Army Regulation 190–17

Military Police

Biological Select Agents and Toxins Security Program

Headquarters
Department of the Army
Washington, DC
5 March 2019

UNCLASSIFIED

SUMMARY of CHANGE

AR 190–17
Biological Select Agents and Toxins Security Program

This administrative revision, dated 19 July 2019—

- Changes supersedes to incorporates Army Directive 2016–24, (Department of Defense Biological Select Agent and Toxins Biosafety Program) (throughout).

This major revision, dated 5 March 2019—

- Provides Army responsibilities for the implementation of DODI 5210.88 (chap 1).
- Provides DODI 5210.88 policy guidance (chaps 2-6).
- Provides Army guidance to facilitate DODI 5210.88 implementation (apps A-F).
- Provides risk assessment procedures and worksheet for Biological Research Development Test & Evaluation facilities (throughout).
- Prescribes Select Agent Program security plan template and Army-specific requirements (throughout).
- Provides process for requesting waiver or exception for security measures that exceed or do not meet standards prescribed by DOD policy (throughout).
- Incorporates guidance from Army Directive 2016–24 (Department of Defense Biological Select Agent and Toxins Biosafety Program) (throughout).
- Supersedes and rescinds AR 50–1 Biological Surety, incorporating Biological Personnel Reliability Program guidance and prescribes use of AR 50–6, Chemical Surety, Chemical, and Biological Personnel Reliability Program, DA Form 3180–1, DA Form 3180–2, and DA Form 3180–3.

Headquarters
Department of the Army
Washington, DC
5 March 2019

*Army Regulation 190–17

Effective 5 April 2019

Military Police

Biological Select Agents and Toxins Security Program

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is a major revision.

Summary. This regulation prescribes DOD policy, Army responsibilities and guidance for safeguarding Army research, development, test, and evaluation and medical centers working with or storing biological select agents and toxins.

Applicability. This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent of this regulation is the Provost Marshal General. The proponent has the authority to approve exceptions or waivers to the biosecurity provisions of this regulation that are consistent with controlling law and regulations. Requests for exceptions or waivers to the biosafety provisions of this regulation must be directed to the Directory of Army Staff. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits, and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or director (senior leader) of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix F).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Provost Marshal General (DAPM–MPO–PS), 2800 Army Pentagon, Washington DC 20310–2800.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Provost Marshal General (DAPM–MPO–PS), 2800 Army Pentagon, Washington DC 20310–2800.

Committee management. AR 15–1 requires the proponent to justify establishing/continuing committee(s), coordinate draft publications, and coordinate changes in committee status with the Office of the Administrative Assistant to the Secretary of the Army, Department of the Army Committee Management Office (AARP–ZA), 9301 Chapek Road, Building 1458, Fort Belvoir, VA 22060–5527. Further, if it is determined that an established "group" identified within this regulation later takes on the characteristics of a committee, as found in AR 15–1, then the proponent will follow all AR 15–1 requirements for establishing and continuing the group as a committee.

Distribution. This regulation is available in electronic media only and is intended for the Regular Army, the Army National Guard, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This publication supersedes AR 190-17, dated 3 September 2009 and AR 50-1, dated 28 July 2008.

Contents—Continued

Chapter 1
Introduction

1–1. Purpose
This regulation prescribes Army responsibilities and guidance for the implementation of DOD security standards for safeguarding biological select agents and toxins (BSAT), as defined in Part 73, Title 42, Code of Federal Regulations (42 CFR 73), in the custody, possession, or jurisdiction of the Army to safeguard BSAT against loss, theft diversion, or unauthorized use or access within the United States. This regulation does not abrogate or abridge the authority or responsibility of a commander to apply more stringent security measures during emergencies. The federal regulations above, exempt clinical and diagnostic laboratories presented with specimens for diagnosis or verification, provided that specified actions are taken. These laboratories are exempt from this regulation. This regulation does not apply to other biological agents and toxins or to recovered biological warfare materiel.

1–2. References and forms
See appendix A.

1–3. Explanation of abbreviations and terms
See glossary.

1–4. Responsibilities
a. The Chief Information Officer/G–6 will provide assistance to Army BSAT entities in implementing information assurance guidance in accordance with DODI 8500.01, DODI 8510.01, DODI 8530.01, and AR 380–5.

b. The Inspector General will–

(1) Implement the Joint DOD BSAT inspection guidance in accordance with Army Directive 2016–24.

(2) Provide a copy of the final BSAT inspection report to Office of the Provost Marshal General (OPMG). Other distribution will be based on executive agent-responsible official (RO) and Department of the Army Inspector General (DAIG) policies.

c. The Deputy Chief of Staff, G–1 will—

(1) Establish personnel policies to support implementation of the Army BSAT Security Program.

(2) Provide guidance and procedures for the review of personnel files during initial certification of individuals into the BSAT Personnel Reliability Program (BPRP).

(3) Oversee and coordinate on personnel policies to support implementation of the BSAT Security Program.

d. The Deputy Chief of Staff, G–2 will evaluate and maintain current information concerning hostile intelligence and terrorist threats to the security of BSAT and disseminate the information to the responsible commander or director and law enforcement officials, as appropriate.

e. The Surgeon General will–

(1) Provide subject matter experts to provide technical advice on safeguarding Army laboratories.

(2) Oversee the medical aspects of the BPRP for HQDA. This includes establishing guidance for individuals performing BPRP duties regarding what medical information must be reported to the competent medical authority (CMA), guidance to the CMA describing what medical information should be considered potentially disqualifying for the BPRP, and the required medical documentation in the health record, with respect to medical assessment and information communicated to certifying officials (COs).

(3) Advocate for medical specific resources required to safeguard Army laboratories.

(4) Provide oversight of the inspection regimes to synchronize DOD and Interagency inspection activities for DOD BSAT safety and security as the designated EA RO for the DOD BSAT Biosafety Program per Army Directive 2016–24 and Deputy Secretary of Defense memorandum on "Designation of the Department of Defense Executive Agent for Biological Select Agents and Toxins Biosecurity Program," 3 January 2017.

f. The Provost Marshal General will–

(1) Function as the Army Staff focal point for the Army BSAT Security Program.

(2) Implement the provisions of DODI 5210.88 and the select agent regulation (SAR) and provide guidance to administer the Army BSAT Security Program.

(3) Prepare implementing instructions to the Defense Intelligence Study, Threats to DOD BSAT.

g. Director of Army Safety/Commander, Army Combat Readiness Center will ensure biosafety is synchronized with biosecurity requirements.

h. Commanders of Army commands (ACOMs) and/or direct reporting units (DRUs) responsible for Army BSAT entities will—

(1) Establish and maintain a command BSAT security program consistent with this regulation.

(2) Designate a physical security officer in accordance with AR 190–13 as the focal point for the BSAT physical security program.

(3) Designate personnel in accordance with AR 25–2, DODI 8500.01, DODI 8510.01, and DODI 8530.01 responsible for the cybersecurity of information technology (IT), platform IT, and control systems supporting the command BSAT security program.

(4) Provide command oversight, direction, guidance, and assistance as necessary to ensure compliance with the provisions of this regulation.

(5) Plan, program, budget, and allocate for the implementation of physical security requirements in this regulation.

(6) Ensure current intelligence threat information is provided to Army BSAT entity commanders/directors, to include implementation guidance for the DA Implementing Instructions to the Defense Intelligence Studies.

(7) Provide staff assistance visits when requested by the Army BSAT entity.

(8) Review Army BSAT entity plans for the recovery of lost, seized, or stolen BSAT.

i. Commanding General, U.S. Army Criminal Investigation Command will–

(1) Maintain current, evaluated information concerning the criminal threat to the security of BSAT and disseminate the information to the responsible commander or director and law enforcement officials, as appropriate.

(2) Conduct preliminary investigations into losses (to include inventory shortages) or recovery of BSAT, regardless of dollar value to determine if criminality occurred, and, as applicable, coordinate with the Federal Bureau of Investigation (FBI) and the Army BSAT entity commander/director.

(3) Investigate actual or attempted break-ins or armed robberies of Army BSAT entities and theft of BSAT, to include in-transit moves.

(4) Monitor investigations conducted by Army Civilian law enforcement agencies when such incidents involve BSAT-owned by the Army.

(5) Assist the responsible commander or director with evaluating existing security measures and recommend corrective actions to improve the security of BSAT using the results of completed investigations, crime prevention surveys, or provost marshal physical security inspections.

j. Commanding General, U.S. Army Installation Management Command will—

(1) Oversee garrison support to Army BSAT entity commanders or directors.

(2) Provide assistance in resolving security matters as required.

k. Garrison commanders hosting tenant Army BSAT entities will–

(1) Ensure tenant Army BSAT entity physical security plans are integrated with installation all-hazard planning, as appropriate.

(2) Support tenant Army BSAT entities by providing the necessary local threat assessments, integration and exercising security plans, armed response, common levels of support, and make notifications per serious incident reporting procedures.

l. Commanders and directors of Army BSAT entities will—

(1) Comply with this regulation.

(2) Ensure positive measures are taken for the complete control of BSAT during all life cycle phases.

(3) Develop, implement, and publish plans for the recovery of seized, stolen, or lost BSAT.

(4) Report the below listed events as serious incidents to garrison law enforcement, per AR 190–45—

(a) Theft, loss, recovery, suspected theft, inventory shortage/overage, wrongful disposition, and unauthorized use and/or destruction of Army BSAT.

(b) Attempts to steal or divert Army BSAT outside of physical security controls.

(c) Actual or attempted unauthorized access at an Army BSAT entity.

(d) Significant or disabling damage to an Army BSAT entity.

(e) Discharge of BSAT external to primary containment and into the ambient air or environment.

(f) Mishaps in which there was direct evidence of an exposure to Army BSAT, such as a measurable rise in specific antibody titer to the etiologic agent in question, or a confirmed diagnosis of intoxication or disease.

(g) Other Army BSAT incidents not identified above that the commander determines to be of immediate concern to HQDA based upon the nature, gravity, and potential for adverse publicity or potential consequences of the incident.

(5) Conduct prompt investigation per AR 15–6 of losses or recovery of BSAT after a decision by the U.S. Army Criminal Investigation Command (USACIDC) that criminal acts were not involved.

(6) Conduct a formal RA per chapter 3 and appendix C.

(7) Prepare a security plan per chapter 3 and appendix B.

1–5. Records management requirements
As decreed by AR 25–400–2, the records management (recordkeeping) requirements for all record numbers, associated forms, and reports are included in the Army's Records Retention Schedule-Army (RRS–A). Detailed information for all related record numbers, forms, and reports associated with AR 25–30 are located in RRS–A at https://www.arims.army.mil. (See records management requirements in para 2–12.)

Chapter 2
Waivers and Exceptions

2–1. Waiver requests
Requests for waivers and exceptions from this regulation will be forwarded through the ACOM and/or DRU to OPMG per paragraph B–7. If the waiver or exception requested will cause exceedance of the requirements in DODI 5210.88, OPMG will forward the requests to reach the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (ASD (NCB)) within 30 days of submission by the ACOM and/or DRU. 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. Requirements in this regulation will not be considered for waiver or exception if they are generated from a statute, regulation, or policy of a higher authority, or are imposed by another federal agency or are simply not authorized for waiver or exception.

