



Department of Defense INSTRUCTION

NUMBER 5210.88

January 19, 2016

USD(AT&L)

SUBJECT: Security Standards for Safeguarding Biological Select Agents and Toxins (BSAT)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues DoD Directive (DoDD) 5210.88 (Reference (a)) as an instruction in accordance with the authority in DoDD 5134.01 (Reference (b)), Deputy Secretary of Defense Memorandum (Reference (c)), Deputy Secretary of Defense Memorandum (Reference (d)), and paragraph E1.3 of DoD Instruction (DoDI) 5200.08 (Reference (e)) to establish policy, assign responsibilities, and provide procedures for:

(1) The execution of the DoD BSAT Security Program.

(2) Physical security and information security for BSAT in the possession of the DoD, and personnel reliability for Tier 1 BSAT as defined by part 73 of Title 42, Code of Federal Regulations (CFR) (Reference (f)), part 331 of Title 7, CFR (Reference (g)), and part 121 of Title 9, CFR (Reference (h)), collectively referred to in this instruction as the Select Agent Regulations (SAR).

b. Revises DoD BSAT security policy to:

(1) Conform with Executive Order 13546 (Reference (i)).

(2) Implement the SAR.

(3) Implement sections 201-231 of Public Law 107-188 (Reference (j)).

c. Incorporates and cancels DoDI 5210.89 (Reference (k)).

2. APPLICABILITY. This instruction:

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 (referred to collectively in this instruction as the “DoD Components”) that possess BSAT in quantities justified by a prophylactic, protective, or other peaceful purpose.

(2) DoD entities located overseas not subject to the SAR and Reference (j) to the maximum extent possible. Where implementation of specific provisions is not feasible, alternative provisions will be based on host nation and sponsor requirements (whichever is most stringent) and site-specific risk assessments.

(3) Contracts that cover requirements for access to BSAT to the extent that applicable provisions are incorporated into and made a part of the contract.

b. Applies partially to DoD clinical or diagnostic laboratories and other DoD entities that voluntarily elect to register under the Federal Select Agent Program (FSAP) even though they are exempt from FSAP regulations ((referred to in paragraph 2.c.(2)) in which case application of this instruction is limited to:

(1) Maintain registration with the FSAP, adhere to applicable SAR requirements, and keep this information in the DoD BSAT database in accordance with paragraph 9(c) of Enclosure 4 of this instruction.

(2) Provide the Center for Disease Control and Prevention (CDC) or Animal and Plant Health Inspection Service (APHIS) reports and inspection results that may lead to entity closure in accordance with paragraph 2b of Enclosure 7.

c. 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 (Reference (1)).

(2) DoD clinical or diagnostic laboratories and other entities that do not retain possession of BSAT (or have exempt amounts of BSAT) and are **not** required to be registered with the Federal Select Agent Program (FSAP) because of exemptions in sections 73.5 or 73.6 of Reference (f), sections 121.5 or 121.6 of Reference (h), or section 331.5 of Reference (g). However, such laboratories and other entities that voluntarily register are subject to this instruction to the extent provided in paragraph 2.b.

(3) Non-DoD entities that receive transfers of DoD BSAT, that must comply with the SAR and any appropriate contract clauses regarding use or disposition of DoD BSAT.

3. POLICY. It is DoD policy that:

a. DoD comply with the provisions of the Biological Weapons Convention (Reference (m)) and DoDD 2060.1 (Reference (n)).

b. All DoD entities using, possessing, transferring, or receiving BSAT be registered with the FSAP in accordance with the SAR.

c. Threats to BSAT, including theft, loss, diversion, release, or unauthorized access, transfer, use, or production, be mitigated to an acceptable risk in accordance with this instruction.

(1) Authorities and responsibilities of the DoD Component commanders and directors for security of DoD property are delineated in paragraphs 3.2 and 3.3 of Reference (e) and paragraph C1.2.2 of DoD 5200.08-R (Reference (o)). The countermeasures for risk mitigation may not exceed those stated in this instruction without approval or a waiver.

(2) Requirements in this instruction do not abrogate the responsibility of commanders or directors to apply more stringent security standards during emergencies pursuant to paragraph C1.2.4 of Reference (o).

d. Movement of BSAT be minimized consistent with operational, research, training, teaching, safety, and security requirements.

e. The number of people authorized access to BSAT be kept to the minimum consistent with operational, safety, and security requirements.

f. Individuals with a need to access BSAT be screened through the security risk assessment (SRA) process as described in the SAR. Individuals who need to access Tier 1 BSAT or whose duties afford access to registered spaces (e.g., storage and work areas, storage containers and equipment) containing Tier 1 BSAT will be screened through the SRA process and subsequently for suitability and reliability through the biological personnel reliability program (BPRP) process as described in this instruction.

g. DoD Components include BSAT entities in Combating Terrorism and Antiterrorism (AT) Programs for a collective, proactive effort focused on the prevention and detection of terrorist attacks pursuant to the requirements, policy, and responsibilities specified in DoDI 2000.12 (Reference (p)).

h. Internal control material weaknesses be reported in compliance with DoDI 5010.40 (Reference (q)).

i. Technology transfer and export control requirements for BSAT be implemented in accordance with DoDI 2040.02 (Reference (r)) and other applicable authorities, including: section 2778 of Title 22, United States Code (also known as the “Arms Export Control Act (AECA)”) (Reference (s)); chapter 35 of Title 50, United States Code (also known as the “International Emergency Economic Powers Act (IEEPA)”) (Reference (t)); part 120-130 of Title 22, Code of Federal Regulations (also known as the “International Traffic in Arms Regulations

(ITAR)”) (Reference (u)); and parts 730-774 of Title 15, Code of Federal Regulations (also known as the “Export Administration Regulations (EAR)”) (Reference (v)).

j. Ricin and saxitoxin, regardless of the amount, are subject to accountability, use, and production restrictions under the Chemical Weapons Convention (CWC) (Reference (w)) as Schedule 1 chemicals, and the semi-annual reporting requirements in DoDI 5210.65 (Reference (x)). CWC production and acquisition requirements will be followed when used for protective purposes. Entities possessing ricin and saxitoxin in quantities greater than BSAT threshold amounts must also comply with this instruction for all other purposes.

k. DoD Components not impose more restrictive or stringent implementing requirements for security of BSAT than those in this instruction unless such implementing guidance is approved by the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (ASD(NCB)).

