U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

| **DEPARTMENTAL MANUAL** | NUMBER:<br>DM 9610-001 |
|---|---|
| SUBJECT: Security, Suitability, and Incident Response Procedures for High and Maximum Containment Facilities | DATE:<br>September 27, 2022 |
| OPI: Agricultural Research Service | EXPIRATION DATE:<br>September 27, 2025 |



## 1. PURPOSE

a. The purpose of this Departmental Manual (DM) is to define United States Department of Agriculture (USDA) requirements to secure biological agents used or held within USDA high and maximum containment facilities and facilities holding or utilizing regulated biological select agents and toxins (BSAT).

b. Security of pathogens held at non-high and maximum containment facilities are covered in another technical facility security USDA, DM 9610-002, *Security Policies and Procedures for Laboratories and Technical Facilities (Excluding Biosafety Level (BSL)-3 Facilities)*.

c. In the near future, DM 9610-002 will be updated to be consistent with this DM and may be retitled.

2. SCOPE

a. This DM contains a uniform set of USDA procedures which are intended to cover USDA laboratories that work with or have the capacity to work with biological agents requiring high containment (i.e., High Containment Biological Agents (HCBA)) or BSAT. A separate manual, DM 9610-002, will address requirements for agents that require lower levels of containment and the requirements for such pathogens that may simply be used at higher levels of containment for various logistical reasons (i.e., work at BSL-2 done in a facility capable of BSL-3 containment).

b. The USDA conducts research and regulatory activities, including detection and diagnosis, to protect American agriculture, forestry, and human health from biological agents. USDA scientists utilize biological agents in their research and diagnostic activities that could constitute a threat to either the health of humans, plants, or animals; or the productivity of agricultural systems if purposely or inadvertently released into the environment.

c. Not all biological agents constitute an equal risk of threat to humans. The Centers for Disease Control and Prevention (CDC) and the National Institutes of Health (NIH) provide a classification scheme (see Appendix B, *Definitions*, Biosafety Levels and Animal Biosafety Levels (A)BSLs, which describes all four biosafety levels). It demonstrates increasing levels of protection and can be used to protect researchers from pathogens based upon the risk assessment. In addition, agricultural scientists utilize a parallel set of standards for managing agricultural pests and pathogens to protect researchers and minimize the risk of a release into the environment (see Appendix B, *Definitions*).

d. USDA scientists work with crop pests that generally do not pose a direct threat to human health but may indirectly pose a threat through the production of toxins (e.g., mycotoxins, aflatoxins). The major concern with exotic crop pests is environmental protection due to the potential for harm to American crops.

e. USDA scientists work with animal pathogens and pests that need containment to prevent their release into the environment. An example of such a pathogen is African Swine Fever Virus – it does not pose a health threat to humans but would cause significant loss among impacted animal populations.

f. USDA scientists work with zoonotic pathogens that cause disease in animals and in humans. For example, certain influenza viruses of avians have been identified as the biological agents that cause illness in birds but can also cause serious illness and even death in humans.

g. USDA scientists may also work with human pathogens in order to solve animal disease or food safety problems. Human pathogens are sometimes better understood than their animal counterparts. USDA scientists have used the polio virus as a surrogate for the foot-and mouth disease virus. For example, USDA scientists work with E. coli to develop means to prevent its contamination of the food supply.

h. The Mission Areas, agencies, and staff offices foster a culture of safety. Each USDA employee at a biocontainment facility is ultimately responsible for physical security, biosafety, and biocontainment in the interest of American agriculture. The USDA employs Biosafety Professional(s) as technical resources who are responsible for managing and directing the biosafety program(s) of USDA biocontainment laboratories. Supervisors and managers at all levels within USDA are responsible for implementing operational physical security and biosafety programs, with direct oversight of biosafety and biocontainment being primarily assigned to researchers and diagnosticians.

i. Supervisors and managers provide resources for training, implementation, and monitoring of biosafety, biocontainment policies and programs. Individual researchers or diagnosticians play the primary role for day-to-day biosafety practices related to inventory management and security.

j. Researchers and diagnosticians also oversee utilization of biological agents by technicians and other support staff. USDA collateral duty biosafety officers serve as a resource for biosafety and biocontainment program implementation, quality control, biosafety inspections, and training.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

a. This DM supersedes DM 9610-001, *USDA Security Policies and Procedures for Biosafety Level-3 Facilities*, dated August 30, 2002.

b. Compliance with this DM is the responsibility of each Agency Administrator (or their designee). Each organizational level responsible for a high and maximum containment facility will submit a copy of its current security, biosafety, and incident response plans to an agency designated Headquarters (HQ) office at least annually or after revision.

c. If there is no change in the plan from the previous annual review, an email certification to that effect would be submitted. The entire plan would be resubmitted if any changes occur. The plan must be reviewed by the location at least annually, and revised as necessary using data from incidents, drills, or exercises.

d. Revisions to the plans must be communicated to affected location staff members within 30 calendar days:

(1) Animal and Plant Health Inspection Service – Emergency Management, Safety, and Security Division (APHIS – EMSSD):

Security – Security Branch – (301) 436-3144
Biosafety – (301) 436-3117
Personnel Security – (612) 336-3560

(2) Agricultural Research Service (ARS):
Security – Homeland Security Division (HSD) – (202) 441-6543 or
ARSHomelandSecurityDivision@usda.gov
Biosafety – Office of National Programs – (301) 504-4700 or
AgencyBiosafeyProgram@usda.gov
Personnel Security – (301) 504-1338 or
ARSPersonnelSecurity@usda.gov

(3) Food Safety and Inspection Service (FSIS):
Security – Physical Security – (202) 603-2048
Biosafety – (706) 546-2380
Personnel Security – (612) 659-7054

## 4. POLICY

The procedures in this DM expand on the policies established by forthcoming Departmental Regulation (DR) 9610-xxx, *Security, Suitability, and Incident Response for High and Maximum Containment Facilities.*

## 5. INVENTORY PROCEDURES

This DM defines USDA requirements to secure biological agents or toxins requiring high and maximum containment facilities and facilities holding HCBAs and BSATs. Each high or maximum containment facility will create or modify existing plans for security and incident response that are distinct from their own biosafety plan. The required plans will account for the following elements: Materials Accountability and Control Procedures; Physical Security Systems; Cybersecurity Systems; Personnel Security Determination; Incident Response Planning and Training.