2–2. Temporary relief waiver
A waiver may be approved for temporary relief from a specific requirement prescribed in this regulation 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.

2–3. Permanent relief waiver
An exception may be approved for permanent relief from a specific requirement as prescribed in this regulation when there are unique circumstances at the Army BSAT entity that make conforming to the requirement impractical or an inappropriate use of resources.

2–4. Amendment or cancellation waiver request
Whenever conditions or compensatory measures change, a request for an amendment to or cancellation of the waiver or exception will be sent by the ACOM and/or DRU to OPMG; OPMG will forward to the ASD (NCB).

2–5. Waiver review
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.

2–6. Reference
See paragraph B–13 for assessing and requesting waivers or exceptions.

Chapter 3
Security Standards

3–1. General
This chapter details the security standards necessary to reduce the risk of compromising Army BSAT entity 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 DODI 5200.08, DODM 6055.18, and DOD 5200.08–R, and the security standards in this chapter.

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 select agent regulations (SARs) and as described in chapter 6 and appendix B of this regulation.

c. Security planning and execution will be in accordance with DOD Instruction 5200.08, as applicable, and based on the standards identified in this regulation and a specific risk analysis of the Army BSAT entity. An appropriate risk management process will be used consistent with that prescribed in DOD Instruction 2000.16 to assess the threat and vulnerabilities and provide RO and Army BSAT commander or director with courses of action to mitigate the vulnerabilities or accept the risk. DA Form 7708 (Risk Analysis Process for Biological/Chemical RDT&R Facilities - Worksheet) will be used to conduct risk assessments (see app C).

3–2. 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 chapter 4.

a. Only individuals who successfully complete a security risk assessment (SRA) and obtain approval from the Federal Select Agent Program (FSAP) are authorized access to BSAT.

b. In addition, individuals 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 chapter 5.

3–3. Physical security systems

a. The Army BSAT entity commander or director or RO 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 Army BSAT entities will develop a physical security plan to ensure vulnerabilities are mitigated or the risk accepted in accordance with the SAR and DODI 5200.08 and DOD 5200.08–R, 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 Army BSAT 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 Army BSAT entity is a tenant on a military installation, the physical security plan for BSAT will be integrated into the host installation plan. The Army BSAT entity commander or director will identify any off-installation support requirements to the garrison commander who will incorporate those requirements into any installation agreements coordinated with off-installation agencies.

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

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

(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 in procedures for securing BSAT-registered spaces, safeguarding keys and combinations, changing access combinations or locks following staff changes, reporting and removing unauthorized individuals, access control and records requirements, inventory controls, and other 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 Army BSAT 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 (for example, natural disasters, fires, power outages, and general emergencies in Army BSAT entities).

(6) Army 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 Army BSAT entity's security program.

(b) Procedures for management of access controls (for example, keys, card-keys, common access cards (CACs), 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 Army BSAT 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 (for example, erroneous alarm).

(f) Procedures for visitor screening.

(g) Procedures for documenting security awareness training for all employees listed on the Army BSAT entity's approved registration including regular insider threat awareness briefings pursuant to DODD 5205.16, 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 Army BSAT entity to share relevant information with the RO to coordinate their efforts pursuant to Section 11(f)(2), Part 73, Title 42, Code of Federal Regulations (CFR) or equivalent section of Part 331, Title 7, CFR or Part 121, Title 9, CFR. The Army BSAT 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 change that effects security, or in response to a threat.

3–4. 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 DODI 5200.08 and DODD 5210.56, garrison commanders will issue the necessary regulations for the protection and security of property or places under their command.

b. The RO, Army BSAT entity commander or director, and the garrison commander will determine the required response time for the security forces (from notification, to arrival at the Army BSAT entity) based on the threat and RA, 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 realistic site defense force training exercises annually and in accordance with (42 CFR Part 73). The training will be tailored to each Army BSAT entity based on the threat and RA conducted at the site.

3–5. Security measures

a. Security barriers. 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 (for example, perimeter fences, walls, locked doors, or security windows) or trained personnel (for example, security guards, laboratory personnel, or escorts).

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

(2) Army BSAT 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 Part 73, Title 42, CFR, they must be dedicated to that task. These physical barriers must be identified on the Army BSAT entity's registration and discussed in the security plan (Sections 5A and 6A of Animal and Plant Health Inspection Service/Center for Decease Control (APHIS/CDC) Form 1 (Application for Registration for Possession, Use, and Transfer of Select Agents and Toxins) that is available at 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.* Army BSAT entities will determine perimeter lighting needs based on threat and RAs.

(2) *Intrusion Detection System.* 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 Army BSAT entity may consider using IDS based on a threat and RA.

(b) All areas that reasonably afford access to a Tier 1 BSAT-registered suite or room must be protected by an IDS unless the BSAT-registered space 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, Volume 3.

(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 RAs.

3–6. Access control

Access control measures ensure that only authorized individuals, as described in paragraph 3–2, 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), Part 73, Title 42, CFR or equivalent sections of Part 331, Title 7, CFR or Part 121, Title 9, CFR.

b. Each individual authorized access to BSAT will have a unique means of accessing the BSAT pursuant to section 11(d)(6) of Part 73 of Title 42, CFR or equivalent sections of Part 331, Title 7, CFR or Part 121, Title 9, CFR. Army 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 Army BSAT entity will update the access control logs when an individual's authorization for access changes.

d. Smart card technology will be implemented in accordance with DODI 8520.02.

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. Army BSAT 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 biosafety level (BSL) -3 or BSL–4 containment suites.

f. The Army BSAT 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 below. The AECS will authenticate the ID of an individual and verify the person's authority to enter the area through two separate methods of ID 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 Army BSAT entity and the individual to whom the card is issued. Implement DOD Instruction 8520.02, 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 randomly selected digits 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 used 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 and allow time for security forces to arrive. Protection will address covert or clandestine 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, and will be securely fastened to the wall or other permanent structure to prevent unauthorized access through breaching of attachment mechanisms (such as screws, pins, or 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.

3–7. Biological select agents and toxins 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.

3–8. Reporting incidents

Upon discovery of the theft, loss, release of, or exposure to BSAT, Army BSAT entities must report all incidents as specified in Chapter 6 of this regulation.

3–9. Inventory, accountability, and records

a. Each Army BSAT entity must maintain a current and accurate inventory. The DOD BSAT database will be used to inventory and account for all BSAT-registered with the FSAP at Army BSAT entities. BSAT must be clearly marked and labeled per SAR (42 CFR 73.17, 7 CFR 131.17, and 9 CFR 121.17), 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 Army BSAT entity will also document the names of all individuals who remove BSAT from long-term storage, date of removal, and disposition of BSAT (that is, destruction or return to long-term storage) pursuant to Section 17, Part 73, Title 42, CFR or equivalent sections of Part 331, Title 7, CFR or Part 121, Title 9, CFR.

c. Army components will review subordinate BSAT entities' facility information in the DOD BSAT database monthly, including facility name, address, and contact information; names of RO, alternate responsible official (ARO), and registering certificate number and expiration date.

3–10. Information and information security systems security

a. Data will be processed on systems assessed and authorized in accordance with DODI 8510.01. Platform IT and control systems as defined in DODI 8530.01 will be secured in accordance with DODI 8510.01 and applicable Army guidance.

b. Websites will be administered in accordance with DODI 8550.01.

c. Systems that use transmission lines to carry BSAT access authorizations, personal ID data, or verification data between devices or equipment located outside of the BSAT-registered space will comply with DOD requirements as described in DOD Manual 5200.01, Volume 3 to restrict unauthorized access and tampering.

d. Any classified or controlled unclassified information will be handled and protected in accordance with DOD Manual 5200.01, Volumes 3 and 4. Applicable program security classification guides will be developed for use when discussing or processing information related to BSAT. DD Form 254 (DOD Contract Security Classification Specification) must include applicable classification guidance.

e. Public release of information will be in accordance with DODD 5230.09, DODI 5230.29, and DODD 5122.05.

f. The SAR requires registered BSAT entities 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 Part 73 of Title 42, CFR or equivalent sections of Part 331, Title 7, CFR or Part 121, Title 9, CFR.

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 (for example, floor plans, on-site guard, closed-circuit television, IDS); security plans; and incident response plans.

h. Locations where authorization data and personal ID or verification data are created, stored, or recorded will be protected in accordance with information security standards in DOD Manual 5200.01, Volume 3.

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

3–11. Transportation and transfer of biological select agents and toxins

a. The transportation of BSAT will be in accordance with the SAR and Defense Transportation Regulation, Part II, Chapter 204 (Hazardous Materiel). BSAT will be shipped or transported following submission and approval of the APHIS/CDC Form 2 available at http://www.selectagents.gov, which will ensure the Army BSAT entity's use of carriers

that maintain anonymity during shipment. For Variola Virus, follow the FSAP instructions. Maintain transportation records and delivery receipts for at least 3 years.

b. Army BSAT entities may transfer DOD BSAT to other DOD and non-DOD BSAT entities that are registered with the FSAP for that specific BSAT and that will assume responsibility and accountability for the BSAT in accordance with federal regulations, including section 16 of Part 73 of Title 42, CFR or equivalent sections of Part 331, Title 7, CFR or Part 121, Title 9, CFR. Note that technology transfer and export control requirements for BSAT also apply (for example, DODI 2040.02; section 2778 of Title 22, United States Code; Title 50, United States Code, Chapter 35; Part 120–130, Title 22, Code of Federal Regulations; and Parts 730–774, Title 15, Code of Federal Regulations).

c. Army BSAT entities will not provide DOD BSAT to non-U.S. governmental overseas BSAT entities unless approved by the ASD (NCB). Requests will be submitted by the ACOM and/or DRU through EA–RO (with a copy to OPMG) and 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 RA for the BSAT being transferred. Approval will identify security measures and requirements for the recipients and comply with applicable national and international laws and regulations, as appropriate.

d. BSAT material movement. Army BSAT entities will develop procedures to move materials within or between BSAT laboratories or indoor storage.

Chapter 4
Biological Personnel Reliability Program

4–1. 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. The REV will monitor the BPRP and review and approve suitability actions in the paragraphs below. 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. The commander and/or director may designate a REV, as required.

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

d. The commander or director will designate a CO. 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 Army BSAT 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.

h. In Army overseas BSAT laboratories, 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 BSAT laboratory 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 Section 2778, Title 22, United States Code (22 USC 2778); 50 USC Chapter; Parts 120–130, Title 22, Code of Federal Regulations; and Parts 730–774, Title 15, Code of Federal Regulations.

4–2. Qualifying standards

All individuals' assigned duties requiring BPRP certification must meet and maintain 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 (for example, candor in self-reporting BPRP-relevant information).

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 the Adherence to Federal Laws Prohibiting Marijuana Use Director of National Intelligence Memorandum. Positions requiring BPRP certification will be designated for random testing per AR 600–85. Results of the drug or substance abuse test will be submitted to the CO.

e. Ability to obtain a current and favorably adjudicated personnel security investigation (PSI).