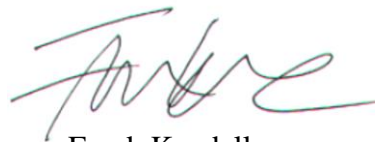
4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3 through 7.

6. INFORMATION COLLECTION REQUIREMENTS. The annual BPRP report, referred to in paragraph 4e of Enclosure 2 and paragraph 2a of Enclosure 7 of this instruction, has been assigned report control symbol DD-AT&L(A)2583 in accordance with the procedures in Volume 1 of DoD Manual 8910.01 (Reference (y)).

7. RELEASABILITY. **Cleared for public release**. This instruction is available on the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

8. EFFECTIVE DATE. This instruction is effective January 19, 2016. Full compliance with Enclosures 4 and 5 of this instruction is required within 180 calendar days of the effective date.



Frank Kendall
Under Secretary of Defense for Acquisition,
Technology, and Logistics

Enclosures

1. References
2. Responsibilities

3. Waivers and Exceptions
 4. Security Standards
 5. BPRP
 6. Visitors
 7. BSAT Reports
- Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....8

ENCLOSURE 2: RESPONSIBILITIES11

 ASD(NCB).....11

 ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND
 GLOBAL SECURITY (ASD(HD&GS))11

 DIRECTOR, DEFENSE INTELLIGENCE AGENCY12

 DoD COMPONENT HEADS.....12

 SECRETARY OF THE ARMY13

ENCLOSURE 3: WAIVERS AND EXCEPTIONS14

ENCLOSURE 4: SECURITY STANDARDS15

 GENERAL.....15

 PERSONNEL SECURITY15

 PHYSICAL SECURITY SYSTEMS15

 SECURITY FORCES17

 SECURITY MEASURES.....18

 ACCESS CONTROL.....19

 BSAT STORAGE.....20

 REPORTING INCIDENTS21

 INVENTORY, ACCOUNTABILITY, AND RECORDS.....21

 INFORMATION AND INFORMATION SYSTEMS SECURITY21

 TRANSPORTATION.....22

 TRANSFER OF DoD BSAT22

ENCLOSURE 5: BPRP23

 GENERAL.....23

 QUALIFYING STANDARDS.....23

 BPRP DENIAL OR TERMINATION CRITERIA24

 INITIAL CERTIFICATION.....25

 CONTINUING EVALUATION27

 REMOVAL FROM BPRP DUTIES27

ENCLOSURE 6: VISITORS.....29

ENCLOSURE 7: BSAT REPORTS30

 GENERAL.....30

 DoD COMPONENT REPORTS TO THE ASD(NCB)31

INVENTORY AND ACCOUNTABILITY RECORDS.....32

GLOSSARY33

PART I: ABBREVIATIONS AND ACRONYMS33

PART II: DEFINITIONS.....34

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5210.88, “Safeguarding Biological Select Agents and Toxins,” February 11, 2004 (hereby cancelled)
- (b) DoD Directive 5134.01, “Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)),” December 9, 2005, as amended
- (c) Deputy Secretary of Defense Memorandum, “Transfer of Under Secretary of Defense for Intelligence Principal Staff Assistant Responsibilities for DoD Chemical and Biological Security Policy,” June 3, 2012
- (d) Deputy Secretary of Defense Memorandum, “Implementation of the Recommendations in the Comprehensive Review Report: Inadvertent Shipment of Live Bacillus anthracis (Anthrax) Spores by Department of Defense,” July 23, 2015
- (e) DoD Instruction 5200.08, “Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB),” December 10, 2005, as amended
- (f) Part 73 of Title 42, Code of Federal Regulations (also known as “Select Agents and Toxins,”) December 4, 2012, as amended¹
- (g) Part 331 of Title 7, Code of Federal Regulations (also known as “Possession, Use, and Transfer of Select Agents and Toxins”) December 4, 2012, as amended¹
- (h) Part 121 of Title 9, Code of Federal Regulations (also known as “Possession, Use, and Transfer of Select Agents and Toxins”) December 4, 2012, as amended¹
- (i) Executive Order 13546, “Optimizing Security of Biological Select Agents and Toxins in the United States,” July 2, 2010
- (j) Public Law 107-188 (sections 201–231 are known as “Public Health Security and Bioterrorism Response and Preparedness Act of 2002”), June 12, 2002
- (k) DoD Instruction 5210.89, “Minimum Security Standards for Safeguarding Biological Select Agents and Toxins,” April 18, 2006 (hereby cancelled)
- (l) DoD Manual 6055.18, “Safety Standards for Microbiological and Biomedical Laboratories,” May 11, 2010
- (m) “Convention on the Prohibition on the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and On Their Destruction (BWC),” ratified March 26, 1975
- (n) DoD Directive 2060.1, “Implementation of, and Compliance with, Arms Control Agreements,” January 9, 2001
- (o) DoD 5200.08-R, “Physical Security Program,” April 9, 2007, as amended
- (p) DoD Instruction 2000.12, “DoD Antiterrorism (AT) Program,” March 1, 2012, as amended
- (q) DoD Instruction 5010.40, “Managers’ Internal Control Program Procedures,” May 30, 2013
- (r) DoD Instruction 2040.02, “International Transfers of Technology, Articles, and Services,” March 27, 2014
- (s) Section 2778, Title 22, United States Code (also known as the “Arms Export Control Act (AECA)”)

¹ Copies and companion guidance documents may be obtained from the Internet at <http://www.selectagents.gov/>

