DoD Instruction 5210.88

Security Standards for Safeguarding Biological Select Agents and Toxins

Originating Component:	Office of the Under Secretary of Defense for Acquisition and Sustainment
Effective:	May 26, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 5210.88, "Security Standards for Safeguarding Biological Select Agents and Toxins (BSAT)," January 19, 2016, as amended
Approved by:	Ellen M. Lord, Under Secretary of Defense for Acquisition and Sustainment

Purpose: In accordance with the authority in DoD Directive (DoDD) 5134.01, the July 13, 2018 Deputy Secretary of Defense Memorandum, and DoDD 5101.20E, this issuance establishes policy, assigns responsibilities, and provides guidance for:

- The execution of the DoD BSAT biosafety and biosecurity programs.
- DoD BSAT security programs and personnel reliability program for Tier 1 BSAT, as defined by Part 73 of Title 42, Code of Federal Regulations (CFR); Part 331 of Title 7, CFR; and Part 121 of Title 9, CFR, collectively referred to in this issuance as the "select agent regulations" (SAR).
- Conformance to Executive Order 13546.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance:

a. Applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD that are registered with the Federal Select Agent Program (FSAP) (referred to collectively in this issuance as the "DoD Components").

(2) DoD entities located overseas that may possess or use Biological Select Agents and Toxins (BSAT) but are not subject to the select agent regulations (SAR) and Sections 201–231 of Public Law 107-188. These DoD entities will comply with the requirements of the SAR to the maximum extent possible. If implementation of specific provisions is not feasible, the entity will document alternative provisions based on host nation and sponsor requirements (whichever is most stringent) and site-specific risk assessments.

(3) Contracts that contain requirements for access to BSAT by contract personnel working in DoD Component entities.

b. Does not apply to:

(1) Infectious agents and toxins not included as BSAT in the SAR. The appropriate safeguards for non-BSAT agents and toxins are in DoD Manual (DoDM) 6055.18.

(2) Non-DoD entities that receive transfers of DoD BSAT. It is recommended that DoD contracts include clauses requiring the contract laboratory to provide FSAP inspection results and agreement to maintain compliance with all FSAP regulatory requirements.

1.2. POLICY.

a. DoD must comply with the provisions of the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction and Department of Defense Directive (DoDD) 2060.01.

b. DoD entities using, possessing, transferring, or receiving BSAT must register with the FSAP in accordance with the SAR.

c. DoD Components must mitigate, to an acceptable risk, threats to security of BSAT, including theft, loss, diversion, release, or unauthorized access, transfer, use, or production, in accordance with this issuance.

(1) Authorities and responsibilities of the DoD Component commanders and directors for security of DoD property are delineated in Paragraphs 3.2 and 3.4 above the signature of DoD Instruction (DoDI) 5200.08.

(2) Requirements in this issuance do not repeal the responsibility of commanders or directors to apply more stringent security standards during emergencies, increased threat level or high risk determinations, or as deemed necessary pursuant to Paragraph C1.2.4 of DoD 5200.08-R.

d. DoD Components must keep to the minimum:

(1) The movement of BSAT consistent with operational, research, training, teaching, safety, and security requirements.

(2) The number of people authorized access to BSAT consistent with operational, safety, and security requirements.

e. DoD Components must screen individuals with a need to access BSAT through the security risk assessment (SRA) process as described in the SAR. Individuals who need unescorted access to Tier 1 BSAT or whose duties afford unescorted access to registered spaces (e.g., storage and work areas, storage containers, and equipment) containing Tier 1 BSAT even if it is not accessible will be screened through both the SRA process and the biological personnel reliability program (BPRP) process.

f. DoD Components must report internal control material weaknesses in compliance with DoDI 5010.40.

g. DoD Components must implement international technology transfer and export control requirements for BSAT in accordance with DoDI 2040.02 and other applicable authorities, including: Section 2778 of Title 22, United States Code (also known as the "Arms Export Control Act (AECA)"); Chapter 58 in Parts 4801-4851 of Title 50, United States Code, also known as the "Export Control Reform Act"; Parts 120-130 of Title 22, CFR (also known as the "International Traffic in Arms Regulations (ITAR)"); and Parts 730-774 of Title 15, CFR (also known as the "Export Administration Regulations (EAR)").

h. Ricin and saxitoxin, regardless of the amount, are subject to accountability, use, and production restrictions in accordance with the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (the "Chemical Weapons Convention") as Schedule 1 chemicals, and the semi-annual reporting requirements in accordance with DoDI 5210.65. Chemical Weapons Convention production and acquisition requirements will be followed when ricin or saxitoxin are used for protective purposes. Entities possessing ricin and saxitoxin in quantities greater than BSAT threshold amounts must also comply with this issuance for all other purposes.

i. DoD Components will not impose more restrictive implementing requirements for security of BSAT than those in this issuance unless such implementing guidance is approved by the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (ASD(NCB)) or is implemented in accordance with Paragraph 1.2.c(2). In implementation of

this issuance, to provide clarity or operationalize guidance, DoD Components are authorized to prescribe procedures.

1.3. INFORMATION COLLECTIONS.

The annual BPRP report, referred to in Paragraphs 2.1.d., 2.4.g., and 7.2.a. has been assigned report control symbol DD-AT&L(A)2582 in accordance with the procedures in Volume 1 of DoDM 8910.01.

SECTION 2: RESPONSIBILITIES

2.1. ASD(NCB).

Under the authority, direction, and control of the Under Secretary of Defense for Acquisition and Sustainment, the ASD(NCB):

a. Establishes security standards for safeguarding DoD BSAT and BPRP standards for individuals with access to DoD Tier 1 BSAT.

b. Reviews all exceptions to this issuance for approval. Through the Assistant Secretary of Defense for Homeland Defense and Global Security (ASD(HD&GS)) acting as the DoD's liaison to the National Security Council (NSC) staff on matters regarding relevant National security policy, coordinates with the NSC staff, as appropriate, for issues that exceed the SAR. This authority will not be delegated.

c. Oversees the BSAT biosecurity program to confirm DoD Components maintain compliance with standards.

d. Establishes procedures for annual DoD Component reporting of statistical data concerning BPRP.

e. Establishes procedures for DoD Components to report BSAT security incidents and mishaps.

f. Provides relevant threat assessment updates to the DoD Components on receipt.

g. Develops and coordinates BSAT security classification guidance, as appropriate, and provides that guidance to the DoD Components to verify consistency in classification and dissemination of information.

2.2. ASD(HD&GS).

Under the authority, direction, and control of the Under Secretary of Defense for Policy, and consistent with DoDD 5111.13 and DoDD 2060.02, the ASD(HD&GS):

a. Acting as the DoD's liaison to the NSC staff on matters regarding relevant national security policy, coordinates with the NSC staff, as appropriate, for issues that exceed the SAR.

b. Coordinates on biosecurity policy and planning and represents the Under Secretary of Defense for Policy on interagency biosecurity committees and working groups.

c. Develops policy to support civil authorities for DoD preparedness, response, and consequence management involving DoD BSAT in accordance with the 2018 National Defense Strategy for Countering Weapons of Mass Destruction.

d. Receives and coordinates with the ASD(NCB) and the Assistant Secretary of Defense for Health Affairs on BSAT incidents that cause a public health emergency within DoD, or may cause a public health emergency of international concern (PHEIC).