4–3. Biological Personnel Reliability Program 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 Diagnostic and Statistical Manual of Mental Disorders.

(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 in the 5 years before the initial BPRP interview (see glossary for definition). Isolated abuse of another individual's prescribed drugs is not a mandatory denial criterion; however, it must be evaluated as stated in paragraph 4–3*b* of this chapter.

(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 denial or termination criteria: however, it must be evaluated following paragraph 4–3*b*.

b. The criteria in paragraphs 4–3*b*(1)-4-3b(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. 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 from the date of the initial BPRP interview 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 as defined in the current American Psychiatric Association Diagnostic and Statistical Manual of Mental Disorders.

(4) Abuse of drugs more than 5 years before the initial BPRP interview or isolated abuse of another person's prescribed drug within 15 years of the initial BPRP interview.

(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 listed below 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.

4–4. Initial certification

a. DA Form 3180–1 (Chemical and Biological Personnel Reliability Program Statement of Understanding) provides a statement of BPRP requirements, and a statement of the individual's understanding that failure to meet or comply with the requirements will result in loss of BPRP certification and may result in loss of job. See appendix E for instructions to complete the form.

(1) Hiring agencies will ensure that a job applicant completes and signs DA Form 3180–1 prior to being provided a firm offer of employment for an Army civilian position that requires BPRP certification. If the applicant refuses to sign the statement of understanding, the applicant will no longer be considered for the position.

(2) Certifying officials will ensure that any other individual (for example, military personnel, or on-site contractor personnel, or current employees) being considered for the Army BSAT entity's BPRP completes and signs the statement of understanding prior to, or at the beginning of, the initial BPRP interview. If the individual refuses to sign the statement of understanding, the individual will not be eligible for the position, and no further initial certification action will be taken.

b. The DA Form 3180–2 (Chemical and Biological Personnel Screening and Evaluation Record) will be used to document the steps taken for initial certification (See app E for instructions). The CO will ensure that initial screening for BPRP certification includes:

(1) *Initial Biological Personnel Reliability Program interview*. The CO will conduct a personal interview with each BPRP candidate. Individuals will be advised of their obligations to report any factors that could have an adverse impact

on performance, reliability, or security while performing BPRP duties, and that failure to report this information may result in denial of entry to the BPRP. The CO will solicit from, and as appropriate discuss with, the individual the qualifying standards in paragraph 4–2 and any relevant disqualifying information as described in paragraph 4–3 of this chapter. As appropriate, the information reviewed by the CO from the personnel security investigation will be discussed with the individual. 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.

(a) The CO may at any point in the initial certification process conduct additional interviews with the individual to clarify or resolve issues that arise during initial certification.

(b) The CO may determine that sufficient information has been developed at any point in the initial certification process to support a decision to deny certification.

(2) *Personnel security investigation.* As part of the required screening process, the CO will verify personnel security clearance eligibility (at the secret level or higher) and review the results of the investigation. A current and favorably adjudicated National Agency Check with Local Agency Checks and Credit Checks (NACLC) investigation or reinvestigation or greater is required for military or contract employees, or an Access National Agency Check with Credit Checks and Written Inquiries (ANACI) investigation or reinvestigation 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 DODD 5230.20, DODM 5200.02, and DODI 5200.02.

(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.

(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, and per U.S. Army Medical Command (MEDCOM) Personnel Reliability Program (PRP) medical guidance, 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 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 not disclose the personal circumstances that resulted in the trauma but is required to inform the CO of any specific medical/psychological BPRP-relevant medical factors that may potentially impact reliability. The CMA will not reveal 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.

(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 AR 600–85, DODI 1010.09, and DODI 1010.01.

(5) *Personnel record review.* The CO will review the individual's personnel records, when available. Any CO who 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 (specifically, any information that meets the criteria in paragraph 4–3, and any information that might affect security clearance eligibility).

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

c. If the CO determines that the individual will be certified into the BPRP, the CO will review the requirements for maintaining BPRP certification, and the individual will sign the DA Form 3180–2 affirming their responsibility to abide by these requirements. Once a determination regarding an individual's certification for access to Tier 1 BSAT is made, the CO will notify the RO.

d. 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. The denial of entry into the BPRP will be documented on the DA Form 3180–2, which will be forwarded for retention in the effected individual's personnel record.

e. The REV will periodically monitor the BPRP certification and denial actions of the CO. If the REV determines that the procedures have been unfairly, inconsistently, or incorrectly applied, the REV will overturn CO decisions and assess whether additional corrective actions are required.

4–5. Continuing evaluation

Individuals certified in the BPRP are observed on a frequent and consistent basis by peers, supervisors, and the CO to ensure their behavior and performance meet all of the requirements of the program.

a. Certifying official observation. COs will observe the behavior and performance of individuals certified in 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 per AR 600–85. Verified positive test results will be reported to the CO and will result in termination from the BPRP (for cause).

e. Personnel security investigations. Individuals will submit requests for periodic reinvestigations within 5 years of the previous completed investigation. An unfavorably-adjudicated reinvestigation that renders an individual ineligible for a security clearance will result in termination from the BPRP (for cause).

f. Medical. Per MEDCOM PRP medical guidance:

(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 relevant medical information to the CO. Health records will document medical information forwarded to the CO for consideration for medical restriction, or termination from the BPRP, and include annotation of how the information was transmitted 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 DODI 6495.02 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.

4–6. Removal from Biological Personnel Reliability Program duties

a. A CO may impose an administrative or medical restriction (see glossary) 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. The CO will notify the individual and the individual's supervisor in writing of the imposition and removal of the restriction. Restriction will not be used for conditions related to BPRP denial or termination criteria (see para 4–3).

b. When the CO receives information relative to the decertifying criteria in paragraph 4–3, or information that could affect the individual's security clearance eligibility, the CO will immediately suspend the individual from the BPRP (and notify the individual and the individual's supervisor of the suspension) pending CMA evaluation and CO decision based on the "whole person" concept. When suspended from the BPRP, 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 Defense Consolidated Adjudications Facility.

(1) 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.

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

(3) The CO will consult with the REV prior to making the decision to terminate the individual from the BPRP for cause or to reinstate an individual into the BPRP, to ensure 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 by the individual. The decision of the REV is final.

c. COs will ensure actions of denial or termination are recorded on DA Form 3180–2 and are forwarded for retention in the effected individual's personnel record and medical record, which is held by the CMA.

d. When an individual is no longer required to perform BPRP duties, the CO will administratively terminate the individual from the BPRP. The CO will note the administrative termination on the DA Form 3180–2, and retain the DA Form 3180–2 for three years, and dispose of the form per local procedures in the fourth year.

4–7. Recertification into the Biological Personnel Reliability Program

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

b. The CO will review the request as part of the initial certification process (see para 4–4). The REV must concur with the CO decision to approve the recertification request (and certify the individual into the BPRP) or to disapprove the recertification request; the REV decision is final.

c. A copy of the DA Form 3180–2 reflecting the recertification steps and the decision to approve or disapprove recertification will be forwarded for retention in the individual's personnel records. It will be maintained with the previous DA Form 3180–2 reflecting the initial denial or termination.

d. An individual denied or terminated for drug/substance abuse that occurred while the individual was in a PRP (see para 4–3*a*(4)) is ineligible for recertification unless an exception has been approved by OPMG.

4–8. Biological Personnel Reliability Program status report

ACOMs and/or DRUs will provide a BPRP status report to Office of the Surgeon General (OTSG) no later than 25 January each year using DA Form 3180–3 (Chemical and Biological Personnel Reliability Program (PRP) Status Report) (see app E for instructions to complete the form). OTSG will provide a consolidated BPRP status report to ASD (NCB) no later than 15 February.

Chapter 5
Visitors

5–1. General

All Army BSAT entities required to register pursuant to the SAR must develop procedures, based on their site-specific RA, 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 Army BSAT entity's security plan to include:

a. Section 11(d) (2), Part 73, Title 42, CFR or equivalent sections of Part 331, Title 7, CFR or Part 121, Title 9, CFR 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 Part 73 of Title 42, CFR or equivalent sections of Part 331, Title 7, CFR or Part 121, Title 9, CFR for Army BSAT entities possessing Tier 1 BSAT.

c. Section 15(a) (2) of Part 73 of Title 42, CFR or equivalent sections of Part 331, Title 7, CFR or Part 121, Title 9, CFR, for providing visitors with information and training on biosafety, security (including security awareness), and incident response.

d. Section 15(d), Part 73, Title 42, CFR or equivalent sections of Part 331, Title 7, CFR or Part 121, Title 9, CFR for RO requirement to ensure a record of the training provided to each escorted individual is maintained.

e. Visitor entry procedures that ensure medical clearance or enrollment in an Occupational Health Program, as prescribed by 42 CFR 73, 7 CFR 331, and 9 CFR 121, and the CDC's Occupational Health Program Guidance Document for Working with Tier 1 Select Agents and Toxins, current edition.

5–2. Escorted access

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 Army BSAT entity's registration, have an approved SRA, be medically cleared by the CMA or enrolled in a Tier 1 BSAT Occupational Health Program, and either be enrolled in the host Army BSAT entity's BPRP or have a BPRP suitability memorandum from the home BSAT entity.

Chapter 6
Biological Select Agents and Toxins Reports

6–1. General

a. An individual or Army BSAT 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. Follow-up information will be submitted as it becomes known, but no later than 24 hours after the initial notification.

c. Within 7 days, the Army BSAT entity must submit a complete APHIS/CDC Form 3 (Incident Notification and Reporting (Theft/Loss/Release) available at http://www.selectagents.gov, to the agency with which it is registered, the CDC or the APHIS.

d. The individual or Army BSAT entity will notify the appropriate Federal, State, or local law enforcement agencies of the theft, loss, or release of BSAT. Army 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. Army BSAT entities will report BSAT mishaps and incidents to the National Joint Operational Intelligence Center (NJOIC) (nonclassified telephone: 703–693–3834; classified telephone: 703–697–4800; non-classified internet protocol router network email: 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 through command channels to the Army Watch in accordance with AR 190–45. Report the following:

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

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

(3) Actual or attempted unauthorized access at an Army BSAT entity.

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

(5) Discharge of 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 BSAT.

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

(8) Other BSAT incidents not identified in paragraphs 6–1*e*(1) through 6–1*e*(7) of this chapter that the Army BSAT entity commander or director determines to be of immediate concern to Army or DOD based upon the nature, gravity, and potential for adverse publicity or potential consequences of the incident.

f. Incidents involving information systems, platform IT and control systems supporting the BSAT program will be reported in accordance with CJCSM 6510.01B.

6–2. Reports to the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense programs

a. OTSG will provide a BPRP status report annually in accordance with chapter 4, paragraph 4–8 of this regulation. 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 (CY).

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

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

b. EA–RO will provide a summary of DAIG/CDC/APHIS reports and inspections results that may lead to Army BSAT entity closure to ASD (NCB).

c. Army BSAT entities will maintain the following records for 3 years, and then handle the records in accordance with AR 25–400–2 in the fourth year:

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

(2) Inspection and exercise records and reports.