- (t) Chapter 35, Title 50, United States Code (also known as the “International Emergency Economic Powers Act (IEEPA)”)
- (u) Parts 120-130 of Title 22, Code of Federal Regulations (also known as the “International Traffic in Arms Regulations (ITAR)” as amended)
- (v) Parts 730-774 of Title 15, Code of Federal Regulations (also known as the “Export Administration Regulations (EAR)” as amended)
- (w) “Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction,” April 29, 1997
- (x) DoD Instruction 5210.65, “Security Standards for Safeguarding Chemical Agents,” January 19, 2016
- (y) DoD Manual 8910.01, Volume 1, “DoD Information Collections Manual: Procedures for DoD Internal Information Collections,” June 30, 2014
- (z) DoD Directive 5111.18, “Assistant Secretary of Defense for Global Strategic Affairs (ASD(GSA)),” June 13, 2011
- (aa) DoD Directive 2060.02, “Department of Defense (DoD) Combating Weapons of Mass Destruction (WMD) Policy,” April 19, 2007
- (ab) DoD Instruction 5230.29, “Security and Policy Review of DoD Information for Public Release,” August 13, 2014
- (ac) DoD Directive 5122.05, “Assistant Secretary of Defense for Public Affairs (ASD(PA)),” September 5, 2008
- (ad) DoD Instruction 2000.16, “DoD Antiterrorism (AT) Standards,” October 2, 2006, as amended
- (ae) DoD Directive 5205.16, “The DoD Insider Threat Program,” September 30, 2014
- (af) DoD Directive 5210.56, “Carrying of Firearms and the Use of Force by DoD Personnel Engaged in Security, Law and Order, or Counterintelligence Activities,” April 1, 2011
- (ag) DoD Manual 5200.01, Volumes 1 - 4, “DoD Information Security Program,” February 24, 2012, as amended
- (ah) DoD Instruction 8520.02, “Public Key Infrastructure (PKI) and Public Key (PK) Enabling,” May 24, 2011
- (ai) DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” March 12, 2014
- (aj) DoD Instruction 8550.01, “DoD Internet Services and Internet-based Capabilities,” September 11, 2012
- (ak) DoD Directive 5230.09, “Clearance of DoD Information for Public Release,” August 22, 2008
- (al) Defense Transportation Regulation (DTR) 4500.9-R, “Defense Transportation Regulation, Part II, Cargo Movement, Chapter 204, Hazardous Material,” August 16, 2013
- (am) DoD Directive 5230.20, “Visits and Assignments of Foreign Nationals,” June 22, 2005
- (an) DoD 5200.2-R, “Personnel Security Program,” January 1, 1987, as amended
- (ao) DoD Instruction 5200.02, “DoD Personnel Security Program (PSP),” March 21, 2014, as amended
- (ap) Director of National Intelligence Memorandum, “Adherence to Federal Laws Prohibiting Marijuana Use,” October 25, 2014
- (aq) American Psychiatric Association, “American Psychiatric Association Diagnostic and Statistical Manual (DSM) of Mental Disorders,” Fifth Edition, Arlington, VA, 2013

- (ar) DoD Instruction 6495.02, "Sexual Assault Prevention and Response (SAPR) Program Procedures," March 28, 2013, as amended
- (as) DoD Instruction 1010.09, "DoD Civilian Employee Drug-Free Workplace Program," June 22, 2012
- (at) DoD Instruction 1010.01, "Military Personnel Drug Abuse Testing Program (MPDATP)," September 13, 2012
- (au) Title 18, United States Code

ENCLOSURE 2

RESPONSIBILITIES

1. ASD(NCB). Under the authority, direction, and control of the Under Secretary of Defense for Acquisition, Technology, and Logistics, the ASD(NCB):

a. Establishes security standards for safeguarding BSAT and approves waivers and exceptions to those standards. Coordinates with the National Security Council as appropriate for issues that exceed the SAR. This authority will not be delegated.

b. Establishes standards for a BPRP for individuals with access to Tier 1 BSAT.

c. Oversees the BSAT security program.

d. 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).

e. Coordinates with the CDC and APHIS FSAP proponent offices. Serves as the Department point of contact with the CDC and APHIS on incidents covered by this Instruction. Stays current on changes to the SAR, including the listing of agents or toxins designated as BSAT and Tier 1 BSAT. Provides guidance to DoD Components accordingly.

f. Establishes, where applicable, procedures for each DoD Tier 1 BSAT entity to report through command channels to ASD(NCB) individuals who are denied entry or terminated from the BPRP and a method to share that information across DoD personnel reliability programs.

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

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

2. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY (ASD(HD&GS)). Under the authority, direction, and control of the Under Secretary of Defense for Policy (USD(P)), and consistent with DoDD 5111.18 (Reference (z)) and DoDD 2060.02 (Reference (aa)), the ASD(HD&GS):

a. Coordinates on biosecurity policy and planning and represents USD(P) on interagency biosecurity committees and working groups.

b. Develops policy for DoD consequence management involving biological agents.

3. DIRECTOR, DEFENSE INTELLIGENCE AGENCY. Under the authority, direction, and control of the Under Secretary of Defense for Intelligence and in addition to the responsibilities in section 4 of this enclosure, the Director, Defense Intelligence Agency, produces for the ASD(NCB) a multidisciplinary threat assessment addressing the foreign intelligence and security services, terrorism, information operations, sabotage, and proliferation threats related to BSAT every 3 years, or more frequently if required.

4. DoD COMPONENT HEADS. The DoD Component heads:

a. Direct the commander or director of each DoD BSAT entity in their Component to comply with the requirements established in this instruction and the SAR.

b. Plan and program fiscal and personnel resources necessary to implement the policy and requirements in this instruction.

c. Notify the ASD(NCB) before registering any new DoD BSAT entity with the CDC or APHIS and following removal of registration.

d. Ensure BSAT entities are registered according to federal, State, and local regulations.

e. Submit to the ASD(NCB) annual statistical data concerning the BPRP in accordance with guidance from the ASD(NCB) and paragraph 2a of Enclosure 7 of this instruction.

f. Coordinate and approve as part of pre-incident planning proposed public releases of information pertaining to BSAT with the Director, Washington Headquarters Services (WHS), pursuant to DoDI 5230.29 (Reference (ab)). Once Director, WHS has cleared information for public release, coordinate with the Assistant to the Secretary of Defense for Public Affairs (ATSD(PA)) before release, pursuant to DoDD 5122.05 (Reference (ac)). Information related to public safety will be coordinated as part of pre-incident planning, but information release during an incident will not be delayed and will be in accordance with local agreements. Notify Director, WHS and the ATSD(PA) immediately when such information is released.

g. Comply with the secure DoD BSAT database procedures established by the ASD(NCB).

h. Ensure the commander or director of a Component BSAT entity:

(1) Has overall responsibility for execution of the BSAT program at the entity.

