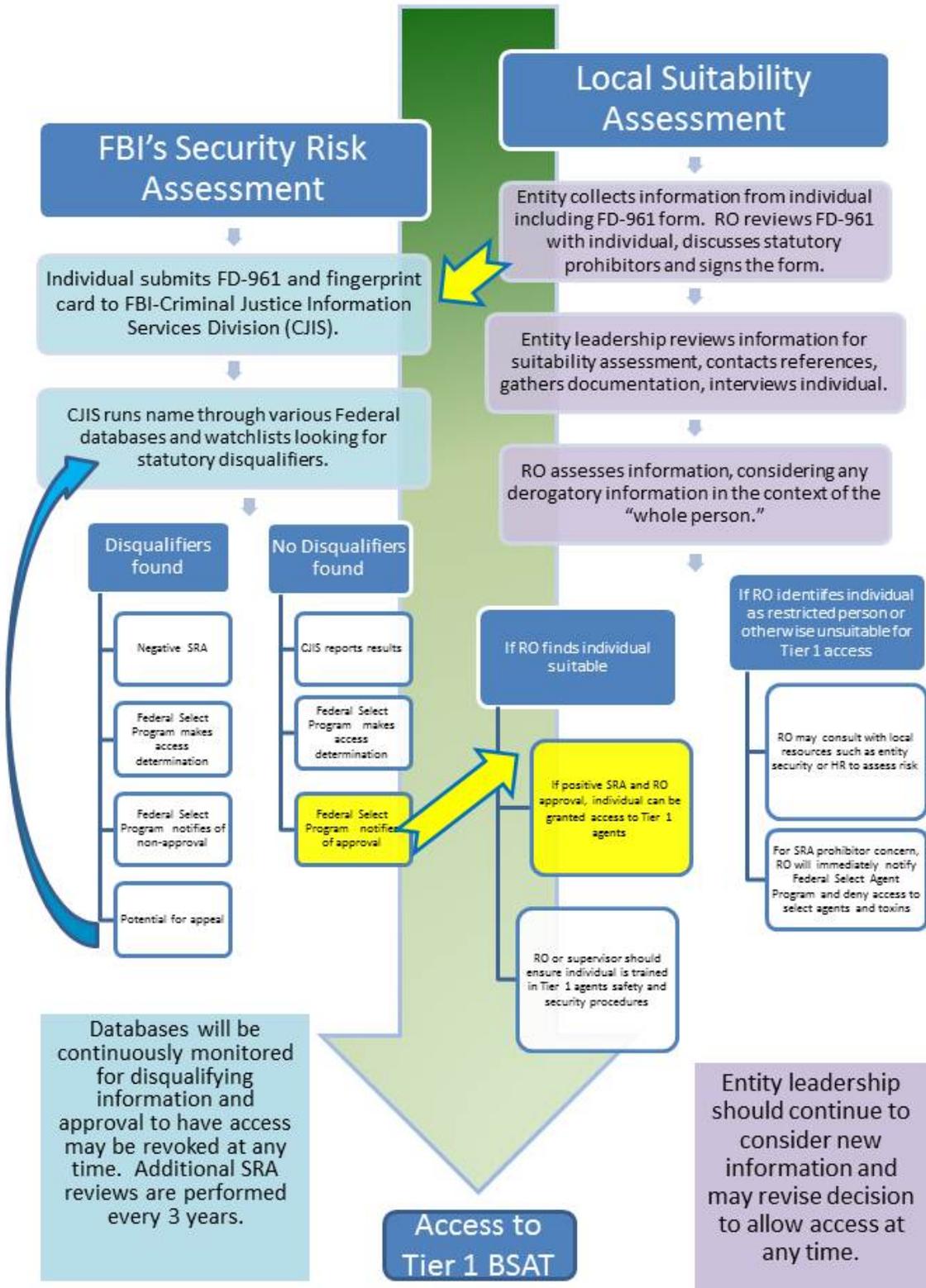
Any individual who did not have access to Tier 1 BSAT prior to the effective date of the security provisions (180 days after the publication of the select agent regulations) must undergo a pre-access suitability assessment and receive approval by the Federal Select Agent Program before they can have access to Tier 1 BSAT (See section 11 of the select agent regulations). The Federal Select Agent Program advises that while adequate academic credentials and prior experience may qualify an individual to perform or support scientific research, academic credentials and scientific expertise and experience do not alone constitute suitability. Entity leadership must look beyond an individual's curriculum vitae and SRA determination to assess whether the individual possesses attributes that support public safety and the security of Tier 1 BSAT.

New Access to Tier 1 BSAT

We recommend that the requirement for a suitability assessment should be included in applicable employment announcements and program descriptions. We also suggest that local entity suitability assessments can be run concurrently with the SRA process (see **Figure 1**).

All personnel information should be uniformly collected, evaluated and protected in accordance with institutional policy, and federal, state and local laws. A "whole person" assessment for each individual should consider both favorable and unfavorable information, along with mitigating circumstances, and overall qualities of credibility to determine suitability for access to Tier 1 BSAT.

Figure 1. Guide to Concurrent Processes of SRA and Local Suitability Assessment for Persons Needing Tier 1 BSAT Access



A. Collection and Verification of Information from the Person needing Tier 1 BSAT access

The Federal Select Agent Program recommends that an entity standardize its procedures for the collection of information from persons when conducting pre-access suitability assessments of persons requesting access to Tier 1 BSAT. The entity may find that the use of a standard form will result in the collection of information in a comprehensive and uniform manner. The Federal Select Agent Program recommends that such a form request and verify the information below, as appropriate and consistent with institutional policy, and federal, state, and local law:

1) Home Address History

In order to understand and corroborate other information provided by the person, an entity may consider a review of the person's home address history for the past 7 years, or from the age of 18, whichever represents a shorter period of time. This information should, at a minimum, include the states or countries where an individual has resided. Such information can facilitate the performance of local criminal conviction and arrest record checks.

2) Work History

An entity may consider requesting a description of all work experiences¹ for the past 7 years, or from the age of 18, whichever represents a shorter period of time, including an explanation of any gaps in employment. This information is important to suitability assessments for two reasons. First, the entity should assess prior work experiences for potential security concerns. Second, this information provides a context for professional references provided by the person for a further "whole person" assessment. If a person is unwilling to provide any work references, careful consideration should be given before an individual is issued access approval to Tier 1 BSAT.