(3) Corrective action and improvements.

(4) Training records.

6–3. Inventory and accountability records

All inventory and accountability records and reports associated with this regulation will be maintained for 3 years and then handled according to AR 25–400–2 in the fourth year.

Appendix A

References

Section I

Required Publications

AR 15–6
Procedures for Investigating Officers and Boards of Officers (Cited in para 1–4*l*(5).)

AR 25–400–2
The Army Records Information Management System (ARIMS) (Cited in para 1–5.)

AR 190–13
The Army Physical Security Program (Cited in para 1–4*h*(2).)

AR 190–14
Carrying of Firearms and the Use of Force for Law Enforcement and Security Duties (Cited in para B–1*b*.)

AR 190–45
Law Enforcement Reporting (Cited in para 6–1*e*.)

AR 190–51
Security of Unclassified Army Property (Sensitive and Nonsensitive) (Cited in para B–1*b*.)

AR 380–5
Department of the Army Information Security Program (Cited in para 1–4*a*.)

AR 380–67
Personnel Security Program (Cited in para B–1*b*.)

AR 525–13
Antiterrorism (Cited in para B–1*b*.)

AR 600–85
The Army Substance Abuse Program (Cited in para 4–2*d*.)

DODD 5122.05
Assistant To The Secretary of Defense for Public Affairs (Cited in para 3–10*e*.)

DODD 5205.16
The DOD Insider Threat Program (Cited in para 3–3*b*(6)(*g*).*)*

DODD 5210.56
Arming and The Use of Force (Cited in para 3–4*a*.)

DODD 5230.09
Clearance of DOD Information for Public Release (Cited in para 3–10*e*.)

DODD 5230.20
Visits and Assignments of Foreign Nationals (Cited in para 4–1*g*.)

DODI 1010.01
Military Personnel Drug Abuse Testing Program (Cited in para 4–4*b*(4).)

DODI O–2000.16, Volume 1&2
DOD Antiterrorism (AT) Program Implementation (Cited in the terms section.)

DODI 2040.02
International Transfers of Technology, Articles, and Services (Cited in para 3–11*b*.)

DODI 5200.02
Personnel Security Program (Cited in para 4–1*g*.)

DODI 5200.08
Security of DOD Installations and Resources and the DOD Physical Security Review Board (Cited in para 3–1*a*.)

DODI 5230.29
Security and Policy Review of DOD Information for Public Release (Cited in para 3–10*e*.)

DODI 6495.02
Sexual Assault Prevention and Response (SAPR) Program Procedures (Cited in para 4–4*b*(3)(*b*).*)*

DODI 8520.02
Public Key Infrastructure (PKI) and Public Key (PK) Enabling (Cited in para 3–6*d*.)

DODM 5200.01, Volume 3
DOD Information Security Program (Cited in para 3–5*b*(2)(*b*).)

DODM 6055.18
Safety Standards for Microbiological and Biomedical Laboratories (Cited in para 3–1*a*.)

Section II

Related Publications

A related publication is source of additional information. The user does not have to read it to understand this publication.

AR 11–2
Managers' Internal Control Program

AR 15–1
Department of the Army Federal Advisory Committee Management Program

AR 25–1
Army Information Technology

AR 25–2
Information Assurance

AR 25–30
The Publishing Program

AR 37–49
Budgeting, Funding, and Reimbursement for Base Operations Support of Army Activities

AR 190–30
Military Policy Investigation

AR 190–56
The Army Civilian Police and Security Guard Program

AR 380–86
Classification of Former Chemical Warfare, Chemical and Biological Defense, and Nuclear, Biological Chemical Contamination Survivability Information

AR 525–2
The Army Protection Program

AR 525–17
Special Mission Badges and Credentials

AR 600–8–14
Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel

CJCSM 6510.01B
Cyber Incident Handling Program
(http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf)

DA Pam 25–1–1
Army Information Technology Implementation Instructions

DODI 5210.88
Security Standards for Safeguarding Biological Select Agents and Toxins (BSAT)

DODI 8500.01
Cyber Security

DODI 8510.01
Risk Management Framework (RMF) for DOD Information Technology (IT)

DODI 8530.01
Cybersecurity Activities Support to DOD Information Network Operations (Available at http://www.dtic.mil/whs/directives/corres/pdf/853001p.pdf.)

DODI 8550.01
DOD Internet Services and Internet-based Capabilities

PL 107–188
Public Health Security and Bioterrorism Preparedness and Response Act of 2002

7 CFR
Agriculture

9 CFR
Animals and Animal Products

15 CFR
Commerce and Foreign Trade

22 CFR
Foreign Relations

40 CFR
Protection of Environment

42 CFR
Public Health

50 USC 797
Penalty for violation of security regulations

Section III

Prescribed Forms

Unless otherwise indicated, DA Forms are available on the Army Publishing Directorate website https://armypubs.army.mil.

DA Form 7778
Risk Analysis Procedure for Biological/Chemical RDT&E Facilities – Worksheet (Prescribed in para C–1*c*.)
.

Section IV

Referenced Forms

Unless otherwise indicated, DA Forms are available on the Army Publishing Directorate website https://armypubs.army.mil; DD Forms are available on the Office of the Secretary of Defense (OSD) website at http://www.esd.whs.mil/directives/forms.

APHIS/CDC Form 1
Application for Registration for Possession, Use, and Transfer of Select Agents and Toxins (Available at http://www.selectagents.gov.)

APHIS/CDC Form 2
Request to Transfer Select Agents and Toxins (Available at http://www.selectagents.gov.)

APHIS/CDC Form 3
Incident Notification and Reporting (Theft/Loss/Release) (Available at http://www.selectagents.gov.)

DA Form 11–2
Internal Control Evaluation Certification

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 3180–1
Chemical and Biological Personnel Reliability Program Statement of Understanding

DA Form 3180–2
Chemical and Biological Personnel Screening and Evaluation Record

DA Form 3180–3
Chemical and Biological Personnel Reliability Program (PRP) Status Report

DD Form 254
DOD Contract Security Classification Specification

SF 701
Activity Security Checklist

Appendix B

Security Planning, Standards, Measures, and Procedures

B–1. General

The characteristics of BSAT are inherently dangerous, potentially lethal, and are possible targets for theft, sabotage, or unauthorized use and warrant in-depth and balanced security measures to ensure proper safeguards against loss, theft, sabotage, diversion, unauthorized use, access, or other hostile acts.

a. The provisions of this regulation are intended to provide adequate security for BSAT.

b. The BSAT Security program will be integrated with Physical Security, AR 190–13 and AR 190–51, AR 190–14, AR 525–13, AR 380–5, and AR 380–67 and other referenced guidance in this regulation.

c. It is essential that oversight of the BSAT security program is maintained and associated inside and outside risks and vulnerabilities are continually assessed.

d. Army BSAT entity commanders/directors must carefully evaluate local or unique conditions that may dictate the need for additional provisions.

e. The following factors will be considered when assessing local security requirements for protection of BSAT--

(1) Threat assessment based on information furnished by intelligence, criminal investigative, or law enforcement agencies.

(2) Location, size, and risk of the Army BSAT entity.

(3) Vulnerability of BSAT to theft and loss.

(4) Geographic location within the installation and relative to surrounding population centers.

(5) Availability and responsiveness of security forces and/or local law enforcement.

(6) Availability of improved or advanced physical security systems or equipment.

B–2. Security planning factors

The Army BSAT entity security system will—

a. Prevent innocent or inadvertent access or trespassing.

b. Assure a capability for positive detection, ID, interception, and prevention of unauthorized access. The security system will be designed to ensure the security force is capable of early detection and apprehension of intruders.

c. Provide positive entry controls into BSAT facilities, laboratories, and storage areas.

d. Facilitate expeditious entry of fire department, explosive ordnance disposal, security, and/or response personnel.

B–3. Security plan review and updates

The Army BSAT entity security plan will—

a. Be reviewed annually and updated as necessary and approved by the Army BSAT entity commander or director or RO.

b. Be reviewed and updated, as necessary after any drills or exercises, after any incident, or changes in the Army BSAT entity's facility configuration or operating procedures.

c. Be reviewed and reapproved within 90 days of any Army BSAT entity commander or director or RO change.

B–4. Security plan outline

a. Army BSAT entities will develop a security plan in accordance with 7 CFR 331.11, 9 CFR 121.11, or 42 CFR 73.11 and Security Guidance for Select Agent or Toxin Facilities and Select Agents and Toxins Security Plan Template. See http://www.selectagents.gov/guidance-securityfacility.html.

b. Security plan will include Army specific requirements in appendixes.

(1) *Threat analysis.* Consider local threat assessment based upon the host installation's evaluation of the threat from terrorism, espionage, sabotage, theft, and vandalism. Persons and organizations threatening or attempting any of these acts will be identified. The threat analysis will be updated at least yearly and more frequently if changing conditions warrant.

(2) *Vulnerabilities.* Review results of the Army BSAT entity RA. Identify structures, containers, buildings, and work areas that require protection. Consider their location, size, function, and contents even if they are only used occasionally.

(3) *Incident response.* Develop and publish guidance and conduct annual training, to include exercises for BSAT staff and security forces. Plans will include specific actions to be taken, procedures to follow, personnel required, security forces (coordination with local law enforcement (if applicable)) scenarios, tactics, weapons/use-of-force, and incident reporting protocols.

(4) *Facility protection/response priorities.* Identify protection/response priorities such as BSAT tier 1 laboratory/storage, BSAT laboratory/storage, and administrative areas.

(5) *Security forces.* The plan will identify the organization responsible for executing armed responses at Army BSAT entities. The size, composition, and response time of the security forces will be identified. The security forces will develop response plans in coordination with the supported Army BSAT entity to ensure acceptable levels of support.

(6) *Add information.* Standard operating procedures for Army BSAT entity access control personnel.

(7) *General.* Memorandum of agreement with local police, if applicable.

(8) *Access control.*

(a) Outline the procedures the Army BSAT entity has in place for management of access controls (for example, keys, card-keys, CACs, badge control requirements, access logs, biometrics, and other access control measures) for each of the security barriers the Army BSAT entity has in place.

(b) Procedures outlining Army BSAT entity personnel access controls (for example, assigned personnel, visitors cleared and un-cleared to include escort requirements, maintenance personnel, non-operational hours access requirements and emergency entrance procedures for fire, security, and medical personnel and duress response procedures).

(9) *Physical security equipment.*

(a) Include descriptions of equipment and devices used to detect or delay intrusion.

(b) Type and construction of storage areas and containers. Walls, windows, openings, ceilings, and floors of such areas and containers. Provide estimated delay time for forced entry.

(c) IDS (If in place or required by this regulation), to include designation of personnel to manage the Army BSAT entity's IDS, including personnel with the IDS alarm code and criteria for changing it, procedures for testing the IDS and managing its configuration.