2.3. DIRECTOR, DEFENSE INTELLIGENCE AGENCY.

Under the authority, direction, and control of the Under Secretary of Defense for Intelligence, in accordance with DoDD 5105.21, and in addition to the responsibilities in Paragraph 2.4., the Director, Defense Intelligence Agency, annually reviews and updates relevant threat capability assessments and provides them to the ASD(NCB).

2.4. DOD COMPONENT HEADS.

The DoD Component heads:

a. Assign responsibilities and provide commanders or directors guidance to comply with the requirements, measures, and standards in this issuance and the SAR.

b. Establish a process for approval of waivers to this issuance and keep the ASD(NCB) and the DoD Executive Agent for BSAT Biosafety and Biosecurity informed of waiver approvals.

c. Plan and program fiscal and personnel resources necessary to implement the policy and requirements in this issuance.

d. Notify the ASD(NCB), through the DoD Executive Agent for BSAT Biosafety and Biosecurity:

(1) Before registering any new DoD BSAT entity with the Centers for Disease Control and Prevention (CDC) or with the U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS).

(2) Following removal of such registration.

e. Require that BSAT entities are registered according to federal, territorial, State, and local regulations.

f. Require that each BSAT entity is supported by an appropriately appointed competent medical authority (CMA).

g. Submit annual statistical data concerning the BPRP to the ASD(NCB) in accordance with guidance from the ASD(NCB) and Paragraph 7.2.a.

h. Coordinate with the DoD Executive Agent for BSAT Biosafety and Biosecurity and approve, as part of pre-event planning, proposed public releases of information pertaining to BSAT.

i. Comply with the secure DoD BSAT database procedures established by the ASD(NCB) and the DoD Executive Agent for BSAT Biosafety and Biosecurity.

j. Endorse deviation requests forwarded through the DoD Executive Agent for BSAT Biosafety and Biosecurity to the ASD(NCB).

2.5. SECRETARY OF THE ARMY.

In addition to the responsibilities in Paragraph 2.4., the Secretary of the Army:

a. Serves as the DoD Executive Agent for the DoD BSAT Biosafety and Biosecurity Programs as designated by the Deputy Secretary of Defense. He or she is responsible for the technical review, inspection, and harmonization of biosafety and biosecurity protocols and procedures across DoD laboratories that handle BSAT, as well as the tasking authority of all DoD Components for this purpose.

b. Establishes and maintains a secure database of all DoD BSAT at DoD BSAT entities and a register of current and previous responsible officials (ROs) and alternate responsible officials (AROs).

c. Coordinates with the CDC and APHIS FSAP proponent offices and serves as the DoD point of contact with the CDC and APHIS regulatory oversight offices. In this capacity, the Secretary of the Army:

(1) Stays current on changes to the SAR, including the listing of agents or toxins designated as BSAT and Tier 1 BSAT and provides guidance to DoD Components accordingly.

(2) Coordinates with the CDC and APHIS on incidents covered by this issuance.

d. Coordinates with the Assistant Secretary of Defense for Health Affairs, the ASD(HD&GS), and the ASD(NCB) on an incident that causes a public health emergency within DoD, or causes, or could cause, a PHEIC, and before public affairs announcements are released.

e. Coordinates with the Director, Washington Headquarters Services (WHS), pursuant to DoDI 5230.29.

(1) Once the Director, WHS, has cleared information for public release, the Secretary of the Army coordinates:

(a) With the Assistant to the Secretary of Defense for Public Affairs before release, pursuant to DoDD 5122.05.

(b) Information related to public safety as part of pre-event planning. Information released during an incident will not be delayed and will be in accordance with local agreements.

(2) The Secretary of the Army notifies the Director, WHS, and the Assistant to the Secretary of Defense for Public Affairs immediately when such information is released.

f. Establishes an inspection process for BSAT entities that maximizes conducting inspections jointly with those scheduled and conducted by APHIS or the CDC. The DoD Joint inspection team, led by the Department of the Army Inspector General and composed of subject matter experts from the Army, Air Force, and Navy, is intended to harmonize inspections across the DoD.

g. Establishes documentation requirements that are not addressed in this issuance.

h. Requires that DoD BSAT entities establish plans, procedures, and processes to secure, safeguard, or destroy DoD BSAT in the event of emergency situations (e.g., natural disasters, fires, power outages, and general emergencies in DoD BSAT facilities).

SECTION 3: DEVIATION PROGRAM (WAIVERS AND EXCEPTIONS)

3.1. Deviations from the requirements of this issuance require an approved waiver or exception. Deviations include cases where the requirements of this issuance are not implemented, and cases that result in more restrictive countermeasures than addressed in this issuance.

a. The DoD Component head, or his or her designee, is the approval authority for waivers to this issuance. A waiver may be approved for temporary relief from a specific requirement prescribed in this issuance, pending actions to conform to the requirement. Such waivers will be approved for only as long as needed and will not exceed 1 year; an extension may be approved for no more than 1 additional year. While a waiver is in effect, compensatory security measures will be implemented as needed to mitigate any increase in risk or vulnerability to an acceptable level. The DoD Component will notify the DoD Executive Agent for BSAT Biosafety and Biosecurity and the ASD(NCB) of approved waivers.

b. The ASD(NCB) is the approval authority for all exceptions to this issuance. An exception may be approved for permanent relief from a specific requirement as prescribed in this issuance when there are unique circumstances applicable to the BSAT entity that make conforming to the requirement impractical or an inappropriate use of resources. Compensatory security measures will be implemented to mitigate any increase in risk or vulnerability to an acceptable level. The ASD(NCB) may be required to coordinate through the ASD(HD&GS) for National Security Council approval if these measures exceed SAR requirements.

3.2. Requests for waivers and exceptions from this issuance will be forwarded through the chain of command to reach the DoD Component within 30 days of initiation. Within 30 days of receipt, the DoD Component will review and respond to waiver requests or will forward exception requests through the DoD Executive Agent for BSAT Biosafety and Biosecurity to the ASD(NCB). The ASD(NCB) will review exception requests and respond within 30 days of receipt. Requests for deviations will include:

a. Any risks and vulnerabilities associated with granting the deviation, ensuring they are classified in accordance with current guidance.

b. Recommended compensatory security measures to mitigate any increased risk or vulnerability as a result of the deviation.

c. The projected duration of the deviation.

d. A complete and specific justification indicating why the deviation is required.

e. The projected costs associated with the recommended compensatory security measures.

f. A recommendation from the DoD Executive Agent for the DoD BSAT Biosafety and Biosecurity Programs for requests forwarded to the ASD(NCB).

3.3. Whenever deviation conditions or compensatory measures change, a request for an amendment to, or cancellation of, the waiver or exception will be sent to the office that granted approval of the original request.

3.4. Physical security surveys, reports, and inspections will include a review of approved deviations to verify that conditions described in the request remain accurate and that compensatory measures are implemented fully. The physical security survey or inspection report will include a comment regarding the actions taken as a result of that review.