3) Education History

An entity may consider requesting a person's records from all post-secondary institutions the individual claims to have attended; or other supporting education documentation if an individual has not attended post-secondary institutions. Additionally, consideration should be given to the accreditation and reputation of the educational institutions that the individual has claimed to have attended.

4) Criminal History (see Appendix II. Options for Obtaining Criminal Records)

Entities need to be aware that in the context of a criminal conviction and arrest history, the outcome of the SRA will only be affected by indictments or convictions of crimes punishable by imprisonment for a term exceeding 1 year. Individuals may have been convicted of lesser crimes or have been arrested for activities that are not relevant to suitability assessments (i.e.,

¹ For the purposes of this document, "work experiences" include paid and unpaid work, fellowship or trainee experiences, and volunteer positions.

misdemeanors). For example, a record of multiple arrests, even without conviction, may point to an instability that may be indicative of a pattern of behavior not consistent with suitability for access to Tier 1 BSAT. An entity should consider the use of a standard form to request information of criminal conviction and arrest history consistent with state and local laws and institutional policy. Further, an entity may already have requested this information from all employees prior to making hiring decisions. The entity may wish for HR to coordinate with the RO to determine if the information has previously been collected and is sufficient for the pre-access suitability assessment for Tier 1 BSAT.

To the extent possible, and consistent with state and local laws, criminal records could be obtained to 1) verify personal reports (or lack of reports) of criminal activity, and 2) determine deliberate withholding of information. Factual information derived from criminal records will usually provide the necessary information to proceed with an assessment to include the nature and seriousness of the offenses and their relevance to Tier 1 BSAT' job duties. Moreover, a review of a person's criminal records may also provide insight into patterns of behavior that may be of concern to the security and safety of the program.

When assessing criminal history, all events should be put into the context of the "whole person." Consideration should be given to: a) the nature of the event and whether the demonstrated behavior increases the risk in the laboratory, b) an individual's circumstances at the time of an event, c) the time that has passed since the event of concern, and d) the total number of events causing concern. Entities may also choose to assess the person's honesty and truthfulness in answering relevant questions, as well as the willingness to provide facts as a 'positive', while an attempt to cover up an event would be assessed as a 'negative.' As possible mitigating factors, positive information about the person should also be considered, including work performance or education since any derogatory event(s), the interpretation of the event(s) by supervisors at the time (and supervisors since), and how the individual interprets the event(s) during his or her interview.

An entity should enlist available security personnel and legal counsel to assist the RO in the evaluation of criminal conviction and arrest records to determine the suitability of an individual.

5) Resume or Curriculum Vitae (including scientific publications and affiliations)

A current resume or curriculum vitae may be used to assess the person's recent paid and unpaid work experiences, scientific publications, and affiliations for research with select agents or toxins, as applicable. This information may be reviewed by entity leadership to ensure that the person's work history, scientific publications, and/or affiliations are consistent with his or her application. Further, any degrees claimed on the resume or curriculum vitae can be verified with the registrar or other administrative body of the degree granting institution.

6) Professional License/Certification History

An entity may consider verifying information with the relevant certifying body, if possible, for licenses or certifications an individual claims to have earned (e.g., technologists/medical

doctors/doctors of veterinary medicine). State boards of licensure in each location where the individual has lived should be contacted to identify any negative information associated with each license possessed by the individual, since this information may not be routinely shared among state boards.

7) **Visa Status (if applicable)**

An entity should establish procedures to verify the identity of the person. Typically, an individual's visa status is tied to employment.

8) **References, including Contact Information**

An entity may consider requesting professional and peer references for each individual.

- A. Professional references can be selected from previous locations of work experiences in the past 7 years or from the age of 18, whichever represents a shorter period of time. Professional references should be able to speak to the person's actions while employed or volunteering that could contribute to a determination of the person's reliability, trustworthiness, honesty, judgment, emotional or mental stability, potential conflicting allegiances and potential or propensity for coercion.
- B. If relevant, professional references should be able to discuss a person's technical competency, including willingness and ability to adhere to administrative controls for safety and security.
- C. If relevant, peer references should be able to speak to the person's reliability, trustworthiness, honesty, judgment, emotional or mental stability, potential conflicting allegiances and potential or propensity for coercion.

With all references, questions should be asked that elicit an impression of the person's reliability, trustworthiness, honesty, judgment, whether their interactions with colleagues have been inconsistent or unusual, if there are potential conflicting allegiances, and if there are any behaviors or personal characteristics that may point to vulnerabilities to coercion (refer to **Appendix III. Example Questions for Use in Reference Interviews**).

An entity may have previously requested some or all of this information from an employee prior to hiring, with the information (such as work and education history) maintained in the individual's permanent employment record. HR personnel may coordinate with the RO to determine if the information has previously been collected and is sufficient for the person's pre-access suitability assessment for access to Tier 1 BSAT.

Other optional information sources may already have been used by an entity as part of the initial hiring process and/or used to determine an individual's suitability to access select agents or toxins, such as:

- Personnel records review (e.g., credit checks, driving records)
- Occupational Health evaluation
- Evaluation by employee assistance program counselors

- Drug testing

If these information sources are used currently to assess an individual's suitability for employment, an entity may decide to incorporate these information sources as a component of the entity's suitability assessment program for access to Tier 1 BSAT.

B. Additional Information Requested for Individuals in a Supervisory Role

In addition to the information collection for individuals acquiring Tier 1 BSAT access, for a person in a supervisory role (e.g., Pls, laboratory managers, RO, AROs, Owners/Controllers, etc.), the Federal Select Agent Program suggests that an entity consider the collection of information from the following sources consistent with institutional policy and applicable federal, state and local laws. The sources may include, but are not limited to the following:

- Review of performance evaluations
- History of grievance/complaint records
- Information gathered upon exit interviews with staff
- History of retention of subordinate staff
- Record of previous or current collaborations
- History of compliance with the Federal Select Agent Regulations
- Life changing events (personal and professional)

C. Interview with the Applicant and Assessment of Personal Behavior and Work Practices

An entity should consider interviewing each person requesting access to Tier 1 BSAT, with follow-up interviews as warranted. Interviewers should utilize open-ended questions to allow a person to discuss their views and ideas. This is also an opportunity for the entity to convey critical information to the person in order to discourage unsuitable persons and/or behavior and to encourage honesty. An interview also allows for the discussion of any missing or questionable information, and provides an opportunity for the entity to request additional information if there are concerns about incorrect, omitted or otherwise unfavorable information.

