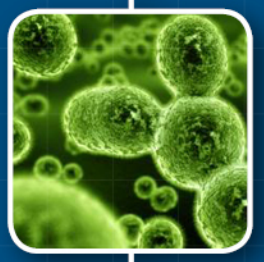


SUITABILITY ASSESSMENT PROGRAM GUIDANCE

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

MARCH 2017

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

Animal and Plant Health Inspection Service (APHIS)
Agricultural Select Agent Program

Change/Highlight Section

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: AgSAS@aphis.usda.gov

Revision History:
October 12, 2012: Initial posting
June 24, 2013 (Revision 1): The revisions are primarily changes to correct editorial errors from the previous version.
March 2017 (Revision 2): The revisions reduce the document to essential regulatory guidance and correct editorial errors from the previous version.

Introduction

The purpose of this guidance document is to assist entities in the development of a site-specific suitability assessment program for individuals with access to Tier 1 select agents and toxins (BSAT), according to section 11(f) of the select agent regulations (42 CFR § 73.11, 7 CFR § 331.11, and 9 CFR § 121.11). This guidance provides recommendations for meeting this requirement; however, the entity should develop the suitability assessment plan according to the specific conditions of their registered space.

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. An entity must ensure that it is compliant with all federal, state and local employment and privacy laws in the development of all suitability assessment plans.

Contents

Change/Highlight Section 2
Introduction 2
Suitability Assessments 4
Suitability Assessment Program Leadership Requirements 4
Pre-Access Suitability Assessments 5
Pre-Access Suitability Assessment: 5
Additional Information Requested for Individuals in a Supervisory Role 7
Applicant Interview 7
Ongoing Suitability Assessments 8
Self-and Peer-Reporting – Section 11(f)(3)(i) 9
Ongoing Monitoring 9
Development of a Risk and Threat Reporting Mechanism 9
Examples of Reportable Conditions, Behaviors, or Other Information 10
Access Privileges for Tier 1 BSAT 10
Individuals with Access to Tier 1 BSAT 11
Training (Section 11(f)(3)(ii)) 12
Denial, Termination or Suspension of Tier 1 BSAT Access 12
Appeal Consideration 13
Voluntary Removal from Access to Tier 1 BSAT 13
Denial, Termination or Suspension of Individual's Access to Tier 1 BSAT 13
Visitors for short term training with Tier 1 BSAT 13
References 14
Appendices 15
Appendix I. Example Questions for Use in Reference Interviews 16
Appendix II. Options for Obtaining Criminal Records 17
Appendix III. Example Pre-Access Suitability Adjudication Flow Diagram 19
Appendix IV. Example Ongoing Suitability Assessment Process Flow 20

Suitability Assessments

The purpose of a suitability assessment program is to reduce the risk of an insider threat, which is an individual or group with authorized access to Tier 1 BSAT as part of their job who has the potential to misuse Tier 1 BSAT. Examples of an 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.

Suitability Assessment Program Leadership Requirements

The suitability assessment program can be divided into two sections. The pre-access suitability assessment determines whether an individual has the appropriate credentials and background to be allowed access to Tier 1 BSAT. The ongoing suitability assessment allows the entity to monitor the behavior of the individual through observation, self-reporting, and peer-reporting to ensure that the individual continues to be suitable for Tier 1 BSAT access.

While the Responsible Official is responsible for ensuring the development and implementation of the suitability assessment program, entity leadership should provide support and resources to ensure that the program is effective. Leadership may include the Owner/Controller, CEO, Ranking Official, Department Chair and other senior leadership personnel. Entity leadership can support the development and implementation of the suitability assessment program as follows:

- Collaborating with the RO to develop and implement a suitability assessment program for personnel access to Tier 1 BSAT.
- Providing 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, Human Resources (HR), security personnel, legal counsel, occupational health program, etc.).
- Supporting the RO in the establishment of policies and administrative procedures to execute an effective suitability assessment program. Essential program components may include:
    - Routine pre-access and ongoing suitability assessment protocols.
    - Policies that allow an individual to voluntarily “opt out” of Tier 1 BSAT work (coordination with human resources, supervisors, etc.).
    - Policies that address the temporary or permanent denial of access to Tier 1 BSAT.
    - Policies and procedures to manage appeals of administrative actions that may result from suitability assessments.
- Supporting efforts to protect from retribution those individuals reporting adverse or derogatory information (i.e., plan for appropriately handling false reports).
- Establishing communication channels for the sharing of suitability program information, as appropriate, among relevant stakeholders and the RO. At a minimum, this involves 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.