(2) Designates the RO who reports directly to the FSAP in coordination with the entity commander or director.

(3) Uses the DoD BSAT database to record inventory and accountability information in accordance with this instruction.

(4) Conducts and documents a site-specific vulnerability assessment initially at each DoD BSAT entity, then reviews and updates it annually or as a new vulnerability or threat becomes known. The vulnerability assessment will consider the current threat assessment, physical surveys, and AT standards from DoDI 2000.16 (Reference (ad)).

i. Establish an inspection process for BSAT entities that ensures:

(1) The RO conducts and documents annual inspections for all registered spaces (each laboratory and storage area) where BSAT are stored or used to comply with the SAR.

(2) DoD Components will accept the results of inspections conducted by APHIS or CDC to verify compliance with the SAR. If the DoD Component opts to conduct its own inspections above entity-level, they will be conducted jointly with the inspections scheduled and conducted by APHIS or CDC to the maximum extent possible.

j. Endorse waiver and exception requests forwarded to the ASD(NCB).

5. SECRETARY OF THE ARMY. In addition to the responsibilities in section 4 of this enclosure, the Secretary of the Army:

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

b. Serves as DoD Executive Agent for the DoD BSAT Biosafety Program as designated in Reference (d), with responsibility for the technical review, inspection, and harmonization of biosafety protocols and procedures across DoD laboratories that handle BSAT and tasking authority of all DoD Components for this purpose.

ENCLOSURE 3

WAIVERS AND EXCEPTIONS

1. Requests for waivers and exceptions from this instruction will be forwarded via the appropriate chain of command to reach the ASD(NCB) within 30 days of submission by the initiator. The ASD(NCB) will review waivers and exceptions on a case-by-case basis and respond within 30 days of receipt; the waivers can be written to apply to multiple situations. If the waiver or exception results in a more stringent or restrictive requirement, the ASD(NCB) will coordinate with the National Security Council. A waiver from this instruction will not be considered if the requirement does not authorize a waiver, and it is based on a statute, a regulation, a policy of a higher authority, or is imposed by another federal agency.
2. A waiver may be approved for temporary relief from a specific requirement prescribed in this instruction pending actions to conform to the requirement. Such waivers will be approved for only as long as needed and will normally not exceed 1 year. While waivers are in effect, compensatory security measures will be required to mitigate any increases in risk or vulnerability as a result of the waiver.
3. An exception may be approved for permanent relief from a specific requirement as prescribed in this instruction when there are unique circumstances at the BSAT entity that make conforming to the requirement impractical or an inappropriate use of resources.
4. Whenever conditions or compensatory measures change, a request for an amendment to or cancellation of the waiver or exception will be sent to the ASD(NCB).
5. Physical security surveys, reports, and inspections will include and document a review of approved waivers and exceptions to ensure that conditions described in the request remain accurate and that compensatory measures are fully implemented. The physical security survey or inspection report will include a comment regarding the actions taken as a result of that review.
6. Requests for waivers and exceptions will include:
 - a. Recommended compensatory security measures to mitigate any increased risk of vulnerability as a result of the waiver.
 - b. The projected duration of the waiver.
 - c. A complete and specific justification indicating why the waiver or exception is required.
 - d. Risks and vulnerabilities associated with granting the waiver or exception.
 - e. Projected costs associated with proposed security compensatory measures.
 - f. Recommendation from the DoD Component head.

ENCLOSURE 4

SECURITY STANDARDS

1. GENERAL. This enclosure 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 within BSAT registered spaces and consolidated to the maximum extent possible. BSAT will be secured, stored, and transported to meet the physical security requirements pursuant to References (e), (l), and (o) and the security standards in this enclosure.

b. Unauthorized access, movement, use of BSAT, or attempts to steal or divert BSAT outside physical security controls will be reported in accordance with the SAR and as described in Enclosure 7 of this instruction.

c. Security planning and execution will be in accordance with Reference (e) as applicable, and based on the standards identified in this instruction and a specific risk analysis and vulnerability assessment of the entity. An appropriate risk management process will be used, consistent with that prescribed in Reference (ad), 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.

2. PERSONNEL SECURITY. Access to BSAT requires the appropriate level of personnel certification based on background investigation evaluations. Personnel may also need escort or supervision by persons certified in the BPRP as described in Enclosure 6.

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.

c. Visitors requiring access to BSAT, Tier 1 BSAT, or BSAT registered spaces will follow the procedures in Enclosure 6 of this instruction.

3. PHYSICAL SECURITY SYSTEMS

a. The DoD BSAT entity commander or director will develop 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 ensure vulnerabilities are mitigated or the risk accepted in accordance with the SAR and References (e) and (o), as applicable.

(1) The plan will be based on a systematic approach in which 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. Commanders and directors in the chain of command may accept the stated risk(s) or direct further mitigation and will ensure resourcing for approved countermeasures.

(2) The security plan will address the controls used to secure the BSAT from misuse, theft, and unauthorized removal from the BSAT registered space.

(3) Where 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 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.

(4) The organization responsible for executing armed responses at BSAT entities will develop response plans in coordination with the supported entity to ensure acceptable levels of support in accordance with the SAR.

(5) 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) Control of access for BSAT registered spaces.

(b) An information protection plan to ensure the appropriate security of information on BSAT and the research or mission being conducted.

(c) Initial and annual training of personnel in procedures for securing BSAT registered spaces, security and positive control of keys, changing access numbers or locks following staff changes, reporting and removing unauthorized individuals, access control and records requirements, inventory control, and other appropriate security measures.

(d) Procedures, reporting requirements, and administrative actions for lost or compromised keys, passwords, combinations, and security incidents and violations.

(e) Procedures for removal of suspicious or unauthorized persons and procedures for reporting of unauthorized or suspicious persons or activities and potential, attempted, or actual loss or theft of BSAT or alteration of inventory records.

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

(g) Inventory control process to ensure strict accountability that includes records of access, records of use, and the final disposition of all BSAT.

(h) Plans, procedures, requirements, and processes for safeguarding or destruction of BSAT in emergency situations (e.g., natural disasters, fires, power outages, and general emergencies in entities containing BSAT).

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

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

(b) Procedures for management of access controls (e.g., keys, card keys, common access card (CAC), access logs, biometrics, and other access control measures) for each of the security barriers in the security plan.