If possible, the entity should provide a common structure for all interviews to ensure consistency across interviews of people with similar functions. Interviewers should assess the individual's responses and attitudes toward biosafety, security, and Tier 1 requirements outlined in the select agent regulations. Discussions with individuals should include the benefits and challenges of work with Tier 1 BSAT, and the institutional expectations for self- and peer-reporting, incidents or conditions that may affect suitability, safety or security of Tier 1 BSAT.

Related to the potential for workplace violence, a personal interview may be able to ascertain an individual's history of drug or alcohol abuse, relationships with coworkers, attitude towards management/leadership/government, criminal history, and civil suit records. Red flags can include a defensive or hostile attitude, a history of frequent job changes, and a tendency to blame others for problems.

Individuals exhibiting behaviors that demonstrate they are incapable of controlling their actions or adhering to safety or security practices should be denied access to Tier 1 BSAT. An entity may consider temporary and permanent access restrictions in accordance with entity policy. Individuals with access to Tier 1 BSAT should be able to support both the entity's general and the laboratory-specific goals of safety, security, and compliance with the select agent regulations in the laboratory.

Chapter Four: Ongoing Suitability Assessment

Purpose

The regulatory requirement for an entity to determine an individual's suitability for access to Tier 1 BSAT is also intended to encompass an ongoing assessment of that individual to ensure that he or she continues to merit access. In addition to an initial assessment for access, it is necessary for entities to remain engaged and regularly update information pertaining to an individual's suitability for continued access to Tier 1 BSAT. Once an individual has access to Tier 1 BSAT, important resources that may be employed to assess his or her continuing suitability include the ongoing relationships with the RO, supervisor(s), PI(s), and colleagues as part of the culture of responsibility and security at the entity.

All Individuals with access to Tier 1 BSAT are subject to an entity's ongoing suitability assessment program. Individuals may be new employees who have been approved through the pre-access suitability assessment program, or individuals who had approved access to Tier 1 BSAT prior to the effective date of the security provisions (180 days after the publication of the select agent regulations).

This section provides guidance on implementing an ongoing assessment program. The examples provided may be used to fulfill the requirements of an ongoing suitability assessment program. However, as may be the case with pre-access suitability assessments, existing infrastructure and entity programs already in place may be extended or modified to institute an ongoing suitability assessment program, provided that they meet the regulatory requirements. The ongoing suitability assessment program requirements that must be implemented by entities registered for Tier 1 BSAT are covered under section 11(f)(3) of the select agent regulations. Requirements addressed in this section include:

- Mechanisms for self and peer-reporting of behaviors of concern. Specifically, incidents or conditions that could affect an individual's ability to have access to, or work safety with, Tier 1 BSAT or to safeguard Tier 1 BSAT from theft, loss, or release.
- Ongoing monitoring of suitability for individuals with access to Tier 1 BSAT.
- Training on entity policies and procedures for reporting, evaluations, and corrective actions concerning the assessment of personnel suitability for employees with access to Tier 1 BSAT.

The entity should make every effort to establish uniform and transparent procedures for ongoing suitability assessments, and implement these procedures to leverage other institutional resources (*i.e.*, legal counsel, administration, security, HR, etc.). If possible, a multi-resource, committee approach to an ongoing suitability assessment program development effort will aid the RO in making sound access decisions to ensure the safety and security of Tier 1 BSAT.

If an entity identifies one of the statutory prohibitors, as listed in **Figure 1**, during an ongoing suitability assessment, the RO must immediately remove the individual's access to select agents or toxins and notify the Federal Select Agent Program in accordance with the regulations.

Self-and Peer-Reporting {Section 11(f)(3)(i)}

The ongoing assessment procedures described in the entity's security plan must include self- and peer-reporting concerning incidents or conditions that could affect an individual's ability to have access to or

work safety with select agents or toxins, or safeguard select agents or toxins from theft, loss, or release. Entities may also want to consider establishing anonymous reporting mechanisms.

Example of Reportable Conditions, Behaviors, or Other Information

Individuals should be advised to share with their leadership any information that may cause concern for their well-being, that of others, or the safety and security of the entity or Tier 1 BSAT. Examples are provided below:

- 1) Circumstances that may affect SRA status of an individual;
- 2) Circumstances that may affect the ability of an individual to perform his or her job in a safe and secure manner (e.g., performance of duties declines markedly; significant increase in distraction or mistakes; increase in risk-taking behaviors);
- 3) Significant changes in behavior, attitudes, demeanor, or actions (e.g., increasingly withdrawn; significant and prolonged deterioration in appearance; unjustified anger or aggression; unexplained absences; signs of alcohol/drug abuse; criminal activity; and unexplained absences)
- 4) Stated or implied threats to colleagues, institutions, the security of Tier 1 BSAT, the well-being of laboratory animals, or the general public;
- 5) Willful non-compliance with the select agent regulations;
- 6) Any information that causes an individual to have concerns about his or her own ability to perform a job safely and securely;
- 7) Any circumstances that appear suspicious such as laboratory work that does not correspond to official project work or goals, requests for security or laboratory information without justification, acts of vandalism or property damage, attempts to gain unauthorized access for friends or colleagues;
- 8) Unlawfully carrying weapons (or carrying weapons in violation of institutional rules);
- 9) Providing false information on applications or other formal institutional documents; and
- 10) Unauthorized work performed by an individual(s) in a facility during off-hours.

Development of a Risk and Threat Reporting Mechanism

We recommend that entity leadership develop an integrated and transparent mechanism for reporting to appropriate entity authorities, all risks and threats in regards to the safety and security of Tier 1 BSAT, staff well-being, and public safety. It is critical that all individuals understand their duty to report such information or behaviors of concern. Therefore, risk and threat reporting mechanisms should be clear and employ a consistent analytical framework to determine any action that may be needed. Examples of potential resources that could be incorporated in an entity's reporting mechanism are exemplified in the violence prevention programs and reporting structures, established at many educational institutions, particularly in response to campus gun violence.