SECTION 4: SECURITY REQUIREMENTS AND MEASURES

4.1. GENERAL.

This section details the security standards necessary to reduce the risk of compromising BSAT security and to safeguard BSAT from theft or unauthorized access.

a. Storage and work sites will be in BSAT registered spaces. BSAT will be secured, stored, and transported to meet the physical security requirements pursuant to DoDI 5200.08, DoDM 6055.18, Volume 6 of Defense Explosives Safety Regulation 6055.09, and the security standards in this issuance.

b. BSAT accidents or incidents will be reported in accordance with the SAR and as described in Section 7.

c. Security planning and execution will be in accordance with DoDI 5200.08 and based on the standards identified in this issuance and a site-specific risk assessment of the entity. An appropriate risk management process will be used, in accordance with Volume 2 of DoDI O-2000.16, to assess the threat and vulnerabilities and provide the RO and entity commander or director with courses of action to mitigate the vulnerabilities or accept the risk.

d. The commander or director of a DoD BSAT entity will conduct and document an initial site-specific risk assessment at each DoD BSAT entity, then review and update it annually or as a new vulnerability or threat becomes known. The risk assessment will consider the current threat assessment, physical surveys, and antiterrorism standards from Volume 2 of DoDI O-2000.16.

4.2. PHYSICAL SECURITY SYSTEMS.

a. The DoD BSAT entity commander or director will establish a reliable security system and process that provides the capability to detect, assess, deter, communicate, delay, and respond to unauthorized attempts to access BSAT.

b. Commanders or directors and ROs of BSAT entities will develop a physical security plan to mitigate vulnerabilities or accept a risk in accordance with the SAR, DoDI 5200.08, and DoD 5200.08-R.

(1) The physical security plan will be based on a systematic approach where threats are identified and defined, vulnerabilities are assessed, and a risk management process is applied. Acceptable risk will be determined using a risk-based process in coordination with the installation staff and approved by the entity's most senior commander or director.

(2) If the entity is a tenant on a military installation, the physical security plan for BSAT will be integrated into the host installation plan. The BSAT entity commander or director will identify any off-installation support requirements to the installation commander, who will

incorporate those requirements into any installation agreements coordinated with off-installation agencies.

(3) The organization responsible for executing armed responses at BSAT entities (when required by a site-specific risk assessment) will develop response plans in coordination with the supported entity to implement acceptable support levels in accordance with the SAR.

(4) The RO and entity commander or director will review the security plan annually and revise as necessary in accordance with the SAR. The plan will address or establish:

(a) The physical security plan that will address the controls used to secure the BSAT from misuse, theft, loss, and unauthorized access or removal from the BSAT registered space.

(b) Control of access for BSAT registered spaces.

(c) Procedures to appropriately secure information in accordance with Paragraph 4.8.

(d) Initial and annual personnel trainings regarding procedures for securing BSAT registered spaces, security and positive control of keys, changing access permissions or locks following staff changes, reporting and removing unauthorized individuals, access control and records requirements, inventory control, and other appropriate security measures. Additional trainings must also be provided whenever the entity significantly amends its security, incident response, or biosafety plans.

(e) Procedures, reporting requirements, and administrative actions for lost or compromised keys, keycards, passwords, combinations, and security incidents and violations that cause a public health emergency within DoD, incidents and violations that could cause, or do cause, a PHEIC, and those security incidents and violations that involve alteration of inventory records.

(f) Procedures to mitigate the presence of suspicious or unauthorized persons or activities that may potentially or actually attempt to misuse or remove BSAT.

(g) Procedures on how to identify and report suspicious packages before they are brought into or removed from a BSAT storage or work area.

(h) Procedures for management control of closed circuit television recording or surveillance, if used by an entity to address a risk or vulnerability.

(i) Contingency plans for unexpected shipments.

(5) Tier 1 BSAT entities will have the following enhancements to their security plan:

(a) Delineation of the roles and responsibilities for security management, including designation of a security officer to manage the entity's BSAT security program.

(b) Procedures for management of access controls (e.g., keys, keycards, common access card, access logs, biometrics, and other access control measures). This may be

accomplished by controlling or interacting directly with a service provider (e.g., a guard company).

(c) Designation of personnel to manage the entity's intrusion detection system (IDS), including personnel with the IDS alarm code and criteria for changing it.

(d) Procedures to test the IDS and manage its configuration.

(e) Procedures to respond to an access control failure, IDS failure, or nuisance alarm.

(f) Procedures to screen visitors in accordance with Section 6.

(g) Procedures to document security awareness training for all employees listed on the entity's approved registration. This will include annual insider threat awareness briefings on how to identify and report suspicious behaviors that occur inside the laboratory or storage area, pursuant to DoDD 5205.16.

(h) Requirements and procedures for all professionals involved in BSAT safety and security at an entity to share relevant information with the RO to coordinate their efforts pursuant to the SAR. The entity's RO, safety, and security professionals will meet on a regular or defined basis. This may be annually in conjunction with the physical security plan review, after a security incident, when there is a significant entity change that affects security, or in response to a threat.

4.3. SECURITY FORCES. a. In accordance with DoDI 5200.08 and DoDD 5210.56, installation commanders will issue the necessary regulations to protect and secure property and places within their command.

b. There will be a sufficient security force available at all times to respond rapidly to unauthorized access (attempted or actual) and prevent the unauthorized removal of BSAT or data.

c. The RO, entity commander or director, and the installation commander will determine the required response time for the security forces (from notification to arrival at the outermost security barrier) based on the site-specific risk assessment. For entities holding Tier 1 BSAT, this includes the time period that physical security measures delay potential unauthorized attempted access. If the response time exceeds 15 minutes, the security barriers must be sufficient to delay unauthorized access until the security force arrives.

d. Security force members will participate in appropriate, realistic, site defense force training exercises at a frequency determined by the DoD Component in accordance with the SAR. The training will be tailored to each BSAT entity based on the site-specific risk assessment conducted at the site.

4.4. SECURITY MEASURES.

a. Security Barriers.

BSAT entities must have security barriers that both deter intrusion and deny access to areas containing DoD BSAT by unapproved personnel. Barriers may consist of physical obstacles (e.g., perimeter fences, walls, locked doors, security windows), trained personnel (e.g., security guards, laboratory personnel, or escorts), or a combination of both to provide a continuous ring of security or layering that provides security in depth.

(1) BSAT entities that are not registered for Tier 1 BSAT require at least one security barrier.

(2) Entities registered for Tier 1 BSAT require three physical security barriers, counted from the Tier 1 BSAT outward. Pursuant to Part 73 of Title 42, CFR, if trained personnel are designated as one of the three barriers, they must be dedicated to that task. These physical barriers must be identified on the entity's registration and discussed in the physical security plan (sections 5A and 6A of APHIS/CDC Form 1, "Application for Registration for Possession, Use, and Transfer of Select Agents and Toxins," available from https://www.selectagents.gov).

b. Other Security Measures.

Perimeter security lighting, IDS, and cameras may be used to monitor access, but are not considered security barriers because they cannot prevent access by themselves.

(1) Perimeter Security Lighting.

BSAT entities will determine perimeter lighting needs based on site-specific risk assessments.

(2) IDS.

The IDS will be equipped with monitoring capability (e.g., tamper alarms or serialized seals) to detect and report attempted or unauthorized penetration to security monitoring or control systems, IDS equipment, junction boxes, or communication lines.