(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 for testing the IDS and managing its configuration.

(e) Procedures for responding to an access control or intrusion detection system failure (e.g., erroneous alarm).

(f) Procedures for visitor screening.

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

(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 section 11(f)(2) of Reference (f) or equivalent section of Reference (g) or (h). Ideally, the entity's RO, safety, and security professionals will meet on a regular or defined basis. This may be annually in conjunction with the security plan review, after a security incident, when there is a significant entity change that affects security, or in response to a threat.

4. SECURITY FORCES

a. There will be a sufficient security force available at all times to respond rapidly to unauthorized attempted penetrations and prevent the unauthorized removal of BSAT or data. Consistent with the requirements of Reference (e) and DoDD 5210.56 (Reference (af)), installation commanders will issue the necessary regulations for the protection and security of property or places under their command.

b. 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 entity) based on the threat and vulnerability assessment, including 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.

c. Security force members will participate in appropriate, realistic, site defense force training exercises at a frequency determined by the DoD Component in accordance with Reference (f). The training will be tailored to each BSAT entity based on the threat and vulnerability assessment conducted at the site.

5. SECURITY MEASURES

a. Security Barriers. BSAT entities must have security barriers which both deter intrusion and deny access by unapproved personnel to the areas containing BSAT. Barriers may consist of physical obstacles (e.g., perimeter fences, walls, locked doors, security windows) or trained personnel (e.g., security guards, laboratory personnel, or escorts).

(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 barriers, counted from the Tier 1 BSAT outward. When trained personnel are designated as one of the three barriers pursuant to Reference (f), they must be dedicated to that task. These physical barriers must be identified on the entity's registration and discussed in the 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 <http://www.selectagents.gov>).

b. Other Security Measures. Cameras, security lighting, and IDS are not considered security barriers because while they may monitor access, they cannot, by themselves, prevent access.

(1) Perimeter Security Lighting. BSAT entities will determine perimeter lighting needs based on threat and vulnerability assessments.

(2) IDS. The IDS will be equipped with monitoring capability to detect and report attempted or unauthorized penetration to IDS equipment or communication lines.

(a) For BSAT registered spaces, an entity may consider using IDS based on a threat and vulnerability 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 an unauthorized penetration and meet the physical security standards in DoDM 5200.01 (Reference (ag)).

(3) Cameras. Although cameras alone cannot be used as security barriers because they cannot prevent access, they can be used to monitor barriers or for other risk mitigation based on site-specific risk assessments.

6. ACCESS CONTROL. Access control measures ensure that only authorized individuals as described in section 2 of this enclosure have access to BSAT or to areas where BSAT is present.

a. The access control system will include provisions for the safeguarding of animals and plants exposed to or infected with BSAT in accordance with sections 11(c)(2) and 11(d)(1) of Reference (f) or equivalent sections of Reference (g) or (h).

b. Each individual authorized access to BSAT will have a unique means of accessing the agent pursuant to section 11(d)(6) of Reference (f) or equivalent sections of Reference (g) or (h). The BSAT entity personnel will review access logs (automated or manual) monthly. The log will reflect the name of the individual, date and time of entry, and name of escort, if appropriate, into a BSAT registered space.

c. The entity will modify the access control system when an individual's authorization for access changes.

d. Smart card technology will be implemented in accordance with DoDI 8520.02 (Reference (ah)).

e. 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 a minimum, a photograph, the wearer's name, and an expiration date. Visitors will be clearly identified as having escorted or unescorted access. Entity administrators will consider using 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 BSL-3 or -4 containment suites.

f. The entity will ensure a duress system is in place to enable authorized personnel to covertly communicate an adverse situation.

g. An automated entry control system (AECS) may be used to control access in lieu of visual control if it meets the criteria stated in paragraphs 6g(1)-(9) of this enclosure. The AECS will authenticate the identification of an individual and verify the person's authority to enter the area through two separate methods of identification that may include ID badges, cards, a personal identification 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. Implement Reference (ah) as applicable.

(2) Personal identity verification via biometrics devices may be used to identify 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) 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 separately entered into the system by each individual using a keypad device and will consist of four or more digits, randomly selected, with no known or logical association with the individual. The PIN will be changed if it is believed it has been 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 4b of this enclosure. Protection will address covert or clandestine entry into BSAT registered spaces through electrical, communications, or HVAC 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, and will be securely fastened to the wall or other permanent structure to prevent unauthorized access through breaching of attachment mechanisms (screws, pins, bolts, etc.). 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.

7. BSAT STORAGE

a. When not in use, all BSAT will be stored in refrigerators, freezers, or other approved storage devices within 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.

8. REPORTING INCIDENTS. Upon discovery of the theft, loss, release of, or exposure to BSAT, entities must report all incidents as specified in Enclosure 7 of this instruction.

9. INVENTORY, ACCOUNTABILITY, AND RECORDS

a. Each BSAT entity must maintain a current and accurate inventory. The DoD BSAT database will be used to inventory and account for all BSAT at DoD BSAT entities registered with the FSAP. BSAT must be clearly marked and labeled to ensure proper handling and protection.

b. The inventory and accountability records will include specific details about the current inventory of BSAT including type and quantities. Documentation of volume is only required for toxins. The entity will also document the names of all individuals who remove agent from long-term storage, date of removal, and disposition of agent (i.e., destruction or return to long-term storage) pursuant to section 17 of Reference (f) or equivalent section of Reference (g) or (h).

c. Each DoD Component will review subordinate BSAT entities' facility information in the DoD BSAT database monthly including facility name, address, and contact information; names of RO, ARO, and registration certificate number and expiration date.