Entities are encouraged to utilize existing institutional guidelines and standards for reporting behavior, and to modify these standards and policies to apply specifically to the entity's Tier 1 BSAT security program. In some instances, medical conditions may need to be considered in the development of self- and peer-reporting policy. Conditions that directly affect an individual's immune status should be self-

reported through appropriate channels to allow for proper evaluation of the enhanced personal risks posed to individuals with such conditions.

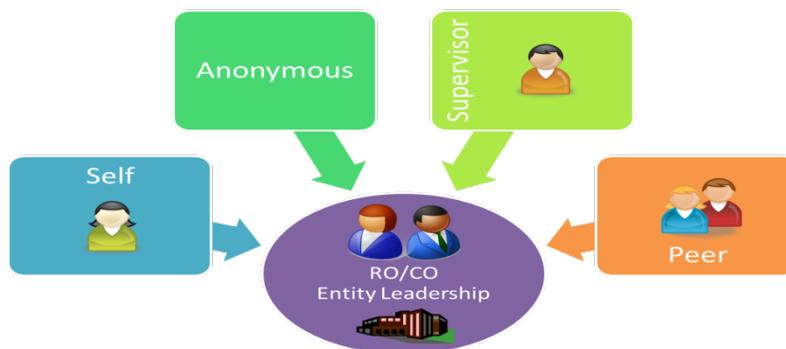
Entity leadership should become involved in supporting the development of reporting mechanisms and provide resources to assist ROs in carrying out reporting tasks. All individuals should be clearly instructed on all policies regarding self- and peer-reporting. Reporting policies include, but are not limited to:

- The types of information to report
- To whom the information should be reported
- How the reported information will be used to assess risks and determine actions
- Documentation requirements and availability of entity resources
- Confidentiality of the reporting process and the information collected

In some instances, the development of methods for anonymous reporting may encourage reporting, and should be considered when developing the entity's reporting policies and procedures. Entity leadership should make a concerted effort to ensure confidentiality when personal information is shared. **Figure 2** provides an outline of reporting options that may be considered for the development of self-, peer-, and anonymous reporting of information in response to behaviors determined by the entity that would increase the risk of a theft, loss, or release of a select agent or toxin. All reporting procedures should employ existing entity resources (i.e., HR, security, occupational health, etc.) in providing recommendations to the RO concerning access decisions in response to reported information.

For reporting procedures to achieve the desired goal of enhancing the safety and security of Tier 1 BSAT, a mutual trust must be forged between the reporter and the entity leadership. The ultimate goal of enhanced Tier 1 BSAT safety and security can be supported through the establishment of confidential avenues for self- and peer-reporting. The reporting mechanism should be fully described in the entity's security plan; and it should include defined communication channels capable of handling reported information in a uniform and confidential manner, and achieve consistent results in a judicious and efficient manner that supports the entity's mission of enhanced security.

Figure 2. Example Tier 1 BSAT Reporting Options for Communication of Concerning Behaviors, Incidents, Conditions, or Other Information



Ongoing Monitoring {Section 11(f)(3)(iii)}

The ongoing assessment procedures described in the entity’s security plan must include procedures for the ongoing suitability monitoring of individuals with access to Tier 1 BSAT.

Ongoing suitability monitoring can be accomplished in different ways. Multiple methods can be considered by the entity to determine what will work best for the entity, and personnel, using currently available resources. Some methods that should be considered include, but are not limited to:

- Annual technical, biosafety, and security performance evaluations of personnel having access to Tier 1 BSAT
- Periodic review of Tier 1 BSAT access requirements, as determined by users’ duties and responsibilities
- Annual evaluations as part of an occupational health program or independent evaluation
- Periodic review of criminal records (refer to **Appendix II. Options for Obtaining Criminal Records**) and visa status

Annual Tier 1 BSAT Technical, Biosafety, and Security Performance Evaluations

An annual evaluation of individuals with access to Tier 1 BSAT provides an opportunity to gauge the performance of the individual with respect to the adherence to entity biosafety and security procedures and training. The annual review also provides an opportunity for the individual’s supervisor and/or RO to review and acknowledge the importance of security, discuss the requirements of the select agent regulations, and address any potential problems that may have affected work performance in the past, or impact work performance in the future.

In developing a system for annual evaluations, the entity should consider systems that may already be in place in other areas of the institution, and extend these procedures and principles into the Tier 1 BSAT on-going monitoring program. In these cases, leadership may be able to draw on existing in-house resources and expertise in developing the annual evaluation procedures.

Entity leadership should consider effective methods for performance evaluation of all individuals who have access to Tier 1 BSAT. The methods utilized to evaluate personnel performance can vary among job titles, and should be implemented to determine an individual's overall suitability, including his or her willingness to adhere to current biosafety and security standards. For example, laboratorians and animal care staff should be evaluated by a supervisor or person most familiar with their laboratory work performance and attributes related to the safety and security of the Tier 1 BSAT.

Individuals in a supervisory role, such as laboratory managers or PIs, may require a different approach to render similar assessment information. Ongoing monitoring of individuals in a supervisory role (e.g., PIs, Laboratory Managers, RO, AROs, etc.) may include, but is not limited to the following:

- Review of performance evaluations
- History of grievance/complaint records
- Information gathered upon exit interviews with staff
- History of retention of subordinate staff
- Record of previous or current collaborations
- History of compliance with the Federal Select Agent Regulations
- Life changing events (personal and professional)

Special attention is warranted by entity leadership in determining the effectiveness of annual performance evaluations. The potential for conflicts of interest will present themselves throughout all levels of the evaluation process, and therefore it is imperative for entities to create uniform procedures for performance evaluations specific to the various job descriptions and particularly concerning the individual's suitability for access to Tier 1 BSAT. Similar to other areas of suitability assessment, the entity should consider involving other entity resources outside of the select agent program (i.e., security, HR, etc.) to gather diverse perspectives and assess suitability for all individuals with access to Tier 1 BSAT.

Access Privileges for Tier 1 BSAT

An enhancement to the biosafety and security of Tier 1 BSAT can be made through a simple evaluation of the needs of the workforce for physical access to these materials. By evaluating the needs of personnel based on their job duties and/or specific project status, entities should be able to divide their personnel into three categories: (1) personnel who currently do not need access to the Tier 1 BSAT, (2) personnel who only need access during regular working hours (e.g., Monday-Friday, 6A -7P), and (3) personnel who need access to Tier 1 BSAT 24 hours, 7 days a week (24/7). Evaluation of personnel access privileges will serve two goals: (1) optimize the number of users with access to Tier 1 BSAT based on each individual's work objectives, and (2) limit the duration of time Tier 1 BSAT can be accessed.