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

(10) *Material control.* Outline the system the Army BSAT entity uses to control movement of packages and material in and out of the protected areas, including inspection and documentation required for the search of hand carried items and sealed packages and containers. To include classified documents or materials relevant to the Army BSAT entity or contract.

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

(12) *Exercises.* These will be conducted in accordance with AR 525–2.

(13) *Security.* These incident reporting procedures in accordance with paragraph 6–1*e* and AR 190–45.

B–5. Restricted area designation standards

a. Commanders of military installations and facilities have the authority to publish and enforce regulations for safeguarding personnel, facilities, and property. This authority is derived from 50 USC 797, and is implemented by DODI 5200.08 and DOD 5200.08–R.

b. The installation commander will designate BSAT facilities as restricted areas.

c. Signs or notices will be posted in conspicuous and appropriate places to identify a restricted area (except when such action would tend to advertise an otherwise concealed area or when in conflict with host nation agreements). Signs will be positioned so they do not provide concealment of an intruder or obstruct visual assessment.

d. Signs will read "This activity has been declared a restricted area by authority of the installation commander in accordance with the provisions of the directive issued by the Secretary of Defense pursuant to the provisions of Section 21, Internal Security Act of 1950. Unauthorized entry is prohibited. All persons and vehicles entering herein are liable to search. Photography of the facilities is prohibited without specific authorization from the commander. Deadly force is authorized."

e. Existing signs containing essentially the same wording as in U.S. Army Corps of Engineers (USACE) Drawing DEF 872–90–01 (Weapon Storage Area, Perimeter Warning Sign) may continue to be used until replacement is necessary, at which time the required wording in USACE Drawing DEF 872–90–01 will be used.

B–6. Biological select agents and toxins facility room and laboratory construction standards

a. Walls, floors, and ceilings will be constructed of at least ½-inch plywood, 1-inch tongue-in-groove wall board or equivalent. Roofs with suspended ceilings will be protected to ensure the crawl space cannot be used for covert entry.

b. Windows and openings such as conduits, vents, and ducts in excess of 96 square inches with a smallest dimension greater than 6 inches will be barred or grilled to ensure a degree of security comparable to that provided by the walls of the room or laboratory.

c. Doors will be constructed of solid-core wood or metal, possess the Underwriters Laboratory fire rating, and be designed to complement the security provided by the exterior wall of such room or laboratory. Hinges should be mounted

inside the room or laboratory. If this is not practical, hinges mounted outside rooms or laboratories will be welded, peened, or brazed to preclude removal from outside the door. Doors not used for primary entrance will be secured from the inside at all times and devoid of external locking hardware. Such doors will be equipped with hardware to permit rapid exit from the room or laboratory in the event of fire or other emergency.

B–7. System certification standards

a. A physical security system may use shared networks in lieu of point-to-point closed communication transmission media, if most practical.

b. Every reasonable effort will be made to physically and logically separate a physical security system on a shared network from other devices and systems to best ensure continuous reliability.

c. Physical security systems must be authorized to operate per the DOD Risk Management Framework. This requirement applies to all systems whether local area network-based, stand-alone, or closed restricted.

d. All IT-based systems must be registered with the Army Portfolio Management Solution (APMS). System owners should consult with the command chief information officer. See AR 25–1 and DA Pam 25–1–1 for more information. APMS is available at https://www.eprobe.army.mil/enterprise-portal/web/apms/home.

B–8. Intrusion detection system standards

a. Intrusion detection system sensors are required for Tier 1 BSAT rooms or laboratories or when determined by the site RA and approved by exception according to this regulation.

b. DOD standardized IDS or ACOM-approved commercial IDS to detect unauthorized entry. The use of commercial off-the-shelf IDS is authorized.

c. The IDS sensors will be installed inside the protected area.

d. Rooms or laboratories will be equipped with a volumetric or motion detection sensor system capable of detecting entry and movement of an intruder within the protected area. Doors to rooms or laboratories having living animals present will not be required to have a volumetric or motion detection sensor, only a balanced magnetic switch on the doors.

e. Doors to BSAT rooms or labs will have a balanced magnetic switch.

f. The IDS control units will be placed inside the room/laboratory. If the control unit cannot be placed inside the protected area, the control unit will be secured inside a locked, tamper-alarmed container on the outside of the protected area in close proximity to the entrance.

g. All IDS will terminate at a manned location with the capabilities to initiate an immediate response by security force personnel as specified in the site Physical Security Plan. Alarm activation will be displayed at the alarm center. Audio and visual indication will show line supervision and access/secure status.

h. The IDS will be in secure mode (ready to respond to an intrusion) at all times when the room or laboratory is unoccupied.

i. Appropriate security measures will be taken when IDS is not operable. The security measures will be established in the site PSP.

j. All IDS will be provided with an uninterruptable power supply (UPS) independent of the primary power supply. The UPS will be capable of operating IDS for a minimum of 4 hours.

k. The IDS UPS will be kept under surveillance or contained in an alarmed cabinet to protect the system against tampering. The UPS will be tested quarterly or more often as recommended by the alarm manufacturer.

l. Procedures will be established in the site PSP to provide immediate security forces to alarms. Alarms will be recorded and retained on file for one year. Records will include the nature of the alarm, the date and time the alarm was received, the location, and action taken in response to the alarm. Records will be reviewed by supervisor personnel to ensure proper actions were taken, and identify and correct IDS reliability problems.

m. All IDS sensors will be tested by causing an actual alarm at least quarterly, or more often, as recommended by the alarm manufacture. Such alarm activation will include opening doors and deliberate movement within the room or laboratory. Test procedures will simulate expected actions of a potential intruder. Testing will be accomplished by security personnel, IDS maintenance or laboratory personnel under the supervision and in the presence of security personnel. The closed-circuit television (CCTV) viewing may be used for this purpose. Detailed test procedures will be developed and will include sensitivity and performance standards for each sensor. Where advanced sensor systems that provide the capability to remotely stimulate individual sensors via an electronically activate sensor phenomenology device are installed, the capability may be used to fulfill the quarterly testing requirement.

n. Security personnel or IDS/laboratory personnel under the supervision of security personnel will conduct an actual test of effected IDS components immediately following maintenance, repair, or modification.

o. A record of all tests of IDS sensors and UPS will be maintained for 12 months. The record will reflect the date of the test, the name of the person(s) conducting the test, results of the test, and any required corrective action resulting from the test. All IDS and UPS tests will be recorded in the guard log.

B–9. Security Identification badge standards

Security ID cards and badges provide a visual means to determine if the bearer is authorized to be in a certain restricted area(s). The intent of using security ID cards and badges is to combine their use with physical protective measures and other security procedural measures to increase safeguards to Army assets against espionage, sabotage, damage, destruction, and theft by controlling personnel movement in restricted areas. See AR 190–13.

B–10. U.S. Army Security Management System-Counter Measure standards

This measure will be used by all Army physical security personnel and planners to standardize procedures used to conduct physical security inspections, surveys, and the conduct of planning and programming. See AR 190–13.

B–11. Key control standards key

This key and lock control requirements in AR 190–51 apply. Keys to installed locks on BSAT storage rooms, laboratories, and containers will be strictly controlled at all times and will not be removed from the facility. These keys will be maintained separately from other keys and will be accessible only to those individuals whose official duties require access to them. Keys will not be left unattended or unsecured at any time. If risk analysis identifies additional key and lock procedures, those procedures will be identified in the physical security plan.

B–12. Entry control standards

a. Only authorized personnel will be permitted entry into rooms or laboratories where BSAT is being used or stored. Written control procedures will be established to validate the ID of all personnel requiring unescorted entry.

b. A Government-issued photographic ID card with sufficient ID data may be used to satisfy ID requirements. The following systems will be incorporated into the entry control program for BSAT rooms and laboratories—

(1) A security/proximity badge system, IDS, and mechanical locking systems.

(2) Visitor control system.

(3) A duress system.

c. Package and materiel control system.

d. Only personnel certified in the BPRP will be granted unescorted access to Tier 1 BSAT rooms or laboratories. Non-BPRP personnel must have a need for access and will be escorted at all times by BPRP-certified escort.

B–13. Waivers and exceptions

The purposes of waivers and exceptions are to—

a. Ensure that prescribed security requirements are properly implemented and observed.

b. Ensure that deviations from established security requirements are systematically and uniformly identified and approved by the proper level of command, so that appropriate compensatory measures are applied.

c. Provide a management tool to monitor corrective actions.

B–14. Limitations

The following limitations apply—

a. Waivers or exceptions will not be used to reduce or eliminate the minimum-security requirements in this regulation.

b. Each waiver or exception will be evaluated and approved on a case-by-case basis. Requests for waivers and exceptions that address identical requirements at more than one Army BSAT entity may be approved on a case-by-case basis.

c. Each exception will be reviewed during physical security inspections or when a major change in site configuration or mission offers the opportunity for corrective action and terminate the exception.

d. Notify the approving authority, through command channels, when the exception is no longer needed.

B–15. Compensatory measures

The following measures apply—

a. Commanders will ensure that prescribed compensatory measures are implemented as required.

b. Compensatory measures will be immediately applied when a deficiency/risk is identified and will remain in effect pending formal review and final approval by the approving authority in paragraph x-x below.

c. Compensatory measures will be instituted for each deficiency. In some cases, one compensatory measure may suffice for more than one deficiency. In some instances, there may not be a need for compensatory measures to deviate from

administrative standards. In these cases, the reasons why compensatory measures are not required will be clearly stated in the request.

d. Security measures will compensate for the specific risk created by the deficiency. A risk is presumed to have been created when a security standard in this regulation cannot be met. A security standard directed by this regulation cannot serve as a compensatory measure for a deficiency.

e. Compensatory measures may include additional security forces, procedures, and/or physical security devices such as additional locks, alarms, lighting, camera surveillance devices, and delay devices. The criteria for accepting compensatory measures will be designed to specifically enhance the security posture in light of the deficient situation.

f. Compensatory measures that consist primarily of instructions to the security force will be clear, specific, and thorough. Compensatory measures that consist primarily of instructions to the security force to increase their alertness does not provide a comparable level of security.

g. Security force response times will be assessed and documented considering the construction design of the facility, the estimated forced entry time against intruders and capabilities described in DOD and DA threat documents. The first defense layer against forced entry is the exterior of the building containing the BSAT. The second defense layer is the shell of the BSAT rooms or laboratories (walls, doors, floors, ceilings, and utility openings). The third defense layer is the BSAT container. Applied compensatory measures will preclude unauthorized access to BSAT prior to the arrival of the security force.

h. A 10-percent deviation from all measurable standards, such as clear zone distances, fence height, and so forth, is permitted. Therefore, such deviation does not require the submission and approval of a waiver or exception request. Compensatory measures will be required when two or more 10-percent deviations, taken together, are determined to constitute a risk in the site security system. For example, a fence that is a few inches below the required height does not by itself constitute a risk. No compensatory measures are necessary. However, if there are additional 10-percent deviations at the Army BSAT entity, such as fence and perimeter lighting, that taken together, are determined to create a risk, then compensatory measures are required. Ten-percent deviations will be documented in the site security plan. Where appropriate, required compensatory measures for 10-percent deviations will be approved by the local commander.

i. Security forces will be made aware of all waivers and/or exceptions and compensatory measures currently in effect.

j. Compensatory measures, when considered in total, must not unrealistically task security forces.