(a) For BSAT registered spaces, an entity may consider using IDS based on a site-specific risk assessment.

(b) All areas that reasonably afford access to a Tier 1 BSAT registered suite or room must be protected by an IDS unless the registered area is physically occupied. The IDS will be configured to detect and report unauthorized access (actual or attempted) and meet the physical security standards in DoDM 5200.01.

(3) Cameras.

Cameras can be used to monitor barriers or for other risk mitigation based on site-specific risk assessments.

4.5. ACCESS CONTROL.

a. Only individuals who successfully complete an SRA and obtain approval from the FSAP are authorized access to BSAT.

b. Personnel granted access to Tier 1 BSAT must be enrolled in the BPRP by the certifying official (CO), with final approval by the RO. Access to laboratory and storage facilities containing Tier 1 BSAT outside of normal business hours must be limited only to those specifically approved by the RO or designee.

c. Visitors requiring access to BSAT, Tier 1 BSAT, or BSAT registered spaces will follow the procedures in Section 6.

d. The access control system will include provisions for the safeguarding of animals and plants exposed to or infected with BSAT in accordance with the SAR.

e. Each individual authorized access to BSAT will have a unique means of accessing the agent pursuant to the SAR. The BSAT entity personnel will maintain a register (automated or manual) to record the entrance and exit of visitors to the BSAT registered space. The register will reflect the individual's name, entrance and exit time and date, and escort's name, if required.

f. The DoD BSAT entity personnel will modify the access control system when an individual's access authorization changes.

g. Smart card technology will be implemented in accordance with DoDI 8520.02.

h. All individuals approved for access to BSAT registered spaces and BSAT must wear visible identification (ID) badges in front, between the neck and waist that include, at least, a photograph, the wearer's name, and an expiration date. Visitors will be clearly identified as having escorted or unescorted access. Entity administrators are encouraged to use easily recognizable marks on the ID badges to indicate access to sensitive and secure areas. Visible ID badges are not required when working in appropriate protective clothing or in Biosafety Level-3 or -4 containment suites.

i. The DoD BSAT entity will implement a duress system to enable authorized personnel to covertly communicate an adverse situation.

j. An automated entry control system (AECS) may be used to control access instead of visual control if it meets the criteria stated in this issuance. The AECS will authenticate the individual's ID and verify the person's authority to enter the area through two separate methods that may include ID badges, cards, a personal ID number (PIN) entry device, or biometric device.

(1) An AECS ID badge or key card will use embedded sensors, integrated circuits, magnetic strips, or other means of encoding data that identifies the entity and the individual to whom the card is issued in accordance with DoDI 8520.02.

(2) Personal identity verification via biometrics devices may be used to validate the individual requesting access by one or more unique personal characteristics. Personal characteristics may include fingerprints, hand geometry, handwriting, retina scans, or voice recognition.

(3) The AECS will be configured to maintain system integrity and to preclude compromise of electronic access data. The AECS will operate on a closed computer network specifically designed and established for the AECS. Data input to the system will require the badge custodian to have log-in and password privileges.

(4) A PIN may be required if smart card technology is used. The PIN will be entered into the system separately by each individual using a keypad device and will consist of four or more digits, selected randomly, with no known or logical association with the individual. The PIN will be changed if it is believed to be compromised.

(5) The AECS will authenticate the individual's authorization to enter BSAT registered spaces with inputs from the ID badge or card, the personal identity verification device, or a keypad with an electronic database of individuals authorized to enter the area. A paper-entry access control roster will be maintained in the event of a system failure or as an alternative.

(6) Protection from tampering, destruction, or access control system failure will be established and maintained for all devices or equipment that constitutes the access control system. The protections can include welding door hinges and pins, eliminating exposed screw heads, ensuring that doors and walls delay access, or IDS to detect unauthorized entry. These emergency systems will allow time for response forces to arrive as discussed in Paragraph 4.4.b. Protection will address covert entry into BSAT registered spaces through electrical, communications, or heating, ventilation, and air conditioning distribution and maintenance areas.

(7) Security and communications devices located outside the entrance to a BSAT registered space will be in protected areas or have tamper resistant enclosures. They will be securely fastened to the wall or other permanent structure to prevent unauthorized access through breaching of attachment mechanisms (e.g., screws, pins, bolts). Control panels located within a BSAT registered space will require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism.

(8) Keypad devices will be designed and installed so that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers.

(9) Electric strikes used in access control systems will be heavy duty, industrial grade.

4.6. BSAT STORAGE.

a. When not in use, all BSAT will be stored in refrigerators, freezers, or other approved storage devices secured against unauthorized access (e.g., card access system and lock boxes) in secured BSAT registered spaces.

b. Procedures will be established for package and material controls, end-of-day security checks, after-duty access controls, and access records.

4.7. INVENTORY AND ACCOUNTABILITY.

a. The DoD BSAT database will be used to inventory and account for all BSAT at DoD BSAT entities registered with the FSAP. Each BSAT registered individual or entity must maintain a current and accurate inventory. The DoD Executive Agent for the DoD BSAT Biosafety and Biosecurity Programs is the authority for managing the format and content of the DoD BSAT database in accordance with DoDD 5101.20E.

(1) The inventory and accountability records will include specific details about the current inventory of BSAT pursuant to the SAR.

(2) Inventory audits will be conducted in accordance with guidance in the SAR.

b. BSAT disposal will be in accordance with guidance in the SAR, DoDM 6055.18, and all applicable federal, State, territorial, and local regulations.

4.8. INFORMATION AND CYBER SECURITY.

a. DoD information systems and DoD information in electronic format:

(1) Will be protected in accordance with DoDI 8500.01.

(2) Must comply with DoDI 8510.01.

b. Classified or controlled unclassified information (in electronic or hardcopy format) will be handled and protected in accordance with Volumes 3 and 4 of DoDM 5200.01. If the contract requires access to classified information, a DD Form 254, "DoD Contract Security Classification Specification," must be completed with the contract and include applicable classification guidance in accordance with DoDM 5220.22, Volume 2.

c. The SAR requires safeguarding BSAT security information. The minimum requirements are:

(1) Inventory access logs.

(2) Passwords.

(3) Entry access logbooks.

(4) Rosters of individuals approved for access to BSAT.

(5) Access control systems.

(6) Security system infrastructure (e.g., floor plans, on-site guard, closed-circuit television, and IDS).

(7) Security plans.

(8) Incident response plans.

d. Public release of information will be in accordance with DoDI 5230.09 and DoDI 5230.29.

e. The DoD BSAT database administrators at all levels will have an approved SRA or a SECRET clearance. Each entity's RO or ARO controls access to detailed quantitative entity records. Unless specifically authorized by an entity RO or ARO, the Military Department or Service representatives are authorized access to their Military Department or Service-specific entity qualitative records, and OSD representatives are authorized access to all DoD entity qualitative records. Requests for Military Department or Service or OSD access will be sent to the DoD Executive Agent for the DoD BSAT Biosafety and Biosecurity Programs.

4.9. TRANSPORTATION.

The transportation of BSAT will be in accordance with the SAR, Defense Transportation Regulation 4500.9-R, 50 USC 1512a, 50 USC 1512, and any applicable federal, State, territorial, and local regulations.