### a. Purpose

The purpose of this section is to describe the requirements for handling, storage, shipping, disposal, record keeping, and monitoring of all biological agents and toxins (including regulated select agents) to ensure the creation of a current, accurate, and verifiable inventory record. The intent of this section is also to ensure that proper chain of custody procedures is utilized. For additional reference see CDC, *Guidance on the Inventory of Select Agents and Toxins, 7 CFR (Code of Federal Regulations) Part 331, 9 CFR Part 121, 42 CFR Part 73*.

b. Accountability Records

(1) A summary inventory at USDA known as the National Biological Agent and Toxin Inventory (NBATI) – formerly the National Pathogen Inventory system, is maintained by USDA ARS for USDA. The purpose for NBATI is to identify agents and toxins held by USDA as well as relevant points of contacts for those holdings. NBATI is validated annually;

(2) A detailed inventory of repository materials to be kept at the research or diagnostic facility;

(3) A materials accountability record for experimental or working stocks (examples include sets of related samples) within a laboratory notebook; and

(4) Records in the summary inventory in Section 5b(1) and the detailed inventory in Section 5b(2) must be maintained electronically and backed up on a separate system. The objective of maintaining such records is to ensure that the agency knows which biological agents are present, or have been present in its facilities, to ensure the accountability of scientists for the biological agents they store and use, and to ensure the final disposition of biological agents, including destruction or shipping to another facility. The NBATI will allow the Secretary of Agriculture to rapidly identify the USDA facilities at which particular biological agents or toxins are in use. The format for each is described below:

c. NBATI

(1) Agencies will maintain a summary inventory database, consisting of the fields listed below, to provide management with the capability to rapidly determine the scope of the biological agents and toxins in use or stored at each facility. USDA agencies will use the NBATI system for this purpose regardless of the containment level.

(2) The NBATI will also maintain a historical record of BSAT maintained by USDA facilities. This record will not be removed until it reaches its end of record retention schedule.

(3) NBATI Inventory records must include:

(a) Agency, Location, Laboratory Name;

(b) Agent type – limit categories to: Arthropods (non-indigenous arthropods and disease vectors or pests), Bacteria and Rickettsiae; Fungi; Oomycetes; Nematodes; Parasites; Parasitoids; Prions; Toxins; Viroids; Viruses; and others not Taxonomically Classified. This list of categories of agent types will allow the database to be searchable. Future distinctions may be appropriate or relevant as necessary to encompass the varied activities of the USDA as a whole and will be reviewed on an annual basis;

(c) Biological Agent Name: (minimum genus name; species if identified to that level). Provision of strain information is recommended, if known. Note: name changes for agents in annual updates in the inventory record; do not relabel tubes unless scientifically necessary (as long as they are uniquely identified and traceable using the inventory record);

(d) Principal Investigator (PI) or alternate contacts (e.g., Laboratory Representative) name with contact information (telephone number, fax number, email address, and laboratory address);

(e) The PI or alternate contact must notify HQ Representative when biological agents are added, destroyed, or transferred within 120 calendar days in order to ensure accuracy of the NBATI database. Do not notify the HQ representative for addition, destruction, or transfer of specific tubes or strains of agents or toxins which are still present within a specific PI's accession. The intent is to know what agents are present at the facility, regardless of strain or isolate identification; and

(f) Only notify HQ of the complete removal of an agent or toxin from a PI's holdings (e.g., all isolates of Bacillus anthracis are destroyed due to the retirement of a PI or the addition of a new agent or toxin that a PI did not previously possess (e.g., a new PI is hired and is bringing a collection of Porcine Reproductive and Respiratory Syndrome Virus isolates). For further information see USDA, DR 9630-001, *USDA Policies and Procedures on Biohazardous Waste Decontamination, Management, and Quality Controls at Laboratories and Technical Facilities*.

d. Facility Inventory of Repository Materials

(1) Each PI, Lead Scientist, Laboratory Director, and Laboratory Supervisor that stores or uses any biological agent or toxin will maintain a current detailed inventory as outlined below. The location information will be maintained in a standard database format and needs to be readily accessible to HQ (i.e., needs to be verifiable within a reasonable timeframe and consistent with the 40 CFR Part 792, *Good Laboratory Practice Standards*, that address record keeping).

(2) Each individual USDA Center Director and Location Coordinator must ensure that a current centralized master database reflecting the cumulative biological agents or toxins of all management units and PIs is maintained at the facility. The database will not only serve as a record of current inventory but will also serve as a historical record of biological agent(s) and toxin(s) used at the facility. Placing records no longer in use in an inactive file rather than deleting them will accomplish this requirement. Inactive records will be kept for a minimum of 3 years but may not be removed until the NBATI historical record for the item is confirmed.

(3) Each scientist working with biological agents is responsible for maintaining their inventory; however, the Center or Laboratory Director or the Responsible Official (RO) must review, or direct the review, of inventory records annually for accuracy and completeness. This review must include documentation of procedures undertaken to address any discrepancies found in the records. Random reviews may be conducted by the Agency Biosafety Officer and other designated staff (Area Safety and Health Managers or other agency official not employed at that specific laboratory) to review inventory procedures, records, or compliance with this policy. If older repository material information elements (e.g., full history of the acquisition) are unavailable, an estimate based on the quantity acquired, the date and the source (if known) may be used.

Information to be included in the database is as follows: an accurate, current inventory of the biological agents and toxins (including viral genetic elements, recombinant, synthetic Nucleic Acids (NA), and organisms containing recombinant or synthetic NA) held in long-term storage, including:

(a) The name and characteristics of the agent or toxin (examples include strain designation, and Genetic Database (GenBank) Accession number);

(b) The quantity acquired from another individual or entity (e.g., containers, vials, tubes); date of acquisition; and the source if known (toxin inventories must include a weight per volume amount for these entries as well; agent inventories do not require volume tracking);

(c) If used completely, transferred, or destroyed: The agent or toxin used and purpose of use, quantity, date(s) of the use, and by whom;

(d) Where stored (minimal requirement is the building and room). However, it is recommended to be able to identify the specific location within the freezer or other storage device within 5 minutes; and

(e) If used and returned to storage: When moved from storage and by whom, for what purpose, quantity, and date returned to storage and by whom (toxin inventories must include a weight per volume amount for these entries as well).

e. Materials that must be inventoried include:

(1) Confirmed clinical specimens, laboratory cultures, animals, animal tissues, plants, and plant tissues containing biological agents, recombinant, or synthetic organisms, as well as genetic elements, recombinant or synthetic NA encoding such genetic material, unless specifically excluded by one or more of the criteria below. Animals or plants intentionally or accidentally exposed to or infected with an agent that must otherwise be inventoried, must be inventoried as distinct, uniquely identified entries (including number and species, location, and appropriate disposition);

(2) Fluid, serum, tissue, or other samples collected from animals or plants infected with or exposed to biological agents, or materials listed in Section 5e(1);

(3) Diagnostic samples from which the presence of an agent or toxin has been detected are subject to these inventory requirements 30 calendar days after receipt; however, diagnostic samples from which only an antibody response to an agent or toxin is detected or expected do not need to be inventoried as long as there is peer-reviewed, scientific evidence to suggest a low risk of biologically active agent or toxin being present in the sample (e.g., convalescent sera where immunity is known to be sterilizing, surveillance samples from clinically healthy animals);

(4) Any substance of biological origin that is not fully classified by the above criteria, or if the classification is unknown, see Section 5e(8) below;

(5) NA are polymeric macromolecules that include deoxyribonucleic acid (DNA) and ribonucleic acid (RNA) that are made from monomers known as nucleotides. The term NA is the overall name for DNA and RNA and is synonymous with "polynucleotide." The basic component of biological NA is the nucleotide, each of which contains a pentose sugar backbone (ribose or deoxyribose), a phosphate group, and a nucleobase. NA are fundamental to biological processes and can be manipulated or generated within the laboratory by many methods;