By optimizing the number of people who have access and/or limiting the time frame for access to Tier 1 BSAT, there are fewer opportunities for potential biosafety or security incidents to occur. An active evaluation of Tier 1 BSAT users' need for access privileges further delineates the personnel who are handling select agents or toxins most frequently, and involves laboratory personnel, supervisors, and entity leadership in access decisions on a continual basis. All entities will require some individuals to

have access to Tier 1 BSAT at all times as in accordance with emergency response procedures. However, not all Tier 1 BSAT users will require access at all times to the select agents or toxins. An evaluation should be conducted by an individual's supervisor or person most knowledgeable of the individual's project or required job duties, and capable of providing justification for unlimited access to reviewers/approvers. Review of access privileges and justifications involving access to Tier 1 BSAT should involve multiple persons, preferably in a hierarchy, with the final access approval decisions made by the RO.

The SRA approval process will serve as the first step for limiting access to select agents or toxins at the entity. Pre-access suitability assessments should serve to further limit the personnel approved to access Tier 1 BSAT. Once individuals have been approved for Tier 1 BSAT access, and have been accepted into an ongoing suitability assessment program, access privileges – particularly unlimited access – may be granted based upon job duty requirements and overall project needs.

Review of Criminal Records and Visa Status

A review of criminal records and personnel visa status performed every 3 years or as needed may be considered to identify criminal behaviors that fall outside the scope of the items listed in Figure 1. Information of this type, discovered by or disclosed to the entity, should be assessed using entity resources (e.g., security, HR, legal, and entity leadership) to determine an individual's suitability for access to Tier 1 BSAT, either initially or on an on-going basis.

Training {Section 11(f)(3)(ii)}

The ongoing assessment procedures described in the security plan must provide for the training of employees with access to Tier 1 BSAT on entity reporting policies and procedures, evaluation, and corrective actions concerning the assessment of personnel suitability.

As presented in section 15 of the select agent regulations, entities with Tier 1 BSAT must conduct annual insider threat awareness briefings on how to identify and report suspicious behaviors.

This training may be coordinated with other required training, encompassing biosafety, security, incident response, and job specific duties, in order to conserve resources and time. The primary focus of the annual Tier 1 BSAT specific training is (1) to promote insider threat awareness, and (2) inform individuals with access approval for Tier 1 BSAT of the policies and procedures contained in the entity suitability assessment program. This training could include, but is not limited to the following:

- Insider threat awareness
- Behaviors of concern
- Entity pre-access suitability policies concerning Tier 1 BSAT
- Self and peer reporting procedures
- Statutory prohibitors
- Tier 1 BSAT user evaluation process
- Entity policy on ongoing suitability assessment procedures
- Entity policy on ongoing suitability monitoring procedures

- Corrective actions, procedures and policies
- Procedures for voluntary and involuntary removal of Tier 1 BSAT access
- Information security (e.g., need to know)

All training should be documented and the training records kept in accordance with section 17 of the select agent regulations.

Chapter Five: Transition of Individuals with Access to Tier 1 BSAT at the Effective Date of the Regulations

Individuals having approved access to Tier 1 BSAT prior to the effective date of the security provisions (180 days after the publication of the select agent regulations) are not required to have a pre-access suitability assessment. Such individuals, however, will be subject to the entity's ongoing assessment and monitoring program. An entity has the discretion as to any pre-access suitability procedures used to transition individuals, currently listed on the entity's registration as having access to Tier 1 BSAT, prior to enrollment into an ongoing suitability assessment program.

All individuals who already have approved access to Tier 1 BSAT must be enrolled in the entity's ongoing suitability assessment program to retain access to Tier 1 BSAT as of the effective date the security provisions (180 days after the publication of the select agent regulations).

Chapter Six: Denial, Termination or Suspension of an Individual's Access to Tier 1 BSAT

Purpose

Section 10 of the select agent regulations requires that the RO immediately notify APHIS or CDC when an entity has terminated an individual's access to select agents or toxins, regardless of whether or not this person had access to Tier 1 BSAT. The notification must include the reason for termination of access. Notification should be submitted in writing via mail, fax, or email to APHIS or CDC.

Termination of access privileges to Tier 1 BSAT may occur when an individual: (1) no longer is employed by the institution, (2) has job duties that no longer require access to Tier 1 BSAT, (3) voluntarily requests to have Tier 1 BSAT access privileges removed, or (4) is found unsuitable for access to Tier 1 BSAT based on an entity's assessment of suitability. In some instances, an individual may retain access privileges to non-Tier 1 BSAT following termination of his/her access to Tier 1 BSAT.