4.10. TRANSFER OF DOD BSAT.

a. The DoD Components may transfer DoD BSAT to other FSAP BSAT entities that are registered for that specific BSAT. The receiving entity will assume responsibility for the BSAT in accordance with the SAR.

b. DoD Components will not provide BSAT to non-U.S. Government overseas facilities or to foreign entities unless the transfer is consistent with U.S. export control laws and regulations and DoDI 2040.02.

c. The DoD Components will not provide DoD BSAT to non-U.S. governmental overseas facilities unless approved by the DoD Executive Agent for the DoD BSAT Biosafety and Biosecurity Programs with subsequent notification to the ASD(NCB).

(1) Requests will identify:

(a) Recipient information.

(b) Name and quantity of the requested BSAT.

(c) Purpose for which the BSAT will be used.

(d) Rationale for providing BSAT.

(e) Authority under which the transfer (export) will take place, for example, an international cooperative agreement, or an export license, DoD exemption, DoD or U.S. Government exemption, DoD or U.S. Government exception, or other authorization.

(2) Approval will identify security measures and requirements for the recipients and comply with applicable U.S. and international laws and regulations, as appropriate.

d. If the transfer of BSAT to a non-U.S. Government overseas facility or a foreign entity takes place outside the auspices of an international agreement, the DoD Executive Agent for the DoD BSAT Biosafety and Biosecurity Programs must ensure that the DoD Component has identified plans to comply with applicable DoD trade security controls in DoDI 2030.08, notably the requirement to assess the BSAT recipient.

SECTION 5: BPRP

5.1. GENERAL.

a. The purpose of the BPRP is to certify that each individual who is authorized access to Tier 1 BSAT meets high standards of integrity, trust, and personal reliability.

b. In most cases, the government reviewing official (REV) is the commander or director. However, the commander or director may designate an REV, as appropriate.

(1) The REV designates the CO, monitors the BPRP administered by the CO, and reviews and approves suitability actions in accordance with the guidance implemented by the DoD Component. The intent is for the REV to monitor certification decisions of the CO; oversee the status and quality of the program; and overturn CO decisions if procedures are unfairly, inconsistently, or incorrectly applied.

(2) The commander or director also designates the RO, who will report directly to the FSAP in coordination with the entity commander or director. The RO is responsible for determining an individual's eligibility for access to BSAT.

c. The BPRP requirements for Tier 1 BSAT are in addition to the SAR requirements for all BSAT, which includes an SRA and RO approval of an individual's access to BSAT. The CO is responsible for determining an individual's BPRP access eligibility to Tier 1 BSAT; however, both the CO and RO must concur for an individual to have access to Tier 1 BSAT.

d. Other personnel may be designated at DoD facilities to assist in program management based on DoD Component implementing guidance.

e. Foreign nationals who receive escorted access to Tier 1 BSAT during training, visits, assignments, or exchanges, as specifically authorized by the RO and the entity commander or director and REV (if designated), will be processed in accordance with the SAR, DoDI 2040.02, DoDD 5230.20, DoDM 5200.02, and DoDI 5200.02.

f. In DoD overseas facilities for both BSAT and Tier 1 BSAT, positions that are usually filled by DoD civilians or military personnel may be filled by local nationals as vetted by the local embassy and supported by a site-specific risk assessment. Employment of the individual in these positions requires the facility commander or director approval, and must be conducted with authorization, or license, license exception, or exemption in accordance with U.S. export control laws and regulations pursuant to the Arms Export Control Act, the Export Control Reform Act, the International Traffic in Arms Regulations, and the Export Administration Regulations.

5.2. INITIAL CERTIFICATION.

a. The CO will require that initial screening for BPRP certification includes:

(1) Initial Interview.

The CO or other designated individual will conduct a personal interview with each BPRP candidate for individuals to acknowledge their understanding of Section 552(a) of Title 5, U.S.C. (also known as the "Privacy Act of 1974," as amended), DoD Instruction 5400.11, the Health Insurance Portability and Accountability Act, and component privacy program specifics. The interviewer will discuss the screening process with the individual, as well as any relevant information as described in Paragraph 5.4. Individuals will be advised that they must report any factors that could adversely impact their ability to perform BPRP duties, and that failure to report this information may result in denial of BPRP certification.

(2) Personnel Security Investigation (PSI).

(a) Clearance Eligibility.

For those requiring access to Tier 1 BSAT, individuals must have a valid eligibility to access information classified at SECRET or higher.

(b) Dossier Review.

Although not a requirement of the program, sites may opt to review the most recent PSI of any individual in, or being considered for, the program.

(c) Foreign Nationals.

Process foreign nationals with requirements for access to Tier 1 BSAT in accordance with DoDD 5230.20 and DoDM 5200.02.

(d) Escorted Access.

COs, with RO concurrence, may approve escorted access to Tier 1 BSAT pending completion of the PSI. The investigation must have been opened and all other BPRP requirements have been completed and reviewed favorably.

(3) Medical Evaluation.

(a) The CO must be confident that the individual is medically, physically, and mentally competent, alert, and dependable, and is not a threat for inadvertent or purposeful compromise of the Tier 1 BSAT program or mission. To that end, a CMA must provide the CO an evaluation of the individual's medical and physical competence and mental stability to perform duties requiring BPRP certification.

(b) When a sexual assault victim elects restricted reporting in accordance with DoDI 6495.02, or the sexual assault victim is not eligible for restricted reporting and intends that the sexual assault remain confidential, the victim is required to advise the CMA of any factors that could have an adverse impact on performance, reliability, or safety while performing BPRP duties. The CMA will inform the CO if there are factors adversely impacting the individual's BPRP eligibility without revealing that the person is a victim of sexual assault.

(4) Drug and Substance Abuse Testing.

All candidates for BPRP positions will be tested for drug and substance abuse and results reported to the CO before being certified into the BPRP pursuant to DoDI 1010.09 and DoDI 1010.01.

(5) Personnel Record Review.

The CO will review the individual's available personnel records. If records are not accessible, the CO will coordinate with the appropriate supervisor, personnel manager, or other designated assistant or specialist to review the record and report any positive or negative factors that reflect on the individual's ability to perform BPRP duties.

(6) Position Qualification.

The CO will consult with the supervisor or hiring manager to verify that the individual has the appropriate professional or technical proficiency, skills, and abilities to qualify for the position.

(7) Final Review.

The CO will:

(a) Conduct a personal interview with each BPRP candidate just prior to final certification determination.

(b) Discuss any relevant information identified during the screening with the individual.

(c) Discuss the individual's responsibilities under continuing evaluation.

b. If the CO determines the individual is eligible for certification into the BPRP, the CO will notify the RO. The eligible individual will sign an agreement affirming his or her responsibility to abide by the requirements for maintaining BPRP certification.

c. If the CO determines that the individual does not meet the requirements for the BPRP, the CO will stop the screening process and deny BPRP certification. DoD Component guidance will establish documentation requirements.

5.3. CONTINUING EVALUATION.

Individuals certified under the BPRP are observed on a regular basis by peers, supervisors, and BPRP officials to determine if their behavior and performance meet all of the requirements of the program.

a. CO Observation.

COs will:

(a) Observe the behavior and performance of individuals certified under the BPRP on a regular basis.