(6) For the purposes of this DM, NA will be considered to be "High Containment Pathogenic Nucleic Acids" (HCPNA) when they are:

(a) Inherently infectious or toxic, or are immediate precursors to production of molecules or organisms that are biologically-active and pathogenic for humans, animals, and plants (i.e., the NA are capable of generating infectious forms of a HCBA virus by utilizing host polymerases but without the need for any additional exogenous factors (e.g., proteins, NA);

(b) Encode for the functional form(s) or functional subunits of any of the HCBA toxins, or toxins produced by HCBA organisms, if the NA can be expressed in vivo or in vitro, or are in a vector or recombinant host genome that can be expressed in vivo or in vitro;

(c) Have been genetically modified but still retain biological activity and pathogenic potential in humans, animals, and plants; or

(d) Comprise a system designed for the generation of any of the above NA (e.g., an intact reverse genetics system for a negative-sense RNA virus, all the genome segments from a segmented viral genome, or expression plasmids containing all such segments when stored together in an individual PI's inventory).

(7) For this DM, the following are examples of materials that would not be covered:

(a) NA that cannot produce infectious forms of any of the HCBA viruses, including genetic elements and genomes of covered viruses;

(b) Polymerase chain reaction products, primers, or DNA fragments of HCBAs (unless they encode for a functional form or subunit of a covered toxin and can be expressed);

(c) Complementary DNA made from HCBA NA (only the positive strand RNA form of the viral genome is covered). Complementary DNA copies of HCBA RNA viral genomes are not covered because they would first need to be transcribed into RNA, then introduced into cells and translated into protein(s), and therefore would not be an immediate precursor to the virus;

(d) NA encoding complete genomes of single negative RNA viruses, double stranded RNA viruses, and double-stranded DNA viruses that require a unique polymerase for expression. These genomes are incapable of producing infectious virus when introduced by itself into an animal or permissive cell without the introduction of rescue plasmids or other exogenous factors;

(e) NA that encodes for the genomes of HCBA bacteria or fungi, including chromosomal, recombinant, or synthetic DNA; and

(f) NA that encodes for toxins not subject to the DM requirements but derived from HCBAs (i.e., non-functional toxins or toxin subunits, toxins or subunits that don't have pathogenic potential in humans, animals, or plants). HCPNA sequence information is also exempt.

(8) Materials exempt from these inventory requirements include:

(a) Animals injected with or exposed to a toxin (for example, by inhalation, dermal absorption, or ingestion) are not considered a "toxin" and would not need to be inventoried as such, but still must be inventoried as an animal for the Institutional Animal Care and Use Committee or other purposes. Until the toxin is injected into or exposed to the animal, the toxin must be inventoried as a distinct, uniquely identified entry. This exemption applies only to those toxins that are bound to cells in a near-permanent fashion or are otherwise detoxified or consumed by metabolic processes of the animal within hours of the injection or exposure;

(b) Diagnostic or clinical specimens being temporarily stored until testing can be completed (e.g., within 30 calendar days of receipt);

(c) Confirmed diagnostic or clinical specimens that are stored for the sole purpose of fulfilling regulatory obligations. Any confirmed diagnostic or clinical

specimen stored for longer than 100 calendar days post-testing must be inventoried regardless of the purpose of retention;

(d) Non-viable agents or toxins, as long as the office of record maintains records that certify negative results in viability testing for at least 3 years. See DR 9630-001 for further information; and

(e) Diagnostic samples from which only an antibody response to an agent or toxin is detected do not need to be inventoried, subject to the limitations noted above.

(9) Procedures for the documentation of external transfers of biological materials:

(a) Agencies must develop procedures for the documentation of external transfers of biological materials. These would include (at a minimum) chain of custody procedures during the transfer and contact information of the recipient; and

(b) Intra-agency transfers must be documented (i.e., in laboratory notebooks, electronic records, and in the adjusted inventories of the sender and receiver). A biological agent or toxin can be transferred internally to another scientist within the same facility, providing that the biosafety level for containment and the level of staff competence are maintained. The receiving scientist must be added as the responsible party in the biological agent database (NBATI) and all required records must be updated to document such transfers.

(10) In the case that a biological agent or toxin is destroyed:

(a) The quantity, date of such action, by whom, and the method of inactivation or destruction is required. This would include information in support of the appropriateness of the method (e.g., concentration and contact time of chemical agent; pressure, temperature, and time of autoclave run). See DR 9630-001 for further information;

(b) If you use or store BSAT inventories, you must comply with 7 CFR § 331.16, *Transfers*; 7 CFR § 331.17; *Records*; and 7 CFR § 331.19, *Notification of theft, loss, or release*; and

(c) Any working cultures that become new repository stocks must be added to the inventory. New biological agents and toxins (not already in inventory) identified in diagnostic or experimental samples or generated through recombinant or synthetic NA technologies must be added to the laboratory or repository inventory and the NBATI (if they are unique), if they are not transferred or destroyed within 120 calendar days of identification or creation.

(11) Material Accountability of Experimental or Working Samples:

Experimental samples and repository stock aliquots used for working stocks or experimental purposes are tracked by laboratory records (e.g., laboratory notebooks, electronic systems). The location of material use must be included. Within 60 calendar days of the conclusion of each experiment or set of related experiments, the disposition of the infectious material, including the means of disposal, must be verified by the signature in the relevant tracking documents of the researcher or diagnostician, or their designee.

(12) Packaging and Shipping of Infectious Material:

Packing and shipping of biological agents or toxins will meet current national and international regulations and guidelines:

(a) Shipping and receiving of biological agents will meet applicable guidelines and be tracked by each agency. Organisms and vectors may require an APHIS permit for transport (9 CFR § 122, *Organisms and Vectors* and 7 CFR § 330.200, Subpart B – *Movement of Plant Pests, Biological control Organisms, and Associated Articles.* USDA laboratories employ a small number of agents designated CDC, *Federal Select Agent Program (FSAP)* as select agents. Shipping and tracking of these agents will be done in accordance with select agent regulations found in, 7 CFR § 331, 9 CFR § 121 and 42 CFR § 73; and

(b) The Department of Commerce regulations, including requirements for export permits, must be met for the export of pathogenic materials, or intellectual property associated with those agents and toxins. Each agency will ensure that a process is established to ensure compliance with relevant export requirements to include deemed export. A review of these agency processes will be conducted on an annual basis to ensure compliance. These reviews may include activities such as a review of shipping records in the database.

(13) Physical Review of Accountability Records:

Scientists working with biological agents are responsible for the accuracy of electronic databases and laboratory notebook records, which are subject to review by their supervisor, Laboratory Director, and authorized agency personnel. Physical review will be performed at least annually. Methods used during physical review or reconciliation may include counts of entire inventory or statistical sampling of records and repository materials. The Center Director, Laboratory Director, or equivalent authority is responsible for ensuring the physical reviews are accomplished. Random reviews must be conducted on an annual basis by the Agency Biosafety Officer (or equivalent) to ensure compliance at the locations.