Voluntary Removal from Access to Tier 1 BSAT

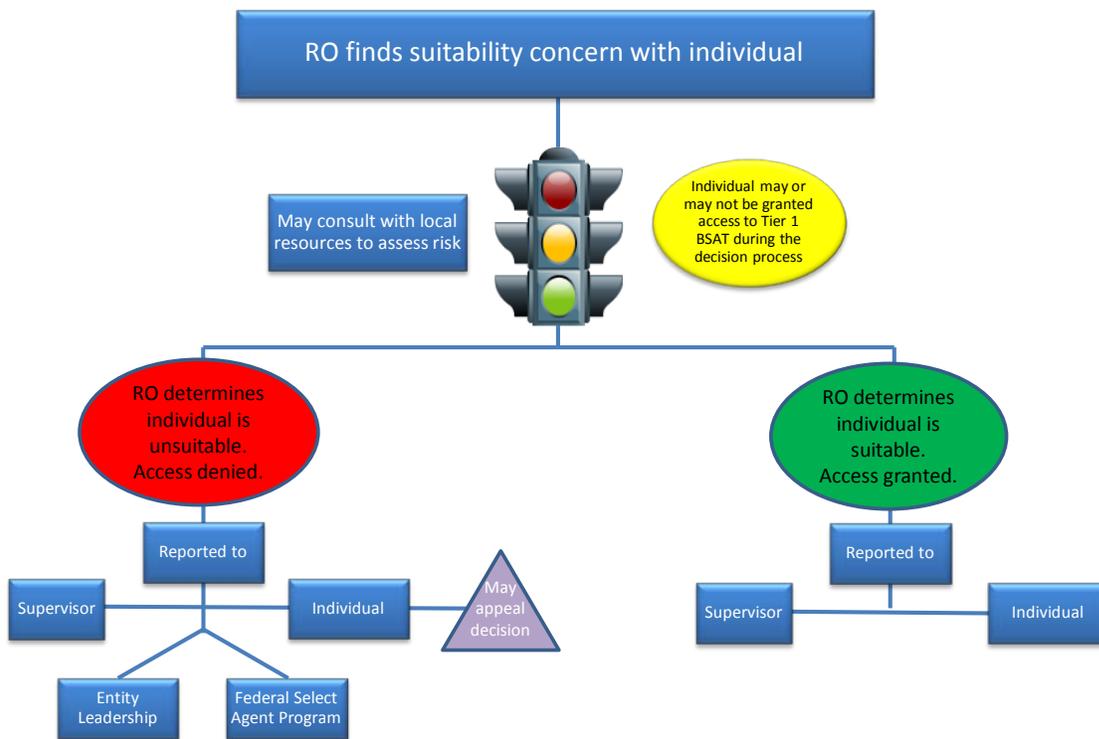
Entity leadership is encouraged to develop a mechanism for individuals to temporarily "opt out" of having access to Tier 1 BSAT for defined periods of time. The "opt out" provision should be a voluntary act initiated by the person having Tier 1 BSAT access through the self-reporting process, and granted by entity leadership for individuals who otherwise would be deemed suitable for access to Tier 1 BSAT. Examples of circumstances in which an "opt out" would be appropriate include extended periods of illness or other leave. Individuals who are removed from Tier 1 BSAT access as a result of an ongoing suitability assessment should be routed through a separate process initiated by the entity. These types of "opt outs" are not required to be reported to the Federal Select Agent Program.

Denial, Termination or Suspension of Individual's Access to Tier 1 BSAT

During the pre-access suitability assessment, an individual may be denied access to Tier 1 BSAT based on the results of the assessment. It is also plausible that information collected or reported (self or peer) as a result of the ongoing suitability assessment program may lead to the termination or suspension of an individual's access to Tier 1 BSAT. Information related to the safety and security of Tier 1 BSAT could result in a temporary suspension of an individual's access to allow for further evaluation of the situation. It is unrealistic to attempt to describe every possible situation that may arise. Hence, to help mitigate the adverse consequences of unforeseeable situations, the procedures in place for the gathering, interpretation, and sharing of information, and decision making should be consistent and allow for the uniform treatment of negative information obtained or reported to entity leadership. Suspension of individual's access to Tier 1 BSAT is not required to be reported to the Federal Select Agent Program. Denial, termination, or suspension of an individual's access to Tier 1 BSAT should not be taken lightly, and could potentially have severe consequences for the individual's work objectives and/or career. Therefore, these decisions should be made by entity leadership in consultation with the entity's legal counsel utilizing existing entity resources for technical assistance and guidance.

Further, if during the ongoing monitoring of suitability the entity discovers evidence of statutory prohibitors or information that might warrant the rescinding of SRA approval, the RO should immediately remove the individual’s access to select agents or toxins and immediately notify the Federal Select Agent Program.

Figure 3. Reporting Procedures for Suitability Concern Identified During Ongoing Monitoring of Individual with Access to Tier 1 BSAT



Appeal Consideration

Although not required by the select agent regulations, the entity might consider developing a policy in accordance with state and local law, implementing an administrative procedure allowing an individual to appeal a negative suitability assessment decision. This process could involve representatives from administrative and other areas of institutional oversight (i.e., security, HR, legal, etc.) to provide an independent review of the final decision.

References

1. Connecting Research in Security to Practice (CRISP) report on “Strategies to Detect and Prevent Workplace Dishonesty” (<http://www.asisonline.org/foundation/dishonesty.pdf>)
2. Defense Science Board Task Force on Department of Defense Biological Safety and Security Program (<http://www.acq.osd.mil/dsb/reports/ADA499977.pdf>)
3. Department of Justice publication: “Workplace Violence: Issues in Response” (<http://www.fbi.gov/stats-services/publications/workplace-violence>)
4. Executive Order 13486 Working Group on Strengthening Laboratory Security in the United States (<http://edocket.access.gpo.gov/2009/pdf/E9-818.pdf>)
5. Federal Experts Security Advisory Panel report, found at: (<http://www.phe.gov/Preparedness/legal/boards/fesap/Documents/fesap-recommendations-101102.pdf>)
6. National Academy of Sciences report: “Responsible Research with Biological Select Agents and Toxins,” (http://www.nap.edu/catalog.php?record_id=12774)
7. National Academies Committee on Laboratory Security and Personnel Reliability Assurance Systems for Laboratories Conducting Research on Biological Select Agents and Toxins (<http://www8.nationalacademies.org/cp/projectview.aspx?key=49097>)
8. National Science Advisory Board for Biosecurity report: “Enhancing Personnel Reliability Among Individuals with Access to Select Agents” (<http://oba.od.nih.gov/biosecurity/meetings/200905T/NSABB%20Final%20Report%20on%20PR%205-29-09.pdf>)
9. “Regulatory Impact Analysis for 42 CFR Part 73: Possession, Use, and Transfer of Select Biological Agents and Toxins Final Rule”. Centers for Disease Control and Prevention, Department of Health and Human Services. February 3, 2005.
10. “The US Postal Service Response to the Threat of Bioterrorism through the Mail,” Congressional Research Service Report for Congress, February 2002. <<http://www.au.af.mil/au/awc/awcgate/crs/rl31280.pdf>.> Date Accessed: May 18, 2010
11. “Transcript of Amerithrax Investigation Press Conference,” August 6, 2008 (<http://www.justice.gov/opa/pr/2008/August/08-08-0697.html>)

Appendices

The information found in the appendices consists of suggested examples that an entity may consider in development and implementation of personnel suitability assessments for access to Tier 1 BSAT. The user is not required to use, or limited to, the information provided in the appendices.