- Promoting a culture of reliability, safety and security in all matters dealing with access to Tier 1 BSAT.
- Ensuring the authorized need, anonymity and confidentiality of personal information when shared.

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.

Pre-Access Suitability Assessments

Section 11(f)(1) of the select agent regulations requires entities registered to possess, use, or transfer Tier 1 BSAT to include the procedures to evaluate person's suitability for access to these materials in its security plan.

The entity should develop a policy for collecting, evaluating, and protecting personnel information based on institutional policy and federal, state, and local laws. Please see the sample Pre-Access Suitability Adjudication Flow for a detailed example procedure. The entity may have previously requested some or all of this information from an employee prior to hiring, with the information (such as criminal, 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. A consideration could be to include the requirement for suitability assessments in a job announcement.

Pre-Access Suitability Assessment:

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. The following are examples of information which could be reviewed for each individual undergoing the pre-access suitability assessment, as appropriate and consistent with the time frame according to institutional policy, and federal, state, and local law:

1. **Home Address History** – This information could be used to corroborate local criminal conviction and arrest record checks and other information provided by the person. Include at minimum the states/countries where the individual has resided.
2. **Work History** – Assess prior work experiences for security concerns. Requesting multiple professional work references provide a more "whole person" assessment of this individual. If a person is unwilling to provide any work references, careful consideration should occur before issuing the person access approval to Tier 1 BSAT.
3. **Education History** – Consideration should be given to the accreditation of the educational institutions that the individual has claimed to have attended. Consider requesting records from post-secondary institutions the individual claims to have attended, and any other applicable supporting documentation (e.g. if the person has not attended a post-secondary institution).
4. **Criminal History** – 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., misdemeanors). Remaining consistent with state and local laws, obtaining criminal records to:
    - Verify personal reports of criminal

activity and determine deliberate withholding of information. Assess the person's honesty and truthfulness in answering relevant questions. The person's willingness to provide facts may be considered a 'positive', while an attempt to cover up an event would be assessed as a 'negative.'

- Determine the nature and seriousness of any offenses and their relevance to Tier 1 BSAT job duties.
- Determine patterns of behavior that may be of concern to the security and safety of the program. For example, a record of multiple arrests, even without conviction, may point to an instability that may indicate a pattern of behavior not consistent with suitability for access to Tier 1 BSAT.
- All events should be put into the context of the "whole person." Consideration should be given to:
    - The nature of the event and whether the demonstrated behavior increases the risk in the laboratory.
    - An individual's circumstances at the time of an event.
    - The time that has passed since the event of concern.
    - The total number of events causing concern.
- Consider, as possible mitigating factors, positive information about the person, 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.
- Utilizing security personnel and legal counsel to evaluate criminal conviction and arrest records to determine suitability of an individual will assist the RO in the evaluation.

5. **Resume or Curriculum Vitae** – Entity can use this information to assess the person's recent paid and unpaid work experiences, scientific publications, and affiliations for research with select agents or toxins, as applicable. Verification of any degrees claimed on the resume or curriculum vitae with the registrar or other administrative body of each institution could be useful.
6. **Professional License and Certification History** – 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). Contacting State boards of licensure in each location where the individual has lived may 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)** – Establish procedures to verify the identity of the person. Typically, an individual's visa status is tied to employment.
8. **References and Contact Information** – Consider requesting professional and peer references for each individual. Ask questions that elicit an impression of the person's reliability, trustworthiness, honesty, judgment, emotional or mental stability, 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. 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.

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.

Additional Information Requested for Individuals in a Supervisory Role

When considering Individuals acquiring access to Tier 1 BSAT who will be in a supervisory role (e.g., PIs, laboratory managers, RO, AROs, owners/controllers, etc.) may require further collection of information from sources such as

- 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)

Applicant Interview

The entity may interview each person requesting access to Tier 1 BSAT to discuss the person's views and ideas and to convey critical information to the person to encourage honesty and discourage unsuitable behavior. 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. See Example Interview Questions for more detailed recommendations.

Interviewers may assess the individual's responses and attitudes toward biosafety, security, and Tier 1 requirements outlined in the select agent regulations. Discussions with individuals could 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.

Individuals repeatedly exhibiting behaviors that demonstrate they are incapable of 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.

Ongoing Suitability Assessments

Section 11(f)(3) of the select agent regulations require the entity to ensure that individuals granted access to Tier 1 BSAT continue to merit access through an ongoing suitability assessment program.