B–16. Waiver or exception requests

a. Procedures to obtain approval. Requests for waivers or exceptions should be initiated by the commander/director of the Army BSAT entity involved and forwarded in writing to the Office of the Provost Marshal General (OPMG) Physical Security Branch (DAPM–MPO–PS), 2800 Army Pentagon, Washington, DC 20310–2800.

b. All waiver or exception requests will include the following information:

(1) For example, Request for Waiver at Edgewood Chemical and Biological Center.

(2) Outline the issue that constitute requirements below those cited in this regulation. Provide the following–

(a) Reasons for not meeting prescribed requirements or need to exceed requirements.

(b) Explain why the Army BSAT entity cannot comply or garrison commander cannot support the requirement or the reason why measures exceeding the requirements of this regulation is needed.

(c) Explain what action(s) are planned and scheduled. Provide specifics, to include anticipated timelines and completion date.

(d) For waiver requests, identify the projected duration of the waiver.

(3) Risks and vulnerabilities associated with the waiver or exception.

(4) Detailed information about compensatory measures, to include costs.

(5) Status of any other waivers or exceptions currently in place.

(6) Coordination with supporting installation agencies as well as the supporting engineer when structural requirements are involved.

(7) Endorsement of the waiver or exception by each level of chain of command.

(8) Legal opine by the supporting senior legal official.

(9) Classified information contained in requests for waivers and exceptions may require appropriate security classification according to criteria in AR 380–86 (for example, critical vulnerabilities).

c. Exceptions granted under the previous AR 190–17 will be reviewed and resubmitted or cancelled if no longer required.

B–17. Approval authority

a. The ASD (NCB) is the approval authority for waivers or exceptions for requirements that exceed the standards of this regulation.

b. The OPMG is the approval authority for waivers or exceptions for requirements that do not meet the standards of this regulation.

c. The Army BSAT entity commander is the approval authority for waivers to requirements that do not meet the standards of the regulation but can be corrected in 60 days or less. Compensatory measures will be identified and immediately applied. Approved waiver will be provided to OPMG. If the deficiency cannot be corrected in 60 days, submit a formal request for waiver to OPMG outlining the reason for delay.

Appendix C

Risk Assessment Procedure for Biological Research, Development, Test, and Evaluation Facilities

C–1. General

a. Commander and/or directors and RO will identify, analyze, and assess overall risk to BSAT entrusted to them and protect those agents from sabotage, damage, theft, and loss. This RA will assist in determining the type and level of protection required. The RA process will be performed by a team led by a 0080 job series employee. Assessment composition will include the RO, researcher/principal investigator assigned to the entity, facilities/engineer representative, personnel/human resources, CO (if applicable), biosafety representative, and the organizational representative responsible for armed response.

b. The purpose of this assessment is to identify, assess, and implement RA and vulnerability assessment requirements per DODI 5210.88. It assesses the threats and vulnerabilities and provides the facility commander/director with a tool to design and accomplish a robust physical security program based on available intelligence while promoting flexibility and interoperability for the use of physical security resources.

c. DA Form 7778 will be used to conduct risk assessments per the instructions of this enclosure.

C–2. Risk assessment conditions

A RA will be conducted—

a. When an entity or laboratory is activated.

b. When an entity or laboratory relocates to a new site or location.

c. When no record exists of a prior RA.

d. The entity will document the RA and review it at least yearly or as the threat changes.

e. During the planning stages of new facilities, and/or when significant additions/renovations to facilities indicate the need for further assessment as determined by the commander/director or RO.

f. When an incident occurs in which the safety or security of the facility and/or agent or toxin has been compromised.

g. Upon receipt of significant changes to risks based on threat statements, vulnerability assessments, or local conditions.

h. When significant changes or updates to the FSAP's list of agents or toxins provides a risk condition which may adversely affect the overall safety and security posture of the facility.

C–3. Risk assessment process

The facility assessment is a 5-step process, and is documented on the standard assessment/analysis worksheet. Based on the results of the RA, the facility commander/director will implement the physical security measures identified in paragraph C–4. There are various types of risk groups that will be used during this assessment. Characterizations of each group are located in the glossary and include:

a. Unsophisticated criminals.

b. Sophisticated criminals.

c. Violent extremist organizations.

d. Vandals and/or activists.

e. Lone wolf offenders.

f. Insider threats.

C–4. Risk levels

The following physical protective measures and security procedural measures will be implemented based upon the level identified on the risk level worksheet and requirements will be outlined in a physical security plan.

a. *Risk level I.*

(1) Access to rooms or suites will be limited to designated personnel whom possess and operational need and maintain a completed a favorably adjudicated PSI at the appropriate level.

(2) All individuals authorized access to BSAT-registered spaces must wear a visible ID badge.

(3) Visitors to the laboratory or suite will be clearly identified as escort-required or escort-not-required. Escort-required visitors will be escorted by personnel who are authorized unescorted access to that respective area. A visitor access log will be maintained and will include the visitor name, date, and time of entry and records will be maintained for 3 years. Records older than 90 days will be stored in a separate location for safekeeping. Under no circumstances will visitors be allowed to have "hands-on" or access to the agent material.

(4) The physical security plan will outline control procedures for cleaning and maintenance/repair personnel within a registered space. Controls will include use of only approved individuals for cleaning, maintenance and repair, and escorted access in accordance with paragraph C–4*a*(3). The responsible entity is to ensure that these persons have received proper vetting.

(5) The security plan and/or procedures will include a prohibition for the sharing of unique means of access (such as keys, key cards, passwords, and/or combinations) with any other person.

(6) Registered space entry processes will prohibit and prevent "piggybacking" or "tailgating" at entry points.

(7) One physical barrier is in place in BSAT-registered facilities to deter intrusion and deny access by unapproved personnel in the area containing BSAT. Examples of a primary barrier include having a key/combination locked container with sufficient key control measures, a different card-key required for room, a card-key personal identification number (PIN) access room, a biometric lock system on freezer, a PIN access to freezer, and a restricted card-key access to a registered space. During operational hours, personnel trained in access requirements may satisfy a barrier requirement. Training will include initial and annual refresher training. Electronic access control systems will fail secured in the event of power loss and procedures for access during loss of power will be outlined in the physical security plan until power is restored.

(8) Back up power sources will immediately trigger and operate once there is a loss of original power source.

(9) When not in use all BSAT will be stored in refrigerators, freezers, or other approved storage devices within secured BSAT-registered spaces.

(10) An end-of-day security check of BSAT-registered rooms and/or suites will be conducted after room use and recorded on a SF 701 (Activity Security Checklist). Completed 701's will be maintained for a period of 90 days.

(11) Key and lock procedures for access to rooms/suites and to keys, locks, and protective seals protecting assets will be controlled per AR 190–51. 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 measures will be included.

(12) All personnel will be current on initial and annual Tier 1 Threat Awareness and Reporting Program training.

(13) Armed security forces will be identified to respond within 15 minutes to unauthorized or actual or attempted penetrations and prevent removal of BSAT.

(14) Plans and/or procedures will include reporting and removing unauthorized or suspicious persons and will include a challenging process. The process will include an RO incident report to facility security and/or installations response personnel.

(15) The security plan will include reporting processes for the loss or compromise of keys and access cards and how they will be replaced and will include immediate actions to ensure there is no compromise to security including immediate notification to facility and security personnel, and a determination for changes to locking mechanisms or disablement/deactivation of/in the electronic card or system. The plan will also include theft or release of BSAT and indications of whether inventory or use records for BSAT have been altered or otherwise compromised.

(16) Procedures will address processes required for personnel no longer requiring access to BSAT including deactivation of card-key access, email, network, computers, and turn-in of key cards and badges and changes to installed combination locks remaining at the facility.

(17) The appropriate commander will designate a BSAT facility as a restricted area. Signage reflecting such should be conspicuously posted, as necessary.

(18) Information protection requirements will be included in the physical security plan or procedure.

(19) If used, procedures for management of closed-circuit television recording or surveillance will be developed.

(20) Either by inclusion or reference to an inventory procedure, the physical security plan will include the inventory control process that ensures strict accountability, records of access, and the use and final disposition of BSAT.

(21) Either by inclusion or reference to a procedure, safeguards, and destruction of BSAT during emergencies (for example, natural disasters, fires, power outages, and general emergencies) in entities containing BSAT.

b. Risk level II.

(1) Measures required for security level I will be implemented.

(2) An automated entry control system (AECS) will be used to control access to authenticate the ID of an individual and verify the person's authority to enter the BSAT-registered spaces. Retrievable records will be maintained for 3 years.

(3) Agent rooms with openings that exceed 96 square inches will be barred or grated to prevent forced entry. Moveable openings that can be secured from outside or inside (doors and pass through shoots) are exempt from this requirement provided they are attended by an assigned lab person while open or in use.

(4) A two-barrier system that includes the primary barrier requirements of Risk Level I and a secondary barrier, examples include building card, key access, card, and/or key access to the upper floor(s) for multi-level buildings, additional card, key, and/or PIN access rooms, and any other additional barrier meeting the requirements of risk level I.

(5) A determination will be made regarding the need for a security perimeter and/or high mast lighting and documented in the physical security plan.

c. Risk level III.

(1) Measures required for risk levels I and II will be implemented.

(2) Delineation of the roles and responsibilities for security management, including designation of a security officer to manage the entity's security program and intrusion detection system (IDS) will be outlined in the security plan. Management of IDS will also include alarm code management and use (including failures/false alarms), testing, and configuration management.

(3) Tier 1 facility visitor escorts will be enrolled in the BPRP program.

(4) A three-barrier system counted from the BSAT outward will be implemented. All access and emergency exit points must be secured. Emergency exits may have installed interior panic hardware and will be devoid of exterior hardware with a pick plate to inhibit opening. At least one barrier must be monitored in a way to detect circumvention of established control measures under all conditions. Monitoring may include video cameras, monitoring access control logs from a card-key reader, or tamper-evident tape on containers used for long-term storage.

(5) Registered suites or rooms will be protected by IDS unless physically occupied. The RO, safety and security professionals will meet formally at least annually or on a regularly defined basis, following a security incident/response to a threat, and when significant changes occur. When significant changes occur, it should be determined if an update to the RA is required in accordance with paragraph D–2 above. Further, security impacts related to safety procedures, hiring policies, inventory processes, and after-hours work policies will be reviewed to determine if adjustments are required.

(6) Annually a performance assessment will be conducted. The assessment may be conducted during risk analysis and during review of physical security plan updates. Performance requirements of the security system(s) will be defined, and the assessment will determine whether or not improvements are required. The assessment should ensure processes and procedures deter, detect, delay, and response to threats are adequate. Adequacy should be determined by acceptable levels of risk-based on threat statements, and sufficiency of time between detection of threats, the time period required for successful threat acts, and response time of responders.