10. INFORMATION AND INFORMATION SYSTEMS SECURITY

a. Data will be processed on systems assessed and authorized in accordance with DoDI 8510.01 (Reference (ai)).

b. Websites will be administered in accordance with DoDI 8550.01 (Reference (aj)).

c. Systems that use transmission lines to carry BSAT access authorizations, personal identification data, or verification data between devices or equipment located outside of the BSAT registered space will comply with DoD requirements as described in Reference (ag) to restrict unauthorized access and tampering.

d. Any classified or controlled unclassified information will be handled and protected in accordance with Reference (ag). Applicable program security classification guides will be developed for use when discussing or processing information related to BSAT. DD Form 254, "Department of Defense Contract Security Classification Specification," must include applicable classification guidance.

e. Public release of information will be in accordance with DoDD 5230.09 (Reference (ak)) and Reference (ac).

f. The SAR requires a BSAT entity to develop and implement a written security plan that describes procedures for information security control and contains provisions for information security in accordance with sections 11(c)(1) and (c)(9) of Reference (f) or equivalent sections of Reference (g) or (h).

g. The SAR requires safeguarding BSAT security information which includes, at a minimum: inventory access logs; passwords; entry access logbooks; rosters of individuals approved for access to BSAT; access control systems; security system infrastructure (e.g., floor plans, on-site guard, closed-circuit television, IDS); security plans; and incident response plans.

h. Locations where authorization data and personal identification or verification data are created, stored, or recorded will be protected in accordance with information security standards in Reference (ag).

i. The DoD BSAT database administrator will have an approved SRA or a secret clearance. Each entity's RO or ARO controls access to detailed quantitative facility records. Unless specifically authorized by an entity RO or ARO, the Service representatives are authorized access to their Service-specific qualitative records, and OSD representatives are authorized access to all DoD facility qualitative records. Requests for Service or OSD access should be sent to the ASD(NCB).

11. TRANSPORTATION. The transportation of BSAT will be in accordance with the SAR and DoD 4500.9-R (Reference (al)). BSAT will be shipped or transported following submission and approval of APHIS/CDC Form 2, "Request to Transfer Select Agents and Toxins" (available from <http://www.selectagents.gov>), which will ensure the entity's use of CDC-approved carriers that maintain anonymity during shipment. For Variola virus, follow the FSAP instructions. Maintain transportation records and delivery receipts for at least 3 years.

12. TRANSFER OF DoD BSAT

a. The DoD Components may transfer DoD BSAT to other FSAP BSAT entities that are registered for that specific BSAT and will assume responsibility and accountability for the BSAT in accordance with federal regulations, including the SAR, section 16 of Reference (f), or equivalent sections of References (g) or (h).

b. The DoD Components will not provide DoD BSAT to non-U.S. governmental overseas facilities unless approved by the ASD(NCB). Requests will identify recipient information, name and quantity of BSAT to be provided, purpose for which the BSAT will be used, and rationale for providing BSAT. The request will also include a site-specific risk assessment for the agent being transferred. Approval will identify security measures and requirements for the recipients and comply with applicable national and international laws and regulations, as appropriate.

ENCLOSURE 5

BPRP

1. GENERAL

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

b. The reviewing official (REV) in most cases is the commander or director. However, the commander or director may designate a REV, as appropriate. The REV will monitor the BPRP and review and approve suitability actions in accordance with DoD Component implementing guidance. The intent is for the REV to monitor certification decisions of the CO to oversee the status and quality of the program, and to overturn CO decisions if procedures have been unfairly, inconsistently, or incorrectly applied.

c. The RO is responsible for determining an individual's eligibility for access to BSAT.

d. The CO is responsible for determining an individual's BPRP eligibility for access to Tier 1 BSAT.

e. 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.

f. Both the CO and RO must concur for an individual to have access to Tier 1 BSAT.

g. Foreign nationals who receive supervised or 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, Reference (r), DoDD 5230.20 (Reference (am)), DoD 5200.2-R (Reference (an)), and DoDI 5200.02 (Reference (ao)).

h. In DoD overseas facilities, 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, threat, and vulnerability 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 References (s), (t), (u), and (v).

2. QUALIFYING STANDARDS. All individuals assigned duties requiring BPRP certification must meet the qualifying reliability standards in this section.

a. Emotional and mental stability, trustworthiness, physical competence, and adequate training to perform the assigned duties.

b. Dependability in executing BPRP responsibilities.

c. Flexibility and adaptability in adjusting to the restrictive and demanding work environment with Tier 1 BSAT that must be strictly controlled and secured.

d. Ability to pass drug or substance abuse testing before being certified into the BPRP. State laws pertaining to marijuana use do not authorize violations of federal law, nor can they alter existing National Security Adjudicative Guidelines, in accordance with Director of National Intelligence Memorandum (Reference (ap)). Positions requiring BPRP certification will be designated for random testing. Results of the drug or substance abuse test will be submitted to the CO.

3. BPRP DENIAL OR TERMINATION CRITERIA

a. Individuals will be denied admission to or terminated from the BPRP if they have a record of:

(1) Diagnosis of moderate or severe alcohol use disorder without sustained remission as defined in the current American Psychiatric Association's "Diagnostic and Statistical Manual of Mental Disorders" (Reference (aq)).

(2) Illegal trafficking, cultivation, processing, manufacture, or sale of illegal or controlled drugs or substances within the last 15 years.

(3) Drug or substance abuse (as defined in Glossary) in the 5 years before the initial BPRP interview. Isolated abuse of another individual's prescribed drugs is not a mandatory denial criteria, however, it must be evaluated as stated in paragraph 3b of this enclosure.

(4) Abuse of drugs or substances while enrolled or certified in any personnel reliability program. Isolated abuse of another individual's prescribed drugs is not a mandatory termination criteria, however, it must be evaluated following paragraph 3b of this enclosure.

b. The criteria in paragraphs 3b(1)-(7) regarding possible BPRP denial or termination require a competent medical authority (CMA) evaluation and recommendation and CO decision based on the "whole person" concept. COs will ensure an individual's reliability and assignment to a BPRP position is consistent with national security interests. When the criteria in paragraphs 3b(1)-(7) apply to an individual currently certified in the BPRP, the individual will be suspended immediately from BPRP duties pending CMA evaluation and CO decision. CMA recommendation may include the successful completion of a treatment regimen before the individual is certified into the BPRP or returned to BPRP duties.

(1) Alcohol-related incidents during the previous 5 years or any previous diagnosis of alcohol abuse, alcohol dependence, or alcohol use disorder.