(14) Biological Agent Security:

HCBAs must be secured within the high and maximum containment facility. Only authorized personnel with the appropriate position designation will have access to freezer keys and codes, and the secure containment capabilities and requirements of the storage unit will be determined by the highest risk biological agent within the storage unit.

(15) Sample Labeling:

All sample vials in the inventory must be labeled in a permanent manner so that all information is readable. Information can be coded to a separate record but must be verifiable in 5 business days.

(16) Inactivation and Disposal of Biological Agents:

Procedures must be in place at each location for this purpose and must include, as appropriate, autoclaving, other thermal inactivation technology, chemical treatment, or an equally effective comparable process. Validation of procedures for disposal is strongly encouraged, such as load configuration studies for autoclave loading, kill curve generation for chemical inactivation, or other methods that give confidence that the methods used are appropriate to the local conditions. All biological agents and contaminated supplies will be inactivated and disposed through an approved method (which is validated if the materials are inactivated for future use). See DR 9630-001 for further information.

(17) Internal Transfer:

A biological agent or toxin can be transferred internally to another scientist within the same facility, providing that the biosafety level for containment and the level of staff competence are maintained. The receiving scientist must be added as the responsible party in the biological agent database and all required records must be updated to document such transfers.

## 6. PHYSICIAL SECURITY PROCEDURES

a. Purpose.

This section describes the physical security program requirements to:

(1) Ensure appropriate levels of protection against unauthorized access, theft, diversion, or loss of custody of biological agents or BSAT at high and maximum containment laboratories, or registered select agent space, as regulated by the FSAP. This includes loss or theft of information related to these biological agents or BSAT and other acts that may cause unacceptable adverse impacts on national security or on

the health and safety of USDA employees, the public, U.S. animal and plant products, or the environment;

(2) Establish levels of graded protection in accordance with the potential consequences based on the site-specific physical security risk assessment and the Department of Homeland Security (DHS), *The Risk Management Process (RMP), An Interagency Security Committee (ISC) Standard* requirements;

(3) Ensure, based on a site-specific physical security risk assessment and the ISC RMP requirements, effective planning, and prudent application of resources to establish graded protection, including operational procedures and administrative controls;

(4) Provide guidance, based on a site-specific physical security risk assessment and the ISC RMP requirements, to develop a written security plan that addresses the requirements of this DM;

(5) Instruct those entities that possess, use or transfer BSAT to comply with applicable regulations (7 CFR § 331 (Plant); 9 CFR § 121 (Animal) and 42 CFR § 73 (Human)).

b. High Containment Biological Agents (HCBA).

HCBA are ubiquitous, existing both in nature and in laboratories around the world. However, it is mandatory to limit control and monitor access to biological agents and BSAT at USDA-controlled high and maximum containment laboratories, or registered select agent space, to authorized individuals, as well as to deter and detect unauthorized access. This includes information related to these biological agents and BSAT at all high and maximum containment laboratories or registered select agent space.

c. Site-Specific Physical Security Risk Assessment and ISC RMP Requirements.

(1) The physical security system(s) at high and maximum containment or select agent facilities must be designed according to a site-specific physical security risk assessment and ISC RMP requirements, which will evaluate targets, adversary capabilities, consequences, and vulnerabilities. This site-specific physical security risk assessment is a key requirement that, in conjunction with other existing applicable regulations, will determine the graded protection strategies necessary to adequately protect Government assets, as well as the physical security systems necessary to compliment the identified graded protection strategies.

(2) These physical security systems may include, but are not limited to:

(a) Electronic Access Control System;

(b) Intrusion Detection System (IDS);

(c) USDA Enterprise Physical Access Control System (ePACS) Connectivity;

(d) Closed Circuit Television (CCTV) Camera and Recording System;

(e) Information Systems Protection;

(f) Facility Barriers;

(g) Locks and Key Control;

(h) Protection Systems Monitoring;

(i) Protective or Response Force Requirements;

(j) Visitor Requirements; and

(k) Other systems or strategies as required or necessary based on existing regulatory requirements.

(3) DHS, National Protection and Programs Directorate, Office of Infrastructure Protection, ISC Standards has standards that can require very proscriptive security measures based on the criteria that defines the facility physical security requirements (Facility Security Levels (FSL) 1-5). These standards will have to be addressed in any subsequent risk assessment or management plan of USDA high and maximum containment laboratories.

(4) The Select Agent Program also requires increased physical security parameters for those entities that possess, use, or transfer Tier (T) 1 select agents or toxins. Development and implementation of these requirements can be complex and far-reaching. If at any time you have any concerns or questions, please contact either your RO, individual agency security office, or the USDA Office of Safety, Security, and Protection (OSSP), Facility Protection Division.

(5) The site-specific physical security risk assessment and ISC RMP requirements review must be performed by qualified individuals, identified by the Department or agency, who have expertise in physical security. The risk assessment must be revalidated once every 5 years for Level I and II facilities and once every 3 years for Level III, Level IV, and Level V facilities. As outlined in ISC RMP.

(6) The objectives and performance of the physical security program must be reviewed and documented annually by qualified individuals who have expertise in physical security. A model for performance verification requirements (of laboratory competencies) is presented in Section 11*, Training*, of this DM and may provide a framework for assessment of performance of security personnel. Performance verification of the security plan would be accomplished annually through a regular

series of drills or exercises that test various elements of the plan. See also Section 6p, *Performance Testing and Verification*, below.

(7) The site-specific risk assessment and ISC RMP criteria will lead to specific recommendations as to how to implement the concepts of graded protection. Security barriers will be defined and described to such an extent that a knowledgeable person can implement the recommendations, as well as provide training to affected personnel on the implementation of the recommendations (i.e., a detailed-out brief). For example, a barrier requiring key-locks with copy restrictions will recommend specific hardware. Similarly, electronic access requirements will also require hardware recommendations as well as implementation criteria (e.g., on-site or contract control of access assignment).

(8) Finally, barriers will be described according to the principles of graded protection, where requirements for unique items (key cards), unique knowledge (Personal Information Numbers or PINs), or both will be highlighted to aid in training and educational initiatives for affected personnel. Similarly, definitions of critical assets and security layers will solicit the recommendations of on-site personnel, leading to a comprehensive security program based on the site-specific risk assessment that can be adopted and integrated into the overall facility management plan with a minimum of disruption while maximizing both the efficacy of security efforts and the compliance of facility personnel.

d. Site-Specific Considerations.

The physical security program must be tailored to address site-specific characteristics and requirements as well as ongoing operational needs, and to achieve adequate protection levels using current technology in a cost-effective manner. The protection strategy may be tailored to address varying circumstances and may combine elements of deterrence, detection, delay, assessment, and response to achieve the desired goal.

e. Graded Protection.

(1) Physical security programs will provide graded protection in accordance with the assessed risk of the asset. The intent of USDA is to provide the highest level of protection to security interests whose loss, theft, compromise, or unauthorized use could compromise the national security, and the health and safety of USDA employees, the public, U.S. animal and plant products, the environment, and USDA programs.