(7) Exterior of buildings that contain registered spaces will be checked by security patrol(s) on an irregular basis not to exceed 8 hours. There is no requirement to enter a secured building to check individual rooms, but if the building is found unsecure, the building and more specifically the entry/exit thresholds to the laboratory spaces will be inspected. Results of this inspection will be documented and endorsed by the lead physical security specialist and the RO.

(8) IDS will be installed for registered space entry and/or exit doors.

(9) Threat awareness briefings will be conducted annually for assigned personnel and will include ID of suspicious person and reacting to suspicious packages; escort procedures; specific security policies including entry access procedures and tailgating, preventing the sharing of unique means of access, reporting the loss or compromise of passwords, how to identify and report suspicious persons or activities, inventory and records management; response to an alarms and breaches; and insider and outsider threats. Re-training is required when significant changes are made to processes or procedures. An employee verification of understanding processes must be implemented and may include a "read and understood".

d. Risk level IV. This risk level of protection is required when risks exceed the protection afforded up to and including risk level III and additional countermeasures are required to mitigate risks to an acceptable level as determined by the RA. The RA will document specific countermeasures required to achieve acceptable levels of risks and the team will determine if a waiver submission is required in accordance with this regulation.

Appendix D

Minimum Security Standards for Biological Select Agent and Toxins Outside the United States

D–1. General

a. This appendix applies only to biological research laboratories located outside the United States where MEDCOM commanders and/or directors have custody or possession of BSAT. If in custody or possession of Tier 1 BSAT, see requirements in chapter 3 of this regulation.

b. Where conflicts exist between the requirements of this appendix and other parts of this regulation, the requirements of this appendix have precedence.

c. Except as modified in this appendix, the remainder of this regulation applies to BSAT research laboratories located outside the United States.

d. Where requirements of this regulation cannot be met due to host nation requirements, a physical security waiver or exception will be submitted through command channels to OPMG.

D–2. Functions

Commanders and directors of Army BSAT laboratories located outside the United States will—

a. Establish and maintain a command BSAT security program consistent with this regulation.

b. Employ a qualified, school-trained physical security specialist (general schedule-0080 job series) to manage and oversee the BSAT physical security program.

c. Maintain close coordination with the American Embassy Regional Security Officer (RSO) in order to—

(1) Obtain and maintain current, evaluated information concerning the criminal and terrorist threat to the security of BSAT.

(2) Coordinate law enforcement, physical security, security forces, and investigative support from Embassy, FBI, or host nation resources.

D–3. Minimum security requirements

a. Army BSAT laboratory commanders/directors must consider local or unique conditions that may dictate the need for physical protection of BSAT beyond the minimum requirements of this regulation.

b. The IDS will terminate at a manned location with the capabilities to initiate an immediate response by security force personnel as specified in the site PSP. Host nation police, military personnel, or contract security forces may satisfy this requirement.

D–4. Physical security inspections

a. Army BSAT laboratory commanders and/or directors will ensure physical security inspections are conducted in accordance with AR 190–13 and MEDCOM guidance.

b. As a minimum, physical security inspections will be conducted upon activation of an Army BSAT laboratory and at least every 18 months thereafter.

D–5. Investigations

a. The recovery of BSAT that has been misplaced or is otherwise unaccounted for within an Army BSAT laboratory is an operational matter for which the commander and/or director has initial responsibility. The assistance of supporting law enforcement authorities may be sought at any time. If resolution is not achieved within 24 hours, law enforcement must be notified.

b. Once the commander and/or director determines that BSAT has been lost or stolen, recovery becomes an investigative function. The laboratory will provide scientific, operational, and laboratory support.

c. If a BSAT loss occurs and no law enforcement investigation is conducted, the Army BSAT laboratory commander and/or director will promptly request an AR 15–6 investigation through command channels.

D–6. Security forces and use-of-force

a. The Army BSAT laboratory commander/director will ensure sufficient armed security forces are on hand to fulfill the security requirements of this regulation unless prohibited by host nation laws, treaties, or agreements. If prohibited by host nation laws, treaties, or agreements, a physical security exception must be submitted.

b. Rules of engagement and use-of-force policies will be reviewed by the supporting staff judge advocate or legal counsel and the RSO to ensure they are consistent with applicable international treaties, agreements, host country laws, and so on.

D–7. Physical security planning

The Army BSAT laboratories located outside the United States require particularly thorough planning. Commanders and/or directors of these laboratories will—

a. Develop a BSAT physical security plan (PSP) following the guidance of chapter 3, and the format at appendix B.

b. Develop, implement, and publish a laboratory-specific plan for the recovery of seized, stolen, or lost BSAT. This plan will be based on the MEDCOM BSAT Recovery Plan, with special attention to restrictions inherent as the guest of a foreign government.

c. Coordinate the development of PSPs with their parent organization.

d. Identify and coordinate with the organization or agency that will provide security services support (guards, security forces, investigative support, law enforcement support). Generally, these types of support will not be available from those sources identified in paragraph 1–4 of this regulation.

(1) The PSP must identify the agency that will provide investigative support. The USACIDC investigative support will probably not be available locally. Nevertheless, Army BSAT laboratory commanders/directors should formally communicate with the USACIDC element that provides geographic support to the Army Service Component Command, (for example, U.S. Army Europe; U.S. Army Pacific). The MEDCOM Provost Marshal is available to assist with identifying the appropriate investigative agency.

(2) The PSP must be coordinated with the organizations responsible for providing guards, law enforcement support, and security forces. Since these organizations are generally not located on Army installations, garrison commanders are not available to provide these support requirements. Forward final PSPs through command channels to MEDCOM Provost Marshal.

D–8. Threat considerations

a. Army BSAT laboratory commanders and/or directors will develop BSAT threat assessments based on local, regional, environmental, and situational considerations. Commanders and/or directors will request input from local law enforcement and intelligence communities, either directly or through the American Embassy Regional Security Office (RSO).

b. The DA Implementing Instructions to the DOD postulated threats to BSAT will be considered when developing laboratory-specific threat assessments.

c. Commanders/directors will request appropriate assistance through command channels when threat assessments cannot be accomplished with resources available locally.

D–9. Risk assessment threat considerations

The laboratory-specific threat assessment will be used as the threat basis for conducting RAs at Army BSAT laboratories outside the United States (see para D–8 and app C).

D–10. Risk assessment team requirements

a. In addition to the RA team, representation from the American Embassy RSO will be requested to assist with RAs, updates, and annual reviews. If a U.S. Army intelligence representative is not reasonably available, the RSO may serve in that role.

b. In lieu of an "installation security forces representative," the RA team will include a representative from the organization responsible for providing the security forces. If this is not practicable due to security considerations, the reasons will be documented.

D–11. Restricted area signs

a. The supporting staff judge advocate or legal counsel will be consulted prior to posting restricted area signs. This is to ensure they are consistent with applicable international treaties, agreements, host country laws, and so on.

b. When restricted area signs are posted, they will be in the language of the host country in addition to English.

D–12. Key and lock control

a. At some locations outside the United States, Army researchers are guests in laboratories owned and operated by the host nation. In some instances, the host nation may control keys, operate, and respond to IDS, and provide security forces. The Army researchers will make every effort to retain control of locks and keys securing Army-owned or DOD-owned BSAT.

b. Where key control responsibility is retained by the host nation, efforts must be made to include the policies of this regulation in the applicable agreement (treaty, memorandum of understanding, memorandum of agreement, and so on).

D–13. Security forces

a. The Army BSAT laboratory commanders/directors will establish a security force or arrange for security support applicable to their situation to perform the physical security requirements outlined in this regulation, the laboratory PSP, and applicable regulations.

b. If the Army provides security forces, to include contract guards, the requirements of chapters 5 and 6 apply.

c. If the host nation provides security forces, every effort will be made to include the policies of this regulation in the applicable agreement (treaty, memorandum of understanding, memorandum of agreement, and so on).

d. Written guard orders for posts and patrols must be translated into the host nation language for any indigenous guard force.

D–14. Response force

a. The Army BSAT laboratory commanders/directors will ensure response force details are contained in the support agreement with the organization providing the support.

b. Consideration should be given to utilize the American Embassy Special Reaction Team as the response force.

c. The composition, number, arming, and response time of the response force will be determined based on the VA and the PSP and coordinated with response force provider.

D–15. Movement of biological select agents and toxins

The Army BSAT laboratory commanders/directors will develop SOPs for—

a. Movement of BSAT outside the laboratory. Include procedures for—

(1) Transporting BSAT within the host country.

(2) International shipment of BSAT (follow appropriate Army guidance).

b. Movement of BSAT within the laboratory (for example, between laboratory rooms).

c. The SOPs will follow the policies of chapter 3 of this publication as closely as feasible.

D–16. Emergency disposition

The Army BSAT laboratory commanders/directors will develop procedures for emergency disposition (transfer or destruction) of BSAT during periods of instability or natural disasters and incorporate the procedures into the emergency response plan.

Appendix E

Instructions for DA Form 3180–1, DA Form 3180–2, and DA Form 3180–3

E–1. DA Form 3180–1 (Chemical and Biological Personnel Reliability Program Statement of Understanding)

a. Statement of understanding for conditions of employment.

(1) *Block A.* Individual's name.

(2) *Block B.* Applicable job title.

(3) *Block C.* Individual will initial items 1 to 10 to indicate the individual's understanding of each condition of employment.

b. Part II. Agreement. Blocks A and B. Individual's signature and date to reflect understanding and agreement with the conditions of employment.

E–2. DA Form 3180–2 (Chemical and Biological Personnel Screening and Evaluation Record)

a. Initial interview.

(1) *Blocks A through D.* Individual indicates consent or objection to PRP screening requirements. If the individual objects, the individual is not eligible for screening and certification for the PRP.

(2) *Blocks E and F.* The organization and job title for which the PRP screening is being conducted.

(3) *Blocks G through I.* CO's name, signature, and date reflecting the conduct of the initial BPRP interview.

b. Review of personnel security investigation report.

(1) *Block A.* As necessary, indicate whether the individual is eligible for interim certification.

(2) *Block B through D.* Information provided from the Security Manager or directly from the PSI report.

(3) *Blocks E through G.* CO's name, signature, and date reflecting the review of the PSI report.

c. Review of personnel records. Blocks A through C. CO's name, signature, and date reflecting the review of personnel records.

d. Medical records screening.

(1) *Block A.* A competent medical authority indicates whether or not medical information requiring CO review has been forwarded to the CO.

(2) *Blocks B through D.* A competent medical authority's name, signature, and date.

e. Drug testing.

(1) *Block A.* Date the drug test specimen was collected.

(2) *Block B.* The medical review official or other official will check the appropriate block.

(3) *Block C through E.* If the test results are certified negative by the medical review official, provide the medical review official's name, date, and signature. In other cases, provide the name, signature, and date of the official forwarding the results to the CO.

f. Certifying official's evaluation and assignment briefing.

(1) *Block A.* Certifying official's decision on whether the individual is suitable or not suitable for the PRP.

(2) *Block B, C, and D.* Certifying official's name, signature, and date.

(3) *Block E and F.* Individual's signature and date, reflecting the individual's understanding of the standards and objectives of the PRP. Leave blank if the individual was found unsuitable for the PRP.

g. Continuing evaluation. Optional use per local procedures.