- (2) Alcohol-related incidents when the individual is currently certified in the BPRP.
 - (3) Diagnosis of mild alcohol use disorder.
 - (4) Abuse of drugs more than 5 years before the initial BPRP screening or isolated abuse of another person's prescribed drug within 15 years of the initial BPRP screening.
 - (5) Exceeding the recommended safe dosage of over the counter substances or the individual's own prescribed medications.
 - (6) Suicide attempt or threats and jeopardizing human life or safety. The CMA evaluation will include a mental health assessment and evaluation.
 - (7) Medical, physical, or mental conditions not compatible with BPRP duties.
- c. The criteria in paragraphs 3c(1) and (2) will be evaluated by the CO based on the "whole person" concept to determine whether the individual will be denied entry or terminated from the BPRP.
- (1) Negligence or delinquency in performance of duty.
 - (2) Poor attitude or untrustworthiness with respect to BPRP responsibilities.

4. INITIAL CERTIFICATION

- a. The CO will ensure that initial screening for BPRP certification includes:
 - (1) Personnel Security Investigation. As part of the required screening process, the CO will verify personnel security clearance eligibility. If appropriate, the CO will review the results of the investigation. A current and favorably adjudicated National Agency Check with Local Agency Checks and Credit Checks (NACLC) or greater is required for military or contract employees or an Access National Agency Check with Credit Checks and Written Inquiries (ANACI) or greater for civilian employees.
 - (a) Foreign Nationals. Foreign nationals with requirements for access to Tier 1 BSAT will be processed for a Limited Access Authorization pursuant to References (am), (an), and (ao).
 - (b) Escorted Access. COs, with RO concurrence, may approve escorted access to Tier 1 BSAT pending completion of the personnel security investigation, provided the investigation has been opened and all other requirements for escorted access have been completed.
 - (2) 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 of the sexual assault in accordance with DoDI 6495.02 (Reference (ar)) 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. If necessary, the CMA will inform the CO that there are factors adversely impacting the individual's BPRP status and that the person in question should be temporarily suspended, without revealing that the person is a victim of sexual assault. This will preserve the restricted report for military or dependents and the requirement for confidentiality for persons not eligible for a restricted report.

(3) 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 (Reference (as)) and DoDI 1010.01 (Reference (at)).

(4) Personal Interview. The CO will conduct a personal interview with each BPRP candidate. Any relevant disqualifying information as described in section 3 of this enclosure will be solicited and, if appropriate, discussed during the interview. Information disclosed as a result of completed background investigations (e.g., financial issues) will be considered. Individuals must report any factors that could have an adverse impact on performance, reliability, or security while performing BPRP duties. Failure to report this information may result in denial of entry to the BPRP.

(5) Personnel Record Review. The CO will review the individual's personnel records, when available. Any CO that does not have the authority to access an individual's personnel record will ensure that the appropriate supervisor reviews the record and reports any factors that could have an adverse impact on performance, reliability, or security.

(6) Position Qualification. The CO will obtain evidence of demonstrated professional or technical proficiency, as appropriate. Evidence will be obtained through employment or academic records and appropriate interviews of former supervisors or academic instructors.

b. The BPRP eligible individual will sign an agreement affirming his or her responsibility to abide by the requirements for maintaining BPRP certification. Once a determination regarding an individual's certification for access to Tier 1 BSAT is made, the CO will notify the RO.

c. If the CO determines that the individual does not meet the criteria for the BPRP, the CO will stop the screening process and deny the individual entry into the BPRP.

5. CONTINUING EVALUATION. Individuals certified under the BPRP are observed on a frequent and consistent basis by peers, supervisors, and program officials to ensure their behavior and performance meet all of the requirements of the program.

a. CO Observation. COs will observe the behavior and performance of individuals certified under the BPRP on a frequent and consistent basis.

b. Individual and Peer Reporting. Individuals certified in the BPRP are responsible for monitoring themselves and their BPRP-certified peers. Individuals must report to the supervisor, CO, or CMA factors that could have an adverse impact on performance, reliability, or security while performing BPRP duties. Failure to discharge these responsibilities may cast doubt on an individual's reliability.

c. Supervisor Reporting. Supervisors must notify the CO of factors that could have an adverse impact on performance, reliability, or security while performing BPRP duties.

d. Drug Testing. Positions requiring BPRP certification will be designated for random testing. Positive test results will be reported to the CO and result in termination (for cause) unless the result is authorized or explained.

e. Personnel Security Investigations. Individuals will complete periodic reinvestigations in accordance with Reference (an).

f. Medical

(1) Health records will reflect the assignment of an individual to a position requiring BPRP certification to ensure the proper treatment, review, and reporting of disqualifying information to the CO. All disqualifying medical information will be documented in the individual's health records. The record must be annotated to show evidence of transmission to the CO.

(2) The individual will report any medical evaluation, treatment, or medication to the CMA to determine if there is any effect on the individual's reliability to perform BPRP duties. When a sexual assault victim elects restricted reporting of the sexual assault pursuant to Reference (ar) or intends that the sexual assault remain confidential, the victim will inform the CMA. The CMA will not disclose to the CO that the individual is a sexual assault victim.

6. REMOVAL FROM BPRP DUTIES

a. A CO may impose an administrative 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 attitude or trustworthiness.

b. When the CO receives information relative to the decertifying criteria in section 3 of this enclosure, the CO 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. Within 15 workdays of the suspension, the CO will provide the individual, in writing, the reason(s) for suspension. Individuals suspended will remain under continuous evaluation for BPRP purposes until terminated or reinstated into the BPRP.

c. COs will ensure actions of denial or termination and any steps relating to re-certification are accurately recorded in the affected individual's personnel record.

d. When an individual is no longer required to perform BPRP duties, the CO will administratively terminate the individual from the BPRP.

ENCLOSURE 6

VISITORS

1. 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 who require entry into BSAT registered spaces. Escort procedures will be developed as part of each entity's security plan to include:

a. Section 11(d) (2) of Reference (f) or equivalent section of Reference (g) or (h) for allowing individuals not approved for access to conduct routine cleaning, maintenance, repairs, or other activities not related to BSAT.

b. Visitor entry procedures as prescribed by section 11(f) (4)(iii) of Reference (f) or equivalent section of Reference (g) or (h), for entities possessing Tier 1 BSAT.

c. Section 15(a) (2) of Reference (f) or equivalent section of Reference (g) or (h), for providing visitors with information and training on biosafety, security (including security awareness), and incident response.

d. Section 15(d) of Reference (f) or equivalent section of Reference (g) or (h) for RO requirement to ensure a record of the training provided to each escorted individual is maintained.