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 regulations require an ongoing assessment of individuals with access to Tier 1 BSAT to ensure that he or she continues to merit access. Entities must remain engaged and regularly update information pertaining to an individual's suitability for continued access to Tier 1 BSAT.

The entity should establish procedures for ongoing suitability assessments, and implement these procedures to leverage other institutional resources (e.g., legal counsel, administration, security, HR¸ etc.). If possible, use a committee approach to an ongoing suitability assessment program development effort to 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 of a restricted person listed below during an ongoing suitability assessment, the RO must immediately remove the individual's access to select agents or toxins and notify FSAP in accordance with the regulations.

A "restricted person" is an individual who falls under one or more of the following categories:

- Is under indictment for a crime punishable by imprisonment for a term exceeding 1 year.
- Has been convicted in any court of a crime punishable by imprisonment for a term exceeding 1 year.
- Is a fugitive from justice.
- Is an unlawful user of any controlled substance (as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802)).
- Is an alien illegally or unlawfully in the United States.
- Has been adjudicated as a mental defective or has been committed to any mental institution.
- (i)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 U.S.C. App. 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; or (ii) acts for or on behalf of, or operates subject to the direction or control of, a government or official of a country described in this subparagraph.
- Has been discharged from the Armed Services of the United States under dishonorable conditions.

- Is a member of, acts for or on behalf of, 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((iv).

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.

Ongoing Monitoring

Section 11(f)(3)(iii) require that 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.

Multiple methods can be used to set up an ongoing assessment procedure, using currently available resources, including but 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 and visa status.

Development of a Risk and Threat Reporting Mechanism

Develop an integrated and transparent policy for self- and peer-reporting all risks and threats in regards to the safety and security of Tier 1 BSAT, staff well-being, and public safety to the appropriate authorities. Fully describe the reporting mechanism in the entity's security plan, including defined communication channels capable of handling reported information in a uniform and confidential manner.

All individuals must understand their duty to report such information or behaviors of concern. Risk and threat reporting mechanisms should be clear and employ a consistent analytical framework to determine any action that may be needed. Utilize existing institutional guidelines and standards for reporting behavior, and 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 support 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 could 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.
- Anonymous reporting.
- Policies to prohibit reprisal for reporting.

All reporting procedures could 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.

Examples 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 include:

- Circumstances that may affect SRA status of an individual.
- 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).
- 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).
- Stated or implied threats to colleagues, institutions, the security of Tier 1 BSAT, the well-being of laboratory animals, or the general public.
- Willful non-compliance with the select agent regulations.
- Any information that causes an individual to have concerns about his or her own ability to perform a job safely and securely.
- 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.
- Unlawfully carrying weapons (or carrying weapons in violation of institutional rules).
- Providing false information on applications or other formal institutional documents.
- Unauthorized work performed by an individual(s) in a facility during off-hours.

Access Privileges for Tier 1 BSAT

An enhancement to the biosafety and security of Tier 1 BSAT can be made through an 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:

- Personnel who currently do not need access to the Tier 1 BSAT
- Personnel who only need access during regular working hours (e.g., Monday-Friday, 6A -7P)
- 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:

- Optimize the number of users with access to Tier 1 BSAT based on each individual's work objectives.
- 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 could be conducted by an individual's supervisor or the 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 may 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.

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 1 BSAT. Individuals should advise entity leadership of any issues that could have an adverse impact on their performance, suitability, or safety while performing Tier 1 BSAT duties. The entity should establish policies for the following Individual responsibilities:

- 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.

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:

- 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.

Denial, Termination or Suspension of Tier 1 BSAT Access

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:

- Is no longer employed by the institution.
- Has job duties that no longer require access to Tier 1 BSAT.
- Voluntarily requests to have Tier 1 BSAT access privileges removed.
- 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.

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.

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 could 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. 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. The procedures in place for the gathering, interpretation, sharing of information, and decision making should be consistent and allow for the uniform treatment of negative information obtained or reported to entity leadership. Denial, termination, or suspension of an individual's access to Tier 1 BSAT can potentially have severe consequences for the individual's work objectives and/or career. Therefore, would recommend these decisions 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 identified as a restricted person listed above 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 FSAP.

Visitors for short term training with Tier 1 BSAT

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.

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, is on the host entity's registration, and has 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 ongoing 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.

Note: 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 in 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.

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.