[Appendix I. Example of an Entity's Pre-access Suitability Process](#)

[Appendix II. Options for Obtaining Criminal Records](#)

[Appendix III. Example Questions for Use in Reference Interviews](#)

[Appendix IV. Visitors for short term training with Tier 1 BSAT](#)

[Appendix V. Example of self and peer reporting process flow](#)

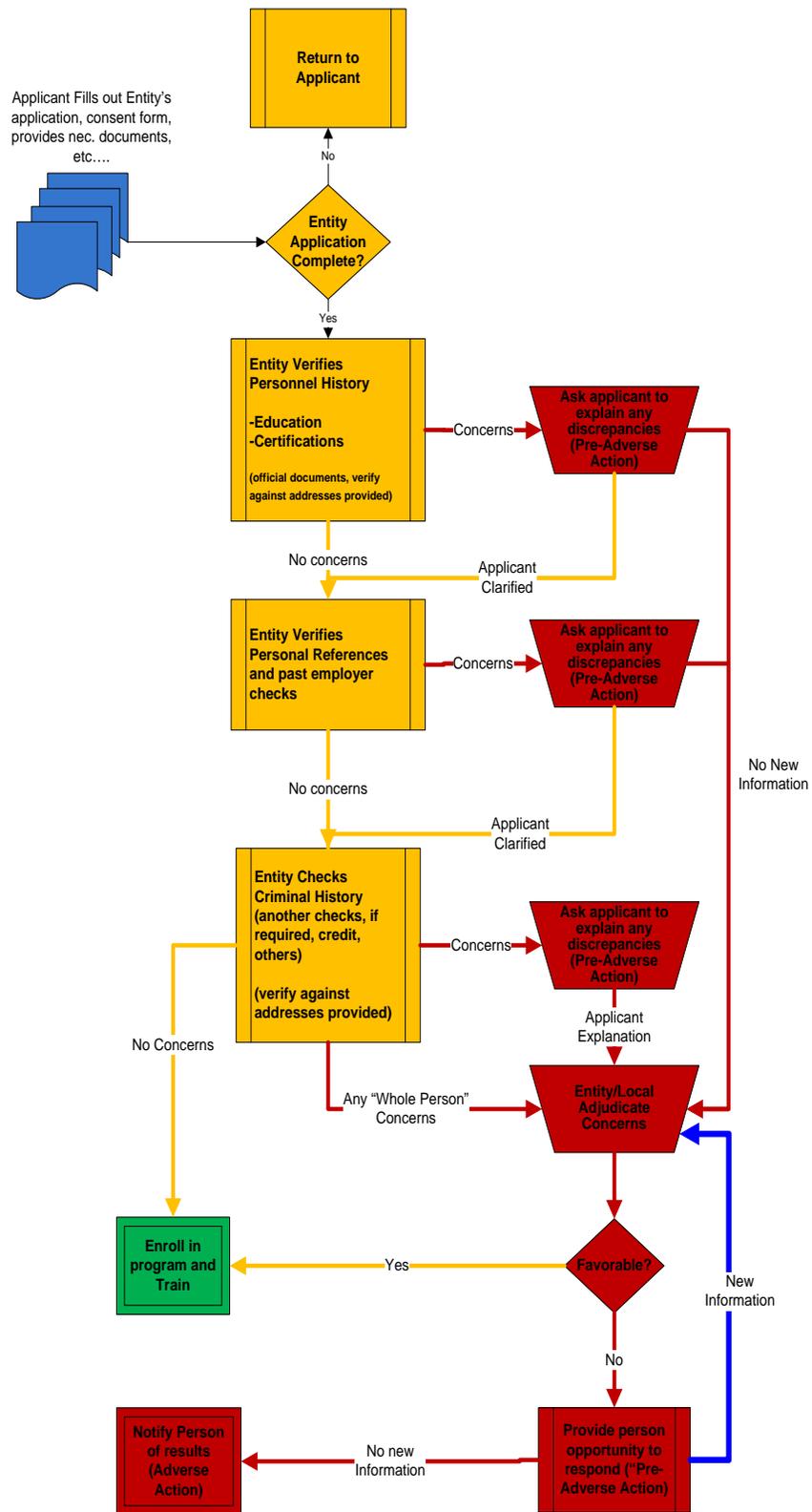
Appendix I. Example of an Entity's Pre-access Suitability Process

Entities must establish their own suitability program. As part of the program, they have to establish what is checked during the pre-access suitability assessment. This is an example of a logical sequencing of an entity's suitability checks.

These pre-access checks are for personnel with access to Tier 1 BSAT. They are beyond the required Security Risk Assessment (SRA). All personnel with access to any select agent or toxin must have an SRA.

In this case, the entity has sequenced the checks both to ensure the 'whole person' is considered while not needlessly spending money. The entity checks education and certifications first (fast/inexpensive). If they are valid, the entity then checks references. If they check out, the entity checks criminal history (longer/more expensive). Doing it in this order also ensures that criminal records (if any) are viewed in the light of all the other factors.

At each step, the applicant is given a chance to respond. In the end, if there are no concerns, the person is enrolled in the suitability program. If there are concerns, they are addressed.



Appendix II. Options for Obtaining Criminal Records

- An Entity may use the campus police department, or public safety office. There may be privacy limitations but an investigator can be recruited to serve in a role that supports the RO.
- An entity may also follow the procedures provided by the state. A public university may not be able to do this.
 - The Virginia Department of Criminal Justice Services provides a clear process for private entities. In Virginia (open records state) you can do a statewide check that covers all jurisdictions. http://www.vsp.state.va.us/CJIS_Criminal_Record_Check.shtm
 - Whereas in Massachusetts (non-open records state) one must do a county-by-county but one must beware of the applicants that have "sealed" their Criminal Offender Record Information <http://www.massresources.org/cori.html#why>
- Additionally, there are a number of vendors that provide criminal background and civil orders checks on the internet. Reports are usually provided as a digest of all findings instead of providing each official report for each jurisdiction.
- An entity may also hire a private investigation firm for this function. Entities may prefer this option because a comprehensive search can often be performed within minutes. There are competent and professional outfits that are available that routinely provide these types of services for a nominal fee.
- Finally, the entity may require that the applicant provide the records him/herself by contacting the appropriate State/local agencies. If State law prohibits the registered entity from conducting a criminal records check on applicants, we recommend that access to Tier 1 BSAT depend on an applicant providing a certified criminal record from places of residence in the past 7 years, or since the age of 18, whichever is shorter. If this mechanism is utilized at an entity, we recommend that this request be disclosed during the application process to access Tier 1 BSAT.