(2) Actions cannot be taken to reduce the probability or consequences of all malevolent events to zero. However, the acceptable level of risk would be determined based on an evaluation of a variety of facility-specific goals and considerations. Protection-related plans (Site-Specific Security Plan or BSAT Security Plan) will describe, justify, and document the graded protection provided to biological agents and BSAT at high and maximum containment laboratories, or registered select agent

space, as well as information related to biological agents and BSAT at high and maximum containment laboratories, or registered select agent space. Following ISC RMP criteria, the Security Plan will be reviewed and updated annually, in response to any incident, or as required by the Select Agent Regulations.

(3) The nature and likelihood of the threat, the vulnerability of the asset as it is stored or used at the facility, and the potential consequences of an adversarial act will be considered in determining the appropriate level of protection against risk. Accordingly, the posture of physical security programs will provide graded protection in accordance with the importance of the asset.

(4) Facilities will consolidate, to the extent practical, biological agents and BSAT at high and maximum containment laboratories, or registered select agent space, concentrate intrusion detection and assessment systems at the locations where the biological agents and BSAT at high and maximum containment laboratories, or registered select agent space are kept, and control access to these locations.

(5) Furthermore, any T1 listed BSAT would be further physically separated away from the other biological agents and BSAT at high and maximum containment laboratories or registered select agent space, when feasible, to avoid implementing the higher security and reliability requirements of the CDC*, Guidance on the Inventory of Select Agents and Toxins*, 7 CFR Part 331, 9 CFR Part 121, 42 CFR Part 73 regulations that apply to T1 BSAT. To facilitate normal operation and maintain continuous operations, the protection strategy will mitigate the severity of the event through a combination of deterrence, detection, response, and recovery option planning.

f. Security and Restricted Access Areas.

(1) Unescorted access will be limited to authorized individuals. An authorized individual is defined as someone who has been approved for access by the entity and has had the appropriate background investigation successfully adjudicated.

(2) In addition, for those individuals to have unescorted access to BSAT registered areas, there will be a requirement to complete a successful Security Risk Assessment (SRA) through the Federal Bureau of Investigation, Criminal Justice Information Services (FBI-CJIS), including approval for access by the FSAP and the RO.

(3) Any individual without approved access will be escorted at all times by an authorized individual consistent with the FSAP, and USDA policy where the HCBA and BSAT are stored, actively manipulated, or accessible in high and maximum containment laboratories or registered select agent space.

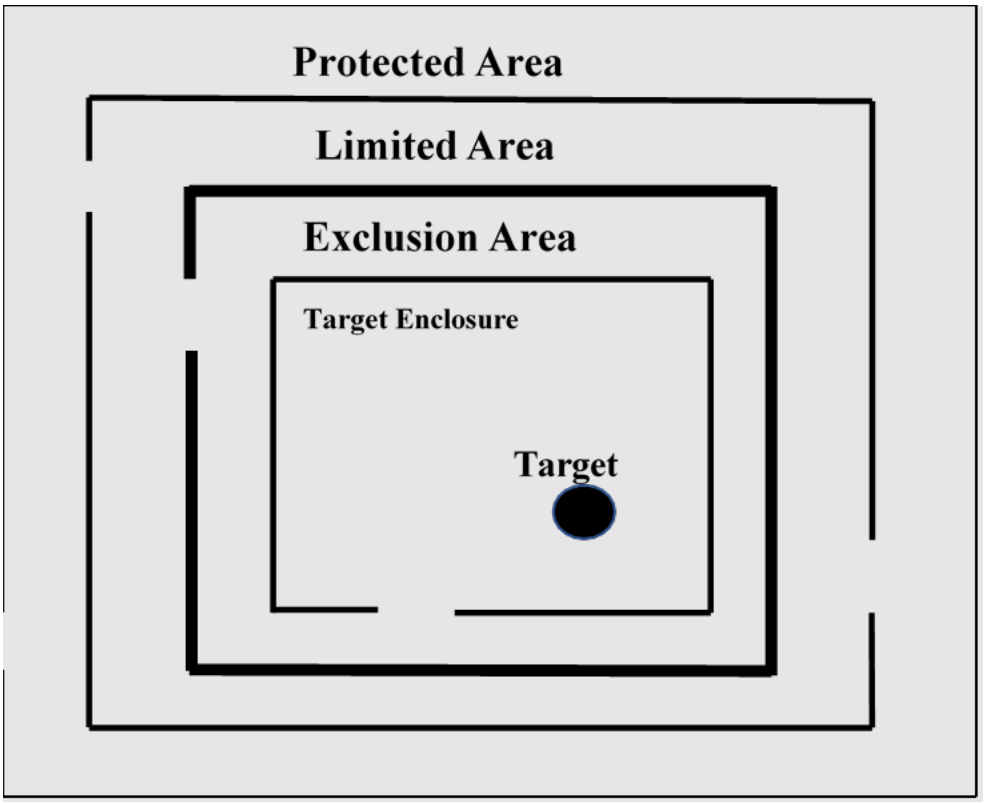
(4) Controls will be established to deter, detect, delay, assess, and respond to unauthorized access to security areas. Access control requirements will be layered

(e.g., graded) as appropriate for the asset being protected. At successive boundaries, access controls will become increasingly exclusionary.

(5) Means will be provided to deter and detect unauthorized intrusion into limited and exclusion areas as defined below.

(6) Methods may include locked barriers, monitored surveillance, use of electronic intrusion detection sensors and alarm systems, random patrols, or visual observation. The protection program will include real time alarm annunciation monitoring to assess alarms. Figure 1, *Graded Protection Model*, depicts the graded protection approach to deterring and delaying unauthorized entry into protected, limited, and exclusion areas by staggering the entrances.

FIGURE 1, *Graded Protection Model*




g. Property Protection Area-Lowest Level of Protection.

A property protection area is a security area established to protect against damage, destruction, or theft of USDA-owned property. At each site, the USDA property boundary would, if at all possible, be identified with signs posted prohibiting trespassing. Physical barriers, where determined to be necessary, will be used to protect property and facilities.

All buildings in the property protection area must be locked and any keys utilized will be protected. To ensure key protection, a key accountability system will be implemented.

h. Limited Area-Intermediate Level of Protection.

(1) A limited area will have barriers identifying its boundaries and encompassing the designated space, as well as access controls to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area without escort. For example, a limited area may be a building (or non-public portion of a building) that contains an exclusion area.

(2) Access to a limited area will require a unique item (e.g., LincPass credential) and an appropriate level of intrusion detection as identified through the physical security assessment. Sufficient exterior lighting will be provided to allow the protective force to detect and assess intrusions. Examples of limited areas could include freezer repositories (except as below), wastewater storage, treatment rooms, air filtration (High Efficiency Particulate Air (HEPA) filter) areas, and critical electronic file storage, etc. Designations of areas would be reviewed based on the required 3-year physical security risk assessment (FSL and ISC RMP criteria) and as necessary based on an incident (select agent rules requirement).

i. Exclusion Area-Highest Level of Protection.