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-opa-697.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 Questions for Use in Reference Interviews
Appendix II. Option for Checking Criminal Records
Appendix III. Example Pre-access Suitability Adjudication Flow Diagram
Appendix IV. Example Ongoing Assessment Flow Diagram

Appendix I. 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?
    - Did the applicant follow entity safety and security policies?
- References should be asked specific questions about the applicant's performance of duties and personality while working as a member of a team, such as:
    - 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 asked whether they would hire the individual again and why or why not.

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, though public university may not be able to do this.

Additionally, there are a number of vendors that provide criminal background and civil order 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 (e.g., 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:

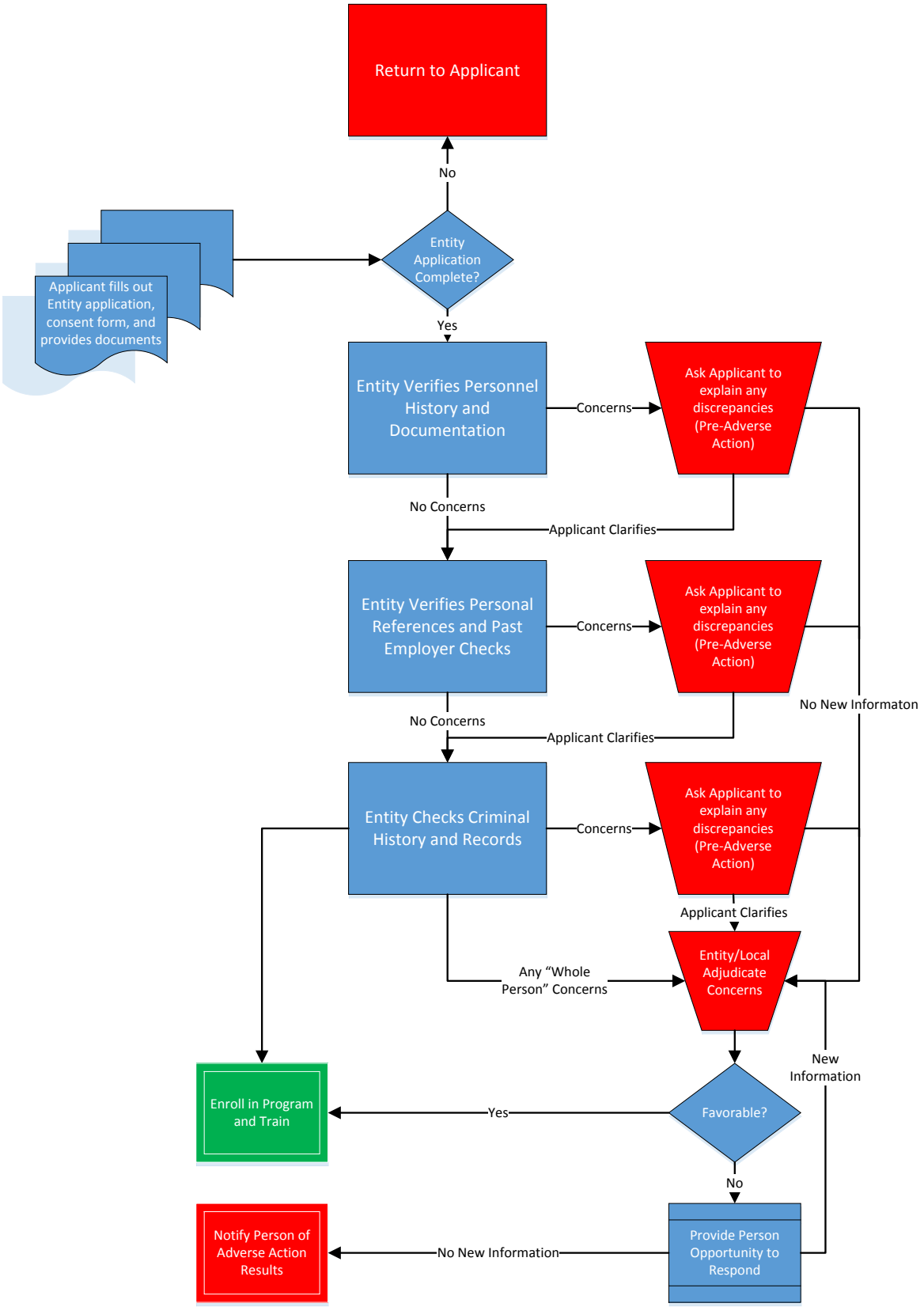
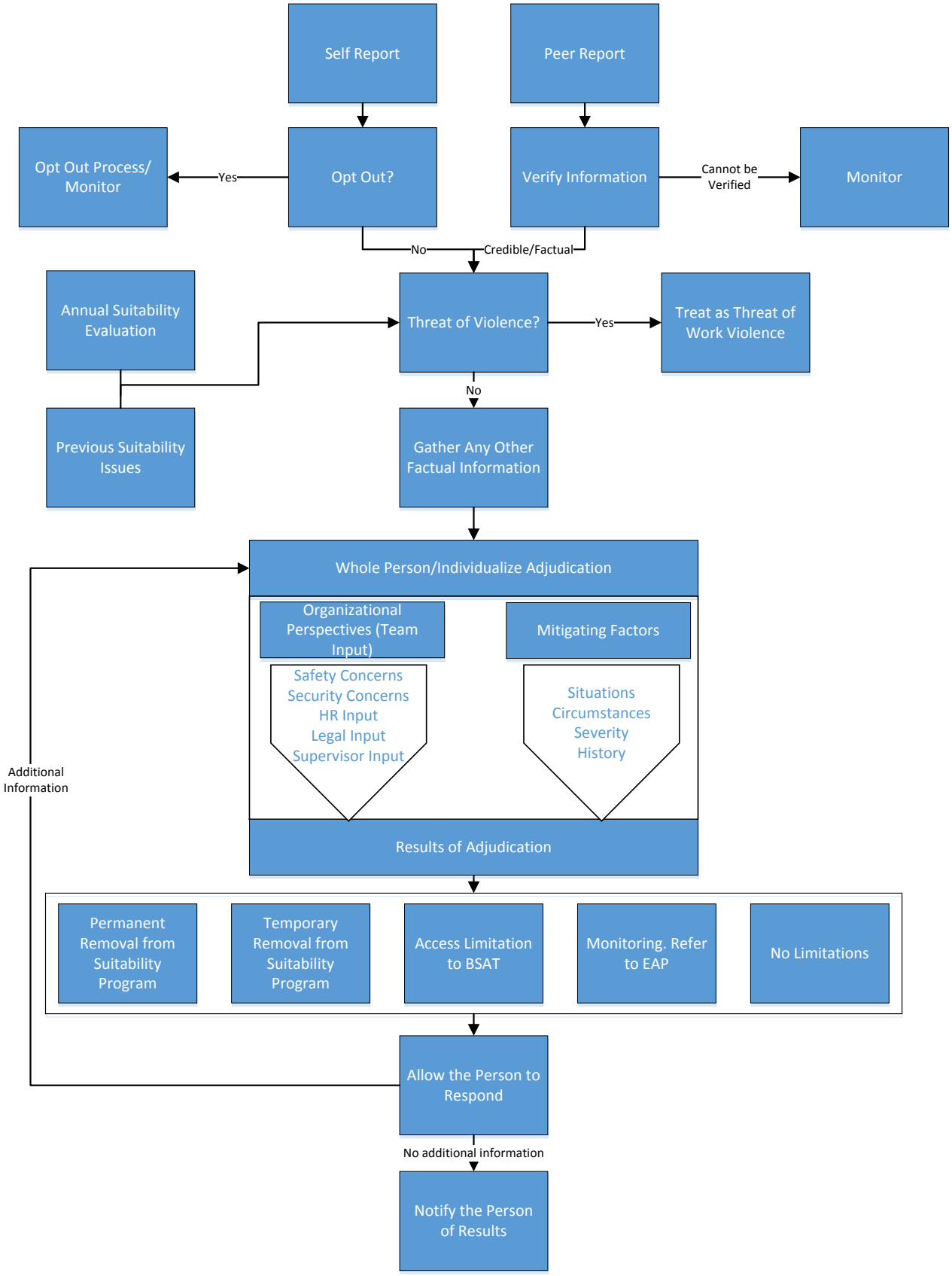
- No central repository exists for federal, state, and local (e.g., county, parish, municipal, etc.) criminal records.
- Not all states have automated systems for collecting data from reporting agencies and local jurisdictions. The content, accuracy, quality and timeliness of the data vary considerably among the states.
- 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.'
- Check the local records. Many jurisdictions have government owned and operated online access where the accuracy of the conviction record can be verified.
- 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.
- 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 Pre-Access Suitability Adjudication Flow Diagram



Appendix IV. Example Ongoing Suitability Assessment Process Flow