2. Only BPRP-certified individuals can be authorized to escort or supervise the access of visitors for training with Tier 1 BSAT. The visitor must be listed on the host entity's registration, have an approved SRA, and either be enrolled in the host entity's BPRP or have a BPRP suitability memorandum from the home entity.

3. The entity commander or director may permit unescorted entry to a BSAT registered space if BSAT are secured in accordance with Enclosure 4 of this instruction and the individual meets SAR requirements for BSAT access. A person requiring access to Tier 1 BSAT who is not BPRP-certified by the entity, but who is part of another BSAT entity's BPRP (or pre-access suitability assessment and ongoing suitability monitoring), may have access with the approval of the RO when supervised or escorted by a BPRP-certified individual present in the BSAT registered space.

ENCLOSURE 7

BSAT REPORTS

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:

(1) If the RO has a reasonable suspicion that a theft, loss, release, or occupational exposure has occurred.

(2) To receive guidance if unsure whether a report is required.

(3) Even if BSAT is subsequently recovered or the responsible parties are identified.

b. Information will be submitted as it becomes known, but no later than 24 hours.

c. 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 <http://www.selectagents.gov>, to the agency with which it is registered, the CDC or the APHIS .

d. The individual or entity will notify the appropriate federal, State, or local law enforcement 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 of thefts or suspicious activity that may be criminal in nature.

e. DoD Components will report BSAT mishaps and incidents to the National Joint Operational Intelligence Center (NJOIC) (non-classified telephone: 703-693-3834; classified telephone: 703-697-4800; NIPRNET e-mail: njoicddo_addo@mail.mil) via direct telephonic notification within 1 hour from the time it is confirmed the event has occurred. Identify the report submitted to NJOIC as a "biological mishap or incident" to trigger the appropriate NJOIC action. All reports will also be forwarded in accordance with DoD Component procedures.
Report:

(1) The theft, loss, recovery, suspected theft, inventory shortage or overage, 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) Discharge 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 1c(1) through 1c(7) of this enclosure that the DoD Components determine to be of immediate concern to DoD based upon the nature, gravity, and potential for adverse publicity or potential consequences of the incident.

2. DoD COMPONENT REPORTS TO THE ASD(NCB). The DoD Components will:

a. Provide a BPRP status report no later than February 15 each year. The report will:

(1) State the entity or organization 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 entity or organization actually certified into the BPRP as of December 31.

(4) List the total number of BPRP-certified personnel (separated into military, DoD civilian, and contractor employees) at each entity or organization denied entry or terminated during the calendar year.

(5) List the number of terminations categorized by primary reason for termination as cited in section 3 and paragraph 6d of Enclosure 5.

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

b. Provide a summary of DoD Component and CDC or APHIS reports and inspection results that may lead to entity closure.

c. Maintain, in accordance with DoD Component guidance:

(1) Security incident reports, threat and vulnerability assessments, and vulnerability assessment annual review.

(2) Inspection and exercise records and reports.

(3) Corrective action and improvements.

(4) Training records.

3. INVENTORY AND ACCOUNTABILITY RECORDS. All records and reports associated with this instruction will be maintained for 3 years and then handled according to appropriate DoD Component administrative instructions.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AECS	automated entry control system
ANACI	access national agency check with written inquiries
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
AT	antiterrorism
ATSD(PA)	Assistant to the Secretary of Defense for Public Affairs
BPRP	biological personnel reliability program
BSAT	biological select agents and toxins
CAC	common access card
CDC	Centers for Disease Control and Prevention
CFR	Code of Federal Regulations
CMA	competent medical authority
CO	certifying official
CWC	Chemical Weapons Convention
DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
FSAP	Federal Select Agent Program
ID	identification
IDS	intrusion detection system
NACLC	national agency check with local agency checks and credit checks
NJOIC	National Joint Operational Intelligence Center

PIN	personal identification number
REV	reviewing official
RO	responsible official
SAR	select agent regulations
SRA	security risk assessment
WHS	Washington Headquarters Services

PART II. DEFINITIONS

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

access. An individual will be deemed to have access to a BSAT at any point in time if the individual has possession of a BSAT (e.g., ability to carry, use, or manipulate) or the ability to gain possession of a BSAT.

alcohol-related incident. Any substandard behavior or performance in which alcohol consumption by the individual is a contributing factor as determined by law enforcement or disciplinary processes. Examples include intoxicated driving, domestic disturbances, assault, disorderly conduct, personal injury, failure to submit to alcohol testing, and underage drinking.

alcohol use disorder. A problematic pattern of alcohol use as defined by Reference (aq). Alcohol use disorders include criteria for severity (mild, moderate, or severe) and for remission (early or sustained).

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.

biological agent. Defined in section 178 of Title 18, United States Code (Reference (au)).

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 entity. An entity that is registered for and possesses BSAT.

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 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 certifying personnel for access to Tier 1 BSAT and ensuring the BPRP member is continually monitored. Responsibilities also include implementing, administering, and managing the BPRP, and supporting the entity commander or director, REV, RO, and ARO. Unless access to BSAT is required, 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 terminate the BPRP certification of an individual in training or 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.

long-term storage. A system designed to ensure viability or toxicity for future use, including but not limited to a refrigerator, freezer, or liquid nitrogen. Typically BSAT which are not part of an ongoing experiment or have not been accessed for a significant period of time (e.g., 30 calendar days) are placed in long-term storage.

random drug and substance abuse testing. A program where each member of the testing population has an equal chance of being selected. Random testing may include either testing of

designated individuals occupying a specified area, element, or position, or testing of those individuals based on a neutral criterion, such as a digit of the social security number.

restricted person. Defined in section 175b of Reference (au).

restriction

administrative. 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.

medical. 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 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 Reference (ad). The end product of the risk management process is the identification of areas and assets that are vulnerable to the identified threat attack means. 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 lessen the severity of the outcome of an attack.

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

administrative. Removal of reliable individuals from the program when they are leaving the position or no longer require access to BSAT or perform BPRP duties.

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.

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.

whole person concept. A balanced assessment of an individual, establishing a behavioral baseline in the environment in which that person works, lives, and socializes, along with mitigating circumstances, and discerning overall qualities of credibility and suitability.