Note: An entity may consider conducting a criminal conviction and arrest history record check for individuals at any time prior to granting access, and as part of an ongoing suitability monitoring program for Tier 1 BSAT. Entities are encouraged to employ institutional resources already in place in consideration of best practices for implementing these records checks.

Entity leadership should take into account that laws differ by state and municipality regarding the legality of employers requesting criminal records checks. Entity leadership could utilize information provided by the applicant regarding time spent in other countries, states, and localities (i.e., prior residences, employment history, etc.) to guide criminal background checks.

If an applicant has resided in other countries, states, and localities, a local criminal background check may be insufficient. A broader check to include other states is recommended for completeness and to address current gaps in criminal records databases because:

- 1) No central repository exists for federal, state, and local (i.e., county, parish, municipal, etc.) criminal records.
- 2) Not all states have automated systems for collecting data from reporting agencies and local jurisdictions. The content, accuracy, quality and timeliness of the data vary considerably among the states.
- 3) No federal law imposes standards for collecting, indexing, searching, and using criminal record data. Among the 50 states, standards vary for collecting the four types of criminal records – arrest, criminal court (federal, state and local), corrections (federal, state and local), and state criminal repository records.

The RO and/or entity leadership may find reviewing these records useful to ensure that all concerning criminal activity is taken into account when making suitability determinations. Therefore, we recommend that entity leadership discuss legal mechanisms for obtaining this information with their legal counsel, HR professionals, local security or law enforcement, or their local FBI WMD Coordinator. It is up to each entity to determine what type of check may be sufficient for a particular institution. Of note, several states are beginning to provide records publicly via the internet (e.g., court actions). An ideal check would include obtaining information in every country, state, and/or county that the applicant has lived, worked, or attended school.

Entities should consider the following information:

- Criminal records may contain errors.
- Entities are encouraged to verify criminal history before the adjudication process begins. This is especially true when using an 'online source.'
 1. Check the local records. Many jurisdictions have government owned and operated online access where the accuracy of the conviction record can be verified.
 2. Check the legal docket for the court in question. Dockets contain more information than simply conviction data; they have the history of the case. Many jurisdictions have online access where the accuracy of the conviction along with any future matters (set-asides, expungements) which affect the record.
 3. If the conviction record conflicts with a local record check, or the docket reveals additional information, the criminal data may no longer meet standards to be considered for adjudication.

Appendix III. Example Questions for Use in Reference Interviews

- References should be asked questions so the interviewer can understand the nature of the reference's relationship to the applicant, in what context they were acquainted, and how well the references knows the individual being assessed such as:
 - What was the period of time in which you worked with the applicant?
 - Describe your relationship to the applicant while at your institution.
 - Did the applicant report directly to you or another supervisor?
- References should be asked specific questions about the applicant's performance of duties and personality while working as a member of a team.
 - What were the applicant's duties and how well did he/she perform while at your institution?
 - Can you describe the applicant's ability to work as part of a team?
 - While the applicant was at your institution, did you have any interactions with the applicant that might have been inconsistent or unusual?
- References should be able to describe the applicant's willingness to abide by applicable safety and security regulations or policies. This speaks to potential issues with authority that may cause an individual to have difficulties adhering to the principles of safety and security required for work with Tier 1 BSAT.
- Interviewers should attempt to confirm any information on the applicant's application. For example, a reference could be asked if they remember where the applicant undertook undergraduate or graduate training, or what city they may have lived in at a given time. Of course, these questions are not useful if the reference does not know the answers, but if their answers are significantly different from the responses of the applicant, those details should be reviewed with the applicant for accuracy.
- References should be questioned as to whether they would hire the applicant again, and if not, why not.

Appendix IV. Visitors for short term training with Tier 1 BSAT

There are instances when a visitor may visit a registered entity to receive specific training on Tier 1 BSAT. Typically in these circumstances a visitor for training (“trainee”) is hosted by another entity (the “host” entity) on a one-time basis of a limited duration for training. These individuals will have access to Tier 1 BSAT as part of their training. Their access is not specifically limited to any time period, but it is usually less than 30 days. This guidance provides a description of what suitability requirement will be needed for that trainee in such situations.

The regulatory requirements do not change for this situation but there are additional personnel security options. Host entities must still verify that each trainee has an SRA, are on the host entity’s registration, and verify a justification for the training. Since the training involves access to Tier 1 BSAT, trainees must receive entity specific training on the host entity’s policies and procedures concerning personnel suitability, however this may be specific training for trainees and different than training for permanent employees. All personnel who have access to the Tier 1 BSAT must have gone through pre-access suitability and are subject to on-going assessments. However, with trainees, entities have options when addressing pre-access suitability and on-going assessment.

The hosting entities have options on how to address pre-access suitability for trainees. Host entities can always enroll trainees into its pre-access suitability program. However, if that is not feasible, an entity can rely on the home entity’s checks. This may include:

- Verify with the home entity or organization that the trainee has gone through a pre-access suitability program and is subject to ongoing assessment.
- Verify with the home entity or organization that the trainee has gone through similar pre-access checks (references, employment, criminal) and accept those checks as sufficient.
- Verify with home entity which pre-access checks have been accomplished and work with the home entity to complete any checks which were not done. Hosting entities are strongly encouraged to adjudicate any new derogatory information with the home entity prior to making an access decision.

The host entity can deny access to Tier 1 BSAT to any trainee if the host entity cannot verify the trainee’s status.

Options for the ongoing assessment requirement in for trainees include:

- Ensure training is monitored. For example, an instructor observes the work and verifies that the trainee is engaged only in that work.
- Limit access to the registered area. Trainees should only have access to the registered area during specific work or training times.
- Limit access within the registered areas. Trainees should not be given access to storage freezers or other registered areas not directly involved in the training program.

If a trainee demonstrates a behavior which may compromise safety or security, their access to select agents and toxins should be removed.

The host entity is responsible for maintaining records outlined in Section 17. If an entity chooses to rely on the home entity’s checks, that must be documented and retained as well.

Appendix V. Example of self and peer reporting process flow