(b) Consult with other BPRP officials and supervisors, as appropriate.

b. Individual and Peer Reporting.

Individuals certified in the BPRP are responsible for monitoring themselves and their BPRP-certified peers. Individuals and peers must report factors to the supervisor, CO, or CMA that could adversely impact the individual's ability to perform BPRP duties. Failure to discharge these responsibilities may cast doubt on an individual's reliability.

c. Supervisor and Security Manager Reporting.

Supervisors and security managers must notify the CO of factors that could adversely impact the individual's ability to perform BPRP duties.

d. Drug Testing.

Positions requiring BPRP certification will be designated for random testing. Verified positive test results will be reported to the CO and result in termination (for cause).

e. PSL.

Individuals will complete periodic reinvestigations in accordance with DoDM 5200.02. An unfavorably-adjudicated reinvestigation that renders an individual ineligible for a security clearance will result in termination (for cause).

f. Medical.

(1) Health records will include an individual's assignment to a position requiring BPRP certification to determine the proper treatment, review, and reporting of relevant medical limitation and duration recommendations to the CO. Medical records will document relevant medical information that raises concerns about the individual's medical and physical competence and mental stability to perform duties requiring BPRP certification, the CMA's recommendations on that information, and the evidence of transmission to the CO.

(2) The individual will report any medical evaluation, treatment, or medication to the CMA in accordance with DoD Component guidance to determine if there is any effect on the individual's ability to perform BPRP duties.

(3) When a sexual assault victim elects restricted reporting pursuant to DoDI 6495.02 or is not eligible for restricted reporting and intends that the sexual assault remain confidential, the victim is required to advise the CMA of any factors that could have an adverse impact on performance, reliability, or safety while performing BPRP duties. The CMA will inform the CO if there are factors adversely impacting the individual's BPRP status and if the person in question should be temporarily suspended without revealing that the person is a victim of sexual assault.

(4) When a sexual assault victim does not elect restricted reporting, the individual will report any factors that could adversely impact his or her ability to perform BPRP duties to the appropriate authority and then to the CO. The victim is required to advise the CMA of any factors that could have an adverse impact on performance, reliability, or safety while performing BPRP duties. The CMA will inform the CO if there are factors adversely impacting the individual's BPRP status and that the person in question should be temporarily suspended.

5.4. BPRP DENIAL OR TERMINATION CRITERIA.

Individuals will be denied BPRP certification, or terminated from the BPRP, if they:

a. Do not meet the criteria established in the Security Executive Agent Directive 4.

b. Have medical, physical, or mental conditions that will have negative effects on BPRP duty performance.

c. Have a positive drug test result.

d. Fail to report any factors that could adversely affect their ability to perform BPRP duties.

e. Fail to obtain or retain a favorably-adjudicated PSI.

f. Are determined to be unsuitable or unreliable by the CO.

5.5. REMOVAL FROM BPRP DUTIES.

a. A CO may impose an administrative restriction or medical restriction on an individual when the individual is affected by short-term conditions that may have a temporary effect on BPRP duty performance but do not raise concerns about the individual's suitability or reliability. Restriction will not be used for conditions that warrant BPRP denial or termination. When an individual is no longer required to perform BPRP duties, the CO will administratively terminate the individual from the BPRP. DoD Components may establish guidelines for duration limitations on restriction and suspension actions, and requirements for review and update of those actions.

b. When the CO receives information relative to the termination criteria in Paragraph 5.4., he or she will immediately suspend the individual while determining whether the facts warrant termination (for cause) and consulting with the RO. When suspended, the individual may not perform duties requiring BPRP certification. In addition, the individual will not have access to non-Tier 1 BSAT unless the RO has reviewed the circumstances of the suspension and documented the decision that access to non-Tier 1 BSAT is warranted. Information relevant to the individual's security clearance eligibility will be forwarded through the security manager to the DoD Consolidated Adjudications Facility.

(1) Within 15 workdays of the suspension, the CO will provide the individual, in writing, the reason or reasons for suspension. Individuals suspended will remain under continuous evaluation for BPRP purposes until terminated or reinstated into the BPRP.

(2) The individual will have 10 work days from the date of receipt of the written notification to provide a response to the CO, if desired.

(3) Prior to terminating the individual from the BPRP for cause, the CO will consult with the RO and the REV to confirm that the procedures have been fairly, consistently, and correctly applied. This consultation will include review of the individual's response to the CO, if provided.

c. COs will verify that termination actions are recorded in the affected individual's personnel record accurately. The RO must notify CDC or APHIS immediately when an individual's access to the select agents or toxins is terminated by the entity and the reasons.

5.6. RECERTIFICATION INTO THE BPRP.

a. An individual denied certification or terminated for cause from BPRP may submit a request for recertification to the CO. The request will explain the causes that led to the previous denial or termination and provide substantive evidence that those causes no longer exist.

b. The CO and the REV must approve a recertification request before the individual is processed for a new initial screening. An individual may be approved for recertification by the REV but may still be denied BPRP certification based on the new initial screening.

SECTION 6: VISITORS

6.1. NO ACCESS TO BSAT.

All DoD entities required to register pursuant to the SAR must develop procedures, based on their site-specific risk assessment, for escorting individuals who do not have approval from CDC or APHIS to access BSAT but require entry into BSAT registered spaces. Escort procedures will be developed as part of each entity's physical security plan and will include:

a. Citations of appropriate sections of the SAR and associated guidance documents that allow individuals not approved for access to conduct routine cleaning, maintenance, repairs, or other activities not related to BSAT only when continuously escorted by an individual if the potential for access to select agents or toxins exists.

b. Visitor entry procedures as prescribed in the SAR and associated guidance documents for entities possessing Tier 1 BSAT.

c. Citations of appropriate sections of the SAR for providing visitors with information and training on biocontainment, biosafety, security (including security awareness), and incident response.

d. Citations of appropriate sections of the SAR for RO requirement to maintain a record of the training provided to each escorted individual.

e. The entity commander or director, in consultation with the RO, permitting unescorted entry to a BSAT registered space if BSAT are secured in accordance with Section 4 to prohibit access to BSAT by this individual.

6.2. ACCESS TO BSAT.

The visitor must be listed on the host entity's registration, have an approved SRA, and have received appropriate training on biocontainment, biosafety, security (including security awareness), and incident response. Visitors requiring access to Tier 1 BSAT must either be enrolled in the host entity's BPRP or have a BPRP suitability memorandum from the home entity outlining pre-access suitability assessment and ongoing suitability monitoring requirements and verifying all pre-access checks have been accomplished. They must also be enrolled in an occupational health program. The entity commander or director, in consultation with the RO, may permit unescorted visitor access to BSAT.

6.3. FOREIGN VISITORS.

Additional foreign visitor requirements are located in Paragraph 5.1.e.