(1) An exclusion area will have barriers identifying its boundaries and encompassing the designated space, as well as access controls to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area. For example, an exclusion area may be a laboratory containing biological agents or BSAT at high and maximum containment laboratories or registered select agent space. Additionally, it may also include information related to the biological agents or BSAT at high and maximum containment laboratories or registered select agent space.

(2) Access to an exclusion area will require a unique item (i.e., LincPass credential) and unique knowledge (i.e., PIN) to gain access. Access control and intrusion detection will be managed by authorized USDA personnel qualified and trained on the local access control system. Examples of exclusion areas could include animal and laboratory facilities and freezer repositories containing, Foot and Mouth Disease virus, Rinderpest virus. Designations of areas risk assessments will be conducted once every 5 years for Level I and II facilities and once every 3 years for Level III, Level IV, and Level V facilities as outlined in the ISC RMP, or as necessary based on an incident (select agent rules requirement).

j. Storage.

Biological agents or BSAT at high and maximum containment laboratories or registered select agent space and information related to biological agents or BSAT at high and maximum containment laboratories or registered select agent space would be stored in either a limited or an exclusion area based on the physical security risk assessment and secured within a locked security container or locked room.

k. Access Control, Entry and Exit Inspections.

(1) Access control points will be designed to provide positive control over pedestrian traffic. The access control points will provide a barrier to personnel entering limited areas and exclusion areas until such time as entry is requested or authorized. Electronic access control systems will read data entered by the person requesting access, and if the data are successfully validated, the portal will be electronically unlocked. When practical, as stated in DM 4620-002, *Common Identification Standard for U.S. Department of Agriculture*, the USDA ePACS would be utilized to administer access control as it provides an authorized system that has controls in place for monitoring system intrusion; change management to monitor and audit system changes; and is compliant with Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, allowing employees to utilize their LincPass. When ePACS cannot be utilized, the Physical Access Control System (PACS) server must be certified and accredited by the Mission Area Assistant Chief Information Officer and be granted authority to operate. In addition, change management processes and a disaster recovery plan must be documented for the PACS server.

(2) A security badge that electronically stores information relevant to the badge and badge holder will be used for automated access control systems. When practical, the USDA LincPass credential will be the primary security badge utilized for access control as it provides a higher level of assurance than a site badge (i.e., proximity card) and authenticates to the USDA ePACS ensuring that, before access is granted, the LincPass is not suspended or revoked. The access authorization database will be updated within 24 hours by ePACS when an individual's access authorization requirement has changed or when an individual is transferred or reassigned. If the situation warrants, revocation of access rights would be terminated immediately by the site security manager and the designated official.

(3) If electronic access control is utilized, to prevent tailgating, a process where the electronic lock will reengage after a valid entry or within 12-20 seconds after a valid card read, to prevent unauthorized access for persons not authorized to enter the secure area.

(4) The electronic access control system will record all transactions to include authorized and unauthorized access for tracking and auditing purposes. Records

will be kept on each transaction for a minimum of 1 year, with the exception of BSAT records, which will be kept on file for at least 3 years.

(5) Access into critical areas such as mechanical areas, electrical and telecom closets, wastewater decontamination areas, emergency generators, and air intakes and handlers will be secured at all times. This is not an exhaustive list and may include other location specific critical areas. If a key lock is utilized, key control policies will be implemented. Key control policies would also include authorization criteria, accountability, and policy for securing keys and preventing copying or loaning of keys. If keys are found to be unaccounted for, locks will be rekeyed within 14 calendar days.

(6) Cypher locks, if utilized, will have their combinations changed whenever someone who possessed the combination separates from their position and no longer has a requirement for access.

l. Intrusion Detection and Assessment Systems.

(1) Intrusion Detection Systems (IDS) will be installed to provide reasonable assurance that breaches of security boundaries are detected, and that alarm annunciation is provided to protective personnel, to include law enforcement.

(2) A means for immediate detection of intrusion will be provided by the use of IDS which will provide notification to a dedicated real-time monitoring staff such as an onsite guard post providing real time monitoring or to a central station alarm company (e.g., by a Underwriters' Laboratories (UL) Certified Monitoring Company). IDS alarms will be investigated by closed circuit television or patrol response. As a secondary means of detection, patrols of facilities will be conducted at random intervals at designated locations. The use of a guard tour tracking system would be recommended.

(3) If deemed appropriate by the site-specific risk assessment, the intrusion detection systems will be:

(a) Continuously monitored 24 hours a day, 7 days a week by the location's guard force, a law enforcement entity, or an accredited UL listed third party by personnel trained to assess alarms and initiate appropriate responses;

(b) Operated and maintained by personnel certified and trained in electronic security systems in a manner ensuring that the number of false and nuisance alarms does not reduce system credibility;

(c) Tamper-resistant or tamper-alarmed and equipped with line supervision for security sensors (including integrity of data transmission). Line supervision in this context refers to the capability of the intrusion detection system to detect

an interruption or a fault in the lines connected to security sensors, such as door contacts, motion detectors or glass break devices.

(d) Other risk mitigation measures will be provided during times when the intrusion detection system is not in operation or at temporary locations where a permanent intrusion detection system is not practical or cost effective.

(e) Records will be kept on each actual or nuisance alarm for a minimum of 1 year, with the exception of BSAT records, which will be kept on file for at least 3 years.

(4) The record will be reviewed, analysis performed, and corrective measures taken to correct system malfunctions. The record will contain, at a minimum: date and time of the alarm; cause of the alarm or probable cause if definite cause cannot be established; and the identity of the recorder or the operator on duty.

(5) Alarm monitoring systems will be self-checking (including intercity of data transmission) and will annunciate system failure(s) to the alarm monitoring station. Systems will indicate the type and location of the alarm source.

(6) Systems will be functionally tested and documented in accordance with established procedures at a frequency that is determined by a security risk assessment or annually at a minimum.

(7) Doors and hatches which provide primary access to limited and exclusion areas will be equipped with IDS devices, unless already within a limited or exclusion area. In certain applications, local audible alarms may also be part of the intrusion detection system. Balanced magnetic switch contacts or equivalent will be used on each door to provide detection of attempted or actual unauthorized access.

(8) Panic hardware or mechanical emergency exit door hardware used on emergency doors located in limited or exclusion areas will be operable only from the secure side of the building or room and will meet all applicable life safety codes. Exterior emergency exit doors will have all door hardware removed from the unsecure side of the door.

(9) Windows which provide access to exclusion areas will have intrusion detection sensors or other physical security barrier securely fastened on the inside. This also applies to doors with windows based on a risk assessment. All windows in exclusion areas will be closed and rendered inoperable at all times.

m. Protection of Access Control and Intrusion Detection.

(1) Systems. Security-related equipment will be protected from unauthorized physical access, which would include all detection, alarm devices, access control system components, and CCTV devices, including transmission lines and integrity of data

transmission to enunciators, and will be supervised in both the access and secure modes.