(1) *Block A and B.* Certifying official's and individual's initials. Use as necessary per local procedures.

(2) *Block C.* Identify the reason for the update.

(3) *Block D.* Date of the update.

h. Administrative termination.

(1) *Block A.* Identify the PRP to which the administrative termination applies.

(2) *Block B through D.* Official's name, signature, and date.

i. Denial or termination.

(1) *Block A.* Identify the individual's status at the time of the denial or termination.

(2) *Block B.* Identify if the individual was military, civilian, or contractor at the time of the denial or termination.

(3) *Block C.* Identify the reason for denial or termination based on the PRP denial or termination criteria. Select one primary criterion for denial or termination; if there were additional applicable criteria, note that in Block D.

(4) *Block D.* Identify the rationale or details for the denial or termination. For Block C, items 1 (Alcohol-related) and 2 (Drug-related), identify by paragraph the specific alcohol or drug denial or termination criteria used. For Block C item 5 (medical, mental, or physical conditions), do not provide further details; use "See individual's medical records."

(5) *Blocks E and F:* Identify how and when the individual was notified of the denial or termination.

(6) *Blocks G through I.* Certifying official name, signature, and date.

(7) *Blocks J through L.* Reviewing official name, signature, and date for termination; not required for denial of certification.

j. Continuing Evaluation Continuation Sheet. Reproduce and use, as necessary.

E–3. DA Form 3180–3 (Chemical and Biological Personnel Reliability Program Status Report)

a. Organization data.

(1) *Block A.* State the entity or organization submitting the report.

(2) *Block B.* Indicate the four-digit CY for which the information is being reported.

(3) *Block C.* Indicate whether the report is for the chemical PRP or the biological PRP. If the organization has separate chemical and biological PRPs, submit a report for each PRP. However, individuals enrolled in both the chemical and biological PRPs should be reported on one form only, with a note in Part V (Remarks) to indicate the dual enrollment.

(4) *Block D and E.* Provide a name and phone number for an individual who can answer questions about the report.

(5) *Block F.* Enter the date of the report.

b. Personnel Reliability Program Activity. Provide the data separately for military, civilian, and contractor personnel in the organization's PRP.

(1) *Block A.* Provide the number of people in the organization's PRP at the beginning of the CY (January 1).

(2) *Block B.* Provide the number of people who completed the screening and initial certification and were enrolled in the PRP during the CY. If any of these were recertified after previous denial or termination, note this in Part V, Remarks.

(3) *Block C.* Provide the number of people who were denied enrollment in the PRP during the CY.

(4) *Block D.* Provide the number of people who had been enrolled in the PRP, but were terminated from the PRP for cause during the CY.

(5) *Block E.* Provide the number of people who had been enrolled in the PRP, but were administratively terminated during the CY.

(6) *Block F.* Provide the number of people in the organization's PRP at the end of the CY (31 December).

c. Reasons for denied enrollment into the Personnel Reliability Program during the calendar year.

(1) *Blocks A through H.* Provide the number of times specific denial of certification criteria were used during the CY.

d. Reasons for Termination for Cause from the Personnel Reliability Program during the calendar year.

(1) *Blocks A through H.* Provide the number of times specific termination for cause criteria were used during the CY.

e. Remarks. Include any comments addressing trends, significant changes, or other relevant factors to assist analysis.

Appendix F

Internal Control Evaluation

F–1. Function
This evaluation covers basic administration of the BSAT Security Program.

F–2. Purpose
This evaluation helps commanders evaluate key internal controls outlined below. It is not intended to cover all processes and procedures.

F–3. Instructions
Answers must be based on the actual testing of key internal controls such as by document analysis, direct observation, sampling, and simulation. Answers indicating deficiencies must be explained and corrective action indicated in supporting documentation. These key internal controls must be formally evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

F–4. Test questions
a. Do commanders/directors of Army BSAT entities by formal process--

(1) Maintain a biosecurity program to plan and coordinate security matters?

(2) What documents support the program, such as a command plan?

(3) Appoint a physical security officer on orders?

(4) Coordinate security/law enforcement requirements with supporting Director of Emergency Services or Provost Marshal?

(5) Conduct inspections or surveys per this regulation?

(6) Designate restricted areas or mission essential vulnerable areas, in writing?

(7) Ensure physical security, antiterrorism, and engineering personnel coordinate any new construction projects?

(8) Record, track, and resolve deficiencies found during inspections or surveys?

(9) Identify and forward through command channels resource requirements to the provost marshal.

(10) Request deviations to requirements exceeding standards of this regulation through command channels to OPMG for endorsement and forwarding to ASD (NCB) per this regulation?

(11) Request deviations to requirements not meeting standards of this regulation to the provost marshal and has the request been reviewed and endorsed by the activity's senior legal officer as required under the proponent and exception authority of this regulation?

(12) Are annual security exercises documented and maintained?

(13) Do all personnel provided unescorted access receive annual access control and security training?

b. Do commanders/directors of Army BSAT entities—

(1) Screen personnel in accordance with the procedures in this regulation and is the process documented on the DA Form 3180–2?

(2) Remove personnel from access/duty with BSAT for disqualifying factors in accordance with this regulation?

F–5. Supersession
Not applicable.

F–6. Comments
Help make this a better tool for evaluating management controls. Submit comments to Provost Marshal General (DAPM–MPO–PS), 2800 Army Pentagon, Washington, DC 20310–2800.

Glossary

Section I

Abbreviations

ACOM
Army command

ACSIM
Assistant Chief of Staff (Installation Management)

AECS
Automated Entry Control System

APHIS
Animal and Plant Health Inspection Service

APMS
Army Portfolio Management Solution

ARO
alternate responsible official

ASD (NCB)
Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs

AT
antiterrorism

BPRP
Biological Personnel Reliability Program

BSAT
biological select agents and toxin

BSL
biosafety level

CAC
common access card

CCTV
closed-circuit television

CDC
Centers for Disease Control and Prevention

CMA
competent medical authority

CO
certifying official

CY
calendar year

CY

DAIG
Department of the Army Inspector General

DRU
direct reporting unit

EA
Executive Agent

EA–RO
Executive Agent Responsible Official

FBI
Federal Bureau of Investigation

FSAP
Federal Select Agent Program

HQDA
Headquarters Department of the Army

ID
identification

IDS
Intrusion Detection System

IT
information technology

MEDCOM
U.S. Army Medical Command

NJOIC
National Joint Operational Intelligence Center

OPMG
Office of the Provost Marshal General

OSD
Office of the Secretary of Defense

OTSG
Office of the Surgeon General

PIN
personal identification number

PRP
Personnel Reliability Program

PSI
personnel security investigation

PSP
Personnel Security Program

REV
reviewing official

RO
responsible official

RSO
regional security officer

SAR
select agent regulation

SRA
security risk assessment

UPS
uninterruptable power supply

USACE
U.S. Army Corps of Engineers

USACIDC
U.S. Army Criminal Investigation Command

Section II

Terms

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 (for example, ability to carry, use, or manipulate) or the ability to gain possession of a BSAT.

Alcohol use disorder
A problematic pattern of alcohol use as defined by the current American Psychiatric Association Diagnostic and Statistical Manual of Mental Disorders. Alcohol use disorders include criteria for severity (mild, moderate, or severe) and for remission (early or sustained).

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.

Alternate responsible official
An individual designated by the Army BSAT 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 Army BSAT 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.

Barrier
A coordinated series of obstacles designed or employed to canalize, direct, restrict, delay, or stop movement.

Biological select agents and toxins
All of the biological agents or toxins listed in the SARs. 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 SARs. Biological agents and toxins identified by the CDCs and Prevention that present a high bioterrorism risk to national security and have the greatest potential for adverse public health impact with mass casualties. The list of select agents is reviewed and updated by the CDCs and Prevention.

Biological select agents and toxins 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 Federal Select Agent Program for, and possessing, BSAT.

Certifying official
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 Army BSAT 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.

Competent medical authority
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).

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-duty and off-duty behavior, and reliability on a continuing basis.

Critical vulnerability
A vulnerability that allows unimpeded access to biological select agents or toxins. For example, during movement or transfer, the agent is received by an individual who is not authorized by virtue of not being screened or certified in the PRP.

Custody
Responsibility for the control of, transfer and movement of, and access to BSAT. Custody may or may not include accountability.

Deadly force
The force that a person uses causing, or that a person knows, or should know, will create a substantial risk of causing death or serious bodily harm.

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.

Duress system
A method to covertly communicate a situation of duress.

Escorted access
The process by which persons who do not have approval from CDC or APHIS to access BSAT and require entry into BSAT-registered spaces are escorted or supervised when access is required to conduct visits, work, or other activities.

Exception
An approved permanent continuation of a deviation from this regulation in which the requirements are not being met and the approving authority determines it is inappropriate to meet the requirements. Compensatory security measures are required to provide adequate security for the deviation.

Insider Threat
Someone with authorized access with the intent and capability to steal or impact a select agent or toxin.

Intrusion detection system
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. A security system consisting of sensors capable of detecting one or more types of phenomena, signal media, enunciators, and energy source, for signaling the entry or attempted entry into the area protected by the system.

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 (for example, 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.

Recertification.
The process by which an individual, previously denied certification or terminated for cause from a PRP, is approved for certification into a PRP position.

Responsible official
An individual designated by the Army BSAT 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.

Restricted area
An area to which entry is subject to special restrictions or control for security reasons or to safeguard property or material

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.

Restriction (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.

Reviewing official
An Army BSAT 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, Volume 1&2.. The end product of the risk management process is the ID 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 RA), 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.

Risk assessment
A systematic evaluation process to determine the site's risk to sabotage, theft, loss, seizure, or unauthorized access, use, or diversion of materials from both external and internal threats.

Security risk assessment
Electronic records check performed by the Criminal Justice Information Service to determine if an individual who has been identified by an Army BSAT entity as having a legitimate need to access BSAT exhibits one of the statutory restrictors which would either prohibit or restrict access.

Select agent regulations
Federal regulations available in Part 73, Title 42, Code of Federal Regulations: Part 331, Title 7, Code of Federal Regulations; and Part 121, Title 9, Code of Federal Regulations.

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 BPRP when they are leaving the position or no longer require access to Tier 1 BSAT or perform BPRP duties.

Termination (for cause)
Removal of individuals who were previously screened, determined reliable, and certified capable of performing duties involving access to Tier 1 BSAT from the BPRP based on receipt of disqualifying information.

Tier 1 Biological select agents and toxins
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.

Two–person rule
Requires two personnel reliability program certified personnel (only one may be interim certified), equally qualified in a task being performed able to detect unauthorized acts one on the part of the other, access to BSAT.

Visitor
A person (for example, 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 Army BSAT entity.

Waiver
An approved temporary continuation of a deviation from this regulation in which the requirements are not being met, pending corrective actions to conform to the requirement. Compensatory security measures are required to provide adequate security for the deviation until corrected.

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.

Section III

Special Abbreviations and Terms
This section contains no entries.