SECTION 7: REPORTS

7.1. GENERAL.

a. An individual or entity must immediately notify the appropriate lead regulatory agency, the CDC or the APHIS, by telephone, fax, or e-mail, if the RO has a reasonable suspicion that a theft, loss, release, or occupational exposure has occurred. Thefts or losses must be reported even if BSAT is subsequently recovered or the responsible parties are identified. This call can also serve as an opportunity to receive guidance from regulatory authorities if there is doubt that a report is required. Additional information will be submitted as it becomes known, but no later than 24 hours after the incident.

b. Within 7 days, the entity must submit a complete APHIS/CDC Form 3, "Report of Theft, Loss or Release of Select Agents or Toxins," available at https://www.selectagents.gov, to the agency with which it is registered, the CDC, or the APHIS.

c. The individual or entity will notify the appropriate federal, State, or local agencies of the theft, loss, or release of BSAT. Entities with Tier 1 BSAT must comply with the Federal Bureau of Investigation notification process for reporting thefts or suspicious activities that may be criminal in nature.

d. The individual or entity must notify the DoD chain of command immediately in accordance with DoDI 6200.03 when a BSAT incident occurs that causes a public health emergency in DoD or could cause or a PHEIC.

e. DoD Entities will report BSAT mishaps and incidents through command channels in accordance with DoD Component procedures through the BSAT Biorisk Program Office to the ASD(NCB) or designee. The following will be reported:

(1) The theft, loss, recovery, suspected theft, wrongful disposition, and unauthorized use or destruction of DoD BSAT.

(2) Attempts to steal or divert DoD BSAT outside of physical security controls.

(3) Actual or attempted unauthorized access at a DoD BSAT entity.

(4) Significant or disabling damage to, explosion, or force majeure at a DoD BSAT entity.

(5) Release of a DoD BSAT external to the containment laboratory and into the ambient air or environment.

(6) Mishaps in which there was direct evidence of an occupational exposure to DoD BSAT.

(7) Mishaps where there is exposure, injury, or death.

(8) Other DoD BSAT incidents not identified in Paragraphs 7.1.d.(1) through 7.1.d.(7) that the entity commander or director determines to be of immediate concern to DoD based upon the nature, gravity, and potential for adverse publicity or potential consequences of the incident.

7.2. DOD COMPONENT REPORTS TO THE ASD(NCB).

The DoD Components will:

a. Provide a BPRP status report by February 15 each year. The report will:

(1) State the DoD BSAT entity submitting the report.

(2) Indicate the year for which the information is being reported.

(3) List the total number of personnel (separated into military, DoD civilian, and contractor employees) at each DoD BSAT entity actually certified into the BPRP as of December 31.

(4) List the total number of personnel (separated into military, DoD civilian, and contractor employees) at each DoD BSAT entity denied certification, terminated administratively, and terminated for cause during the calendar year.

(5) List the number of terminations categorized by primary reason for termination meeting the BPRP denial or termination criteria or administrative termination per Paragraphs 5.4. and 5.5.

(6) Include any comments noting trends or other relevant factors to assist future historical analysis.

b. Provide an executive summary of significant findings associated with the Department-level inspections at BSAT facilities.

c. Provide an annual assessment of the health of the program.

7.3. RECORDS RETENTION.

a. In accordance with DoD Component guidance, DoD BSAT facilities will maintain:

(1) Security incident reports, site-specific risk assessments, and record of site-specific risk assessment annual reviews.

(2) Inspection and exercise records and reports.

(3) Corrective action reports from external inspections.

(4) Training records for each individual with access to BSAT and each escorted individual that includes name of individual, date of training, description of training provided, and the means used to verify the individual understood the training.

b. All records and reports associated with this issuance will be maintained for at least 3 years and then handled according to appropriate DoD Component instructions.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AECS	automated entry control system
APHIS	Animal Plant and Health Inspection Service
ARO	alternate responsible official
ASD(HD&GS)	Assistant Secretary of Defense for Homeland Defense and Global Security
ASD(NCB)	Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs
BPRP	biological personnel reliability program
BSAT	biological select agents and toxins
CDC	Centers for Disease Control and Prevention
CFR	Code of Federal Regulations
CMA	competent medical authority
CO	certifying official
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
FSAP	Federal Select Agent Program
ID	identification
IDS	intrusion detection system
NSC	National Security Council
PHEIC	public health emergency of international concern
PIN	personal identification number
PSI	personnel security investigation
REV	reviewing official
RO	responsible official
SAR	select agent regulations
SRA	security risk assessment
WHS	Washington Headquarters Services

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
administrative restriction	When the ability to maintain continuing evaluation is questionable, the CO may administratively restrict such individuals from BPRP duties for the duration of an extended absence. Administrative restriction is not an assessment of unreliability.
administrative termination	Removal of reliable individuals from the program when they are leaving the position or no longer require access to BSAT or perform BPRP duties.
access	An individual will be deemed to have access to a DoD BSAT at any point in time if the individual has possession of a DoD BSAT (e.g., ability to carry, use, or manipulate) or the ability to gain possession of ~~a~~ DoD BSAT.
ARO	An individual designated by the entity commander or director, approved by the CDC or APHIS for access to BSAT, and with the authority and responsibility to act on behalf of the entity and ensure compliance with the SAR in the absence of the RO. Enrollment in the BPRP is not required unless the ARO will have access to Tier 1 BSAT.
badge custodian	Individual responsible for controlling and issuing AECS ID badges or key cards.
biological agents and toxins	Defined in Section 178 of Title 18, United States Code.
BSAT	All of the biological agents or toxins listed in the SAR. They have the potential to pose a severe threat to public health and safety, animal and plant health, or animal and plant products and whose possession, use, and transfer are regulated by the Department of Health and Human Services and the Department of Agriculture under the SAR.
BSAT registered space	Space registered with the FSAP for BSAT.
CMA	A healthcare provider who is trained and appointed in accordance with procedures established by the DoD Component to review medical conditions and treatment to provide recommendations to the CO on an individual's suitability and reliability for personnel

TERM	DEFINITION
	reliability program duties. The CMA is a physician, nurse practitioner (who is either licensed for independent practice or supervised by a physician licensed for independent practice), or physician assistant (if supervised by a physician licensed for independent practice).
CO	The person responsible for determining an individual's ability to be BPRP-certified and ensuring the BPRP member is continuously monitored. Responsibilities also include implementing, administering, and managing the BPRP, and supporting the entity commander or director, REV, RO, and ARO. Unless the CO requires access to BSAT, the CO is not required to have an SRA or be enrolled in the BPRP.
continuing evaluation	The process by which BPRP-certified individuals are observed for compliance with reliability standards. This is an ongoing process and management function that considers duty performance, physical and psychological fitness, on- and off-duty behavior, and reliability on a continuing basis.
denial	An action taken based on the receipt of disqualifying information to stop the BPRP screening process for an individual being considered for duties involving access to Tier 1 BSAT.
drug and substance abuse	The wrongful use, possession, or distribution of a controlled substance, prescription medication, over-the-counter medication, or intoxicating substance (other than alcohol). "Wrongful" means without legal justification or excuse, and includes use contrary to the directions of the manufacturer or prescribing healthcare provider, and use of any intoxicating substance not intended for human intake.
entity	Any government agency (federal, State, or local), academic institution, corporation, company, partnership, society, association, firm, sole proprietorship, or other legal entity registered with the FSAP.
IDS	A system of sensor devices that trigger an alarm when a security breach occurs, notifying the appropriate response force who have the capability to respond to the alarm and assess or confront a threat.
medical restriction	When performance of BPRP duties may be impaired by a temporary medical condition (including medication for the condition) or psychological condition (such as short-term stress), the CO may determine the individual should be restricted from performing those