(2) System components used for protection of other interests will be protected, consistent with a cost and benefit analysis determined by each facility. Electronics enclosures and wiring junction boxes will be secured, have tamper switches, have tamper resistant hardware, and will have line supervision for all security devices.

n. Auxiliary Power Sources.

(1) Battery, emergency generator auxiliary power, or uninterruptible power supply (UPS) will be available and will be capable of maintaining full operation of the intrusion detection and access control systems for 4 hours. Additional auxiliary power requirements in excess of 4 hours would be addressed in the local continuity of operations plan. Auxiliary power sources will have the capability to facilitate operational testing or routine maintenance.

(2) Transfer to auxiliary power will be automatic upon failure of the primary source and will not affect operation of the security system or device. The alarm monitoring station will receive an alarm indicating failure of the security system power and transfer to the auxiliary power source.

o. Maintenance.

(1) Individual location security-related subsystems and components will be maintained in an operable condition. A regularly scheduled testing and maintenance program is required. Corrective maintenance will be completed within 24 hours of the indication of malfunction or contingency plans will be implemented. The local USDA or entity authority for physical security programs will determine if contingency plan measures are necessary.

(2) The following system elements will be included in a preventive maintenance program:

(a) Intrusion detection, access control and CCTV systems;

(b) Central alarm station enunciators; physical security equipment;

(c) Personnel access control and inspection equipment;

(d) Security lighting and security system-related emergency power;

(e) Auxiliary power supplies; and

(f) Batteries supporting the access control and IDS.

(3) Personnel, who test, maintain, or service security system elements will have appropriate access authorization where the maintenance is being performed.

(4) Records of maintenance and repairs of decontamination equipment (autoclaves) also need to be held. See DR 9630-001, for further information.

(5) Records of testing and all maintenance will be retained for 1 year, with the exception of BSAT records which will be kept on file for at least 3 years.

p. Performance Testing and Verification.

(1) Performance verification programs (e.g., drills or exercises) will provide for operability and effectiveness tests of electronic security systems or components of systems. Testing frequencies of these electronic security systems will reflect site-specific conditions, operational needs, and threat levels.

(2) A system performance test encompassing the electronic security systems will be performed annually. Testing will include integrated systems of equipment and hardware, administrative procedures, protective forces, and other staff.

(3) The performance verification program will provide for operability and effectiveness tests. The program will be implemented in a graded manner. Elements that are determined to be most significant are those that provide protection for biological agents or BSAT at high and maximum containment laboratories or registered select agent space. This is also applicable to information related to biological agents or BSAT at high and maximum containment laboratories or registered select agent space.

(4) After action reports would identify all corrective actions needed to address plan deficiencies and a list maintained of issues not remediated within 30 calendar days.

q. Response Forces.

Response capability to IDS alarms will be provided to protect biological agents or BSAT at high and maximum containment laboratories or registered select agent space and information related to biological agents or BSAT at high and maximum containment laboratories or registered select agent space. Information protection would correlate with cybersecurity requirements. The response capability must be provided by trained first responders, an on-site guard force, or by local law enforcement. Response times will be appropriate for the protection strategy employed at the site, based on the site-specific risk assessment. Pursuant to ISC RMP criteria, a vulnerability and risk assessment will be performed by authorized USDA personnel to determine if the on-site security force would be armed.

r. Duress Systems.

The physical location of duress alarm devices, as determined by the physical security assessment, would be mounted in as unobtrusive location as practicable. Duress alarms will not annunciate at the location initiating the duress alarm. Duress alarms will annunciate to a dedicated real-time monitoring entity.

s. Radios and Other Communication Systems.

Entities that have a contract guard or response force, whose duties include alarm monitoring and response, must use portable two-way radios or other communication system(s) to facilitate immediate and real-time communications between the alarm monitoring station and the responding guard. Portable two-way radios will be tested regularly and be capable of reception over required distances and through obstructions present in high and maximum containment laboratories (such as heavy concrete walls), as well as two-way communication on the primary security channel from within critical buildings and structures; or an alternate means of communication will be provided. Portable two-way radios will contain sufficient battery capacity to operate for an 8 hour period at maximum expected duty cycle. Procedures for radio or battery exchange, or battery recharge, can be used to meet this requirement. Communication system logistics must account for biocontainment needs as well as communication needs (i.e., radios or batteries cannot come freely into or out of a containment laboratory).

t. Exit Inspections for Limited and Exclusion Zones.

Personnel, vehicles, and hand-carried items, including packages, briefcases, purses, and lunch containers, will be subject to random exit inspections to deter and detect unauthorized removal of HCBAs and information related to HCBAs from security areas.

u. Prohibited Articles.

The following articles are prohibited from entering HCBA areas, unless approved by the cognizant USDA local authority for physical security systems: any dangerous weapon, explosive, or other dangerous instruments consistent with DHS, ISC, *Items Prohibited from Federal Facilities*, that lists prohibited and controlled items allowed into Federal facilities, or material likely to produce substantial injury or damage to persons or property. Sites will, at a minimum, employ administrative procedures to prohibit these articles.

v. Visitor Logs.

Visitor Logs are required to be utilized and maintained at all USDA locations to document any visitors (non-USDA employees) visiting a facility. The Visitor Log can be either in paper or electronic format. Visitor Logs will be retained for at least a period of 1 year. In addition, visitors being escorted by security risk assessment approved personnel into registered select agent space will be required to sign in and sign out on a

Visitor Log pursuant to FSAP. These Visitor Logs will be retained for a period of 3 years pursuant to Federal Select Agent Regulations.

w. CCTV Technology.

(1) CCTV would be used to assist in monitoring access into limited, exclusionary, and other critical areas. CCTV cameras would be considered in the site security plan to assist in the monitoring of storage of biological agents or BSAT at high and maximum containment laboratories, or registered select agent space, such as freezers, coolers, and incubators.

(2) When implemented, the CCTV system, at a minimum, will be programmed to record on a 24 hour a day, 7 days a week basis (24x7) basis or programmed to record on motion detection and alarm activation. The system would be designed to retain video for a minimum of 30 calendar days up to a maximum of 45 calendar days or longer based on local budget and storage capabilities. The CCTV system would be integrated with IDS to provide "Hands-Free Alarm Call Up" and camera view presets. This allows the cameras to be automatically focused towards the breached area, while simultaneously allowing the responsible entity monitoring the system to view video in real time.

7. OPERATIONAL SECURITY PROCEDURES

a. Purpose.

(1) The objective of operational security is to ensure the safety of employees and Government assets by augmenting and supporting the physical security features that are in place, commensurate with a site-specific security assessment. This describes operational procedures that are intended to mitigate the risk of loss, theft or misuse of biological materials and secure information.