TERM	DEFINITION
	BPRP duties. Medical restriction is a precaution based on the possibility of duty impairment and not an assessment of unreliability.
REV	An entity official whose duties include monitoring the suitability assessment program and reviewing warranted suitability actions.
risk assessment	The process of systematically identifying, assessing, and managing risks arising from operational factors and making decisions that balance risk cost with mission benefits as described in DoDI O-2000.16. The end product of risk assessment is the identification and assessment of areas and assets that are vulnerable to the identified threat attack means or to the identified hazard. From the assessment of risk based upon the three critical components of risk management (threat assessment, criticality assessment, and vulnerability assessment), the commander must determine which assets require the most protection and where future expenditures are required to minimize risk of attack or exposure to a hazard or lessen the severity of the outcome of an attack or of a hazard.
RO	An individual designated by the entity commander or director and approved by the CDC or APHIS for access to BSAT. The RO has the authority and responsibility to act on behalf of the entity and ensure compliance with the SAR. Enrollment in the BPRP is not required unless the RO will have access to Tier 1 BSAT.
SRA	Electronic records check performed by the Criminal Justice Information Service to determine if an individual who has been identified by a BSAT entity as having a legitimate need to access BSAT exhibits one of the statutory restrictors which would either prohibit or restrict access.
suspension	An action taken to temporarily remove an individual from the BPRP when the CO has information that could be expected to affect an individual's job performance or reliability.
termination (for cause)	An action, based on the receipt of disqualifying information, to remove an individual from the BPRP who was previously screened, determined reliable, and certified capable of performing duties involving access to Tier 1 BSAT.
Tier 1 BSAT	A subset of the BSAT listed in the SAR, they present the greatest risk of deliberate misuse with the most significant potential for mass casualties or devastating effects to the economy, critical infrastructure, or public confidence.

TERM	DEFINITION
visitor	A person (e.g., regular, recurrent, maintenance and other non-scientific support, or first responder/emergency personnel) who is not authorized unescorted access to BSAT.
vulnerability	A situation or circumstance that, if left unchanged, may result in the loss of or damage to the BSAT or the BSAT facility.

REFERENCES

Code of Federal Regulations, Title 7, Part 331

Code of Federal Regulations, Title 9, Part 121

Code of Federal Regulations, Title 15, Parts 730-774 (also known as the "Export Administration Regulations (EAR)," as amended)

Code of Federal Regulations, Title 22, Parts 120-130 (also known as the "International Traffic in Arms Regulations (ITAR)," as amended)

Code of Federal Regulations, Title 42, Part 73

"Convention on the Prohibition on the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and On Their Destruction (BWC)," March 26, 1975[1]

"Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction." April 29, 1997[2]

Defense Explosives Safety Regulation 6055.09, Volume 6, "DoD Ammunition and Explosives Safety Standards: Contingency Operations, Toxic Chemical Munitions and Agents, and Risk-Based Siting," February 29, 2008, as amended

Defense Transportation Regulation (DTR) 4500.9-R, "Defense Transportation Regulation, Part II, Cargo Movement, Chapter 204, Hazardous Material," May 2014, as amended

Department of Health and Human Services, Office of the Assistant Secretary for Preparedness & Response, "(U/FOUO) Operational Framework to Promote Rapid Access to Biological Material Related to non-Influenza Pathogens with the Potential to Cause a Public Health Emergency of International Concern and Facilitate its Sharing Among U.S. Federal Departments and Agencies," July 3, 2019[3]

Deputy Secretary of Defense Memorandum, "Establishment of the Office of the Under Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment," July 13, 2018

DoD 5200.08-R, "Physical Security Program," April 9, 2007, as amended

DoD Directive 2060.01, "Implementation of, and Compliance with, Arms Control Agreements," January 9, 2001, as amended

DoD Directive 2060.02, "DoD Countering Weapons of Mass Destruction (WMD) Policy," January 27, 2017

DoD Directive 5101.20E, "DoD Biological Select Agents and Toxins (BSAT) Biosafety and Biosecurity Program," January 25, 2019

DoD Directive 5105.21, "Defense Intelligence Agency (DIA)," March 18, 2008

[1] Available at http://disarmament.un.org/treaties/t/bwc/text
[2] Available at https://www.opcw.ord/chemical-weapons-convention
[3] Available upon request from the Department of Health and Human Services, Office of the Assistant Secretary for Preparedness & Response, hhs.soc@hhs.gov, (202) 619-7800.

DoD Directive 5111.13, "Assistant Secretary of Defense for Homeland Defense and Global security (ASD(HD&GS))," March 23, 2018

DoD Directive 5122.05, "Assistant to the Secretary of Defense for Public Affairs (ATSD(PA))," August 7, 2017

DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005, as amended

DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, as amended

DoD Directive 5210.56, "Arming and the Use of Force," November 18, 2016

DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005

DoD Instruction 1010.01, "Military Personnel Drug Abuse Testing Program (MPDATP)," September 13, 2012, as amended

DoD Instruction 1010.09, "DoD Civilian Employee Drug-Free Workplace Program," June 22, 2012, as amended

DoD Instruction O-2000.16, Volume 2, "DoD Antiterrorism (AT) Program Implementation: DoD Force Protection Condition (FPCON) System," November 17, 2016, as amended

DoD Instruction 2030.08, "Implementation of Trade Security Controls (TSCs) for Transfers of DoD Personal Property to Parties Outside DoD Control," February 19, 2015, as amended

DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014, as amended

DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013

DoD Instruction 5200.02, "DoD Personnel Security Program (PSP)," March 21, 2014, as amended

DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005, as amended

DoD Instruction 5210.65, "Security Standards for Safeguarding Chemical Agents," January 19, 2016, as amended

DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019

DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019

DoD Instruction 6200.03, "Public Health Emergency Management Within the Department of Defense," March 28, 2019

DoD Instruction 6495.02, "Sexual Assault Prevention and Response (SAPR) Program Procedures," March 28, 2013, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011

DoD Manual 5200.01, Volumes 1 – 4, "DoD Information Security Program," February 24, 2012, as amended

DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017

DoD Manual 5220.22, Volume 2, "National Industrial Security Program: Industrial Security Procedures for Government Activities," August 1, 2018

DoD Manual 6055.18, "Safety Standards for Microbiological and Biomedical Laboratories," May 11, 2010, as amended

DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014, as amended

Executive Order 13546, "Optimizing the Security of Biological Select Agents and Toxins in the United States," July 2, 2010

National Defense Strategy for Countering Weapons of Mass Destruction, December 1, 2018

Public Law 107-188, Sections 201–231, "Public Health Security and Bioterrorism Response and Preparedness Act of 2002," June 12, 2002

Security Executive Agent Directive 4, "National Security Adjudicative Guidelines," June 8, 2017

United States Code, Title 5, Section 552(a) (also known as the "Privacy Act of 1974," as amended)

United States Code, Title 18

United States Code, Title 22, Section 2778 (also known as the "Arms Export Control Act (AECA)")

United States Code, Title 50, Chapter 58, 4801-4851 (also known as the "Export Control Reform Act")

United States Government Framework for the Rapid Sharing of Biological Material Related to non-Influenza Pathogens with the Potential to Cause a Public Health Emergency of International Concern, July 3, 2019