(2) Logical and necessary considerations for implementation would be given to the best practices listed in the remainder of this section:

b. Varied needs for authorized entry by visitors, lab workers, management officials, students, cleaning and maintenance staff, and emergency response personnel will be considered.

c. Mail screening and handling requirements would be evaluated based on a site-specific risk assessment. See DHS, ISC, *Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors*, 1st Edition.

d. The roles and responsibilities of all levels of management and programs will be clearly defined.

e. Describe the operational details of a site protective guard force or describe response requirements by local law enforcement based on a site-specific risk assessment, following practices in the DHS, ISC, *Best Practices for Armed Security Officers in Federal Facilities*, 2nd Edition.

f. Facilities are encouraged to coordinate with local medical, fire, police and other emergency officials when preparing incident response and security plans.

g. Operational procedures would describe the reporting and investigation of potential security breaches such as missing biological agents, unusual or threatening phone calls, or unauthorized personnel in restricted areas. Reporting to local law enforcement and FBI Weapons of Mass Destruction Coordinators for incidents concerning BSAT may be appropriate.

h. Describe the training programs to be instituted by the site's physical security manager that inform and educate individuals regarding their responsibilities within the laboratory and institution. Practice performance assurance (drills) or performance testing (exercises) would address a variety of scenarios such as loss or theft of materials, emergency response to incidents such as accidents and injuries, incident reporting, and identification of (and response to) security breaches.

i. Describe the development and conduct of security program audits and implementation of corrective actions as needed. Audit results and corrective actions would be documented as part of this initiative. The appropriate site manager would maintain records.

j. For assistance with planning or questions concerning operational security needs or requirements, contact the USDA Office of Safety, Security, and Protection, physicalsecurity@usda.gov, or phone: 202-720-2582.

8. CYBERSECURITY SYSTEMS PROCEDURES

a. Purpose.

This Section establishes the USDA policy for the security of high and maximum containment biological agent Information and Information Technology (IT) located at USDA high and maximum containment laboratory facilities or facilities with registered select agents.

b. Scope.

(1) This Section contains the set of USDA Information System Security requirements for USDA laboratories that work with or have the capacity to work with regulated biological select agents and toxins, or high and maximum containment biological agents, and other facilities as deemed appropriate. This section applies to

information and information systems or services such as cloud computing. It does not apply to physical containment provisions related to the biological agents possessed, used, or transferred to or from USDA high and maximum containment laboratories.

(2) It has become widely recognized that the American public and U.S. agricultural interests are ultimately safer with increased knowledge and scientific tools as important security elements of the overall scientific enterprise. Additionally, research and diagnostic activities are necessarily collaborative in today's scientific environment. Therefore, data intended for publication or public reporting is dealt with differently than other, non-public data related to the management and operations of the USDA.

(3) As cited below, Federal Information Processing Standards Publication (FIPS PUB) 199, *Standard for Security Categorization of Federal Information and Information Systems*, and National Institute of Standards and Technology (NIST), Special Publication (SP) 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, classify information as to its impact in three general categories: confidentiality, integrity, and availability. When considering information for "General Science and Innovation" and "Knowledge Creation and Management" (referred to below as "research data"), the assigned impact is low for confidentiality and availability, but moderate for integrity. This classification is a basic recognition that information of this sort is destined for public consumption and use but must be correct as it is disseminated to protect the reputation of the Department.

(4) Given the focus of these data on public dissemination in furtherance of the USDA's commitment to safe and secure science for the American public and U.S. agriculture, the overall protection scheme applied to research data must be designed to facilitate information flow and transit over, protection and archival activities.

(5) Conversely, the classification of what will be termed "diagnostic and regulatory data" is a mixture of low and moderate classifications, reflecting the occasionally sensitive nature of that type of data and the impact it can have if released early (e.g., before confirmation) or made public (e.g., inspection findings, confidential business information). For the purposes of this DM, data of these types will be considered "moderate" following NIST's "high water mark" strategy outlined in FIPS PUB 199.

(6) This distinction allows researchers and their high and maximum containment laboratory management to make an intentional risk management decision (as allowed by NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*) as to what information can be classified as research data, and what information is worthy of a higher level of protection, or what can be publicly disseminated and what is protected or archived.

c. Introduction.

(1) USDA high and maximum containment laboratories are reliant on technology to ensure the effective and efficient operations of facilities and to perform their missions.

(2) Laboratory information and information assets require appropriate risk-based controls to minimize hazards to confidentiality, integrity, availability, privacy, non-repudiation compromise, and unauthorized access to USDA information and information assets.

(3) USDA, DR 3540-003, *Security Assessment and Authorization* (A&A), requires that all information systems complete the A&A process to ensure that, based on the value of the information contained in the systems, the required security controls are in place, assessed, operating as intended and providing adequate security.

(4) The USDA's adoption of the NIST, SP 800-37, Revision 2, *Risk Management Framework (RMF) for Information Systems and Organizations*, *A System Life Cycle Approach for Security and Privacy*, provides operational details meeting requirements as set forth by the Office of Management and Budget (OMB), NIST and *Federal Information Security Modernization Act* (FISMA) requirements, codified at 44 United States Code (U.S.C.) § 3551 *et seq*.

(5) Each facility will have to evaluate their needs based on site-specific considerations and would perform a site-specific information security risk assessment, including a formal A&A of their information systems. In addition to the Information security requirements, select agent facilities may also require additional physical containment and protection requirements as specified by other regulations. Both the information security system(s) and physical protections at a high and maximum containment, (A)BSL 3, BSL-3, or select agent facility will be designed according to a site-specific information security risk assessment, which will evaluate data type (i.e., "research" or "diagnostic and regulatory") targets, adversary capabilities, consequences, and vulnerabilities.

(6) This site specific risk assessment is a key requirement that, in conjunction with other existing applicable regulations, will determine the graded protection strategies necessary to adequately protect government assets, as well as the necessary or recommended information security systems necessary to compliment the identified graded protection strategies.

(7) These information security systems may include, but are not limited to:

(a) Laboratory Information Management Systems (LIMS);

(b) BSAT Inventory Systems;

(c) Electronic Access Control Systems;

(d) Building Automation Control Systems;

(e) Building Environmental Control Systems;

(f) Laboratory Equipment;

(g) Laboratory Applications;

(h) Laboratory Network Infrastructure; and

(i) CCTV and Cameras.

(8) To resolve issues and address new initiatives, laboratory workers (e.g., end users) and management officials would meet with the Information Systems Security Manager (ISSM), system administrators, and laboratory management officials to ensure adequate flow of information on needs and requirements for systems from an end user's perspective within the limits of available technology. For example, the ISSM and system administrators would create a method to allow a researcher to transfer data from their system to another, external system that may have a different set of protections than those mandated by USDA (e.g., protected connections, transfer on a storage device). Additionally, those IT management officials would create a process to receive data from (possibly) unsecure systems, such as an independent computer system used for pre-screening data transfer devices that are brought back from conferences.

(9) The first step in managing risks is to determine security categories based on the types of information and information systems, as mandated by the FIPS PUB 199. For each type of information, the impacts to confidentiality, integrity, and availability are determined. The overall security impact categorization, however, is driven by the "high water mark." The highest of the three impacts determines the security categorization of the information system. This, in turn, determines the set of controls needed to protect the information and the system. Thus, when data must be highly accurate (that is, high integrity) and nearly always available (high availability), the system is categorized as high impact. By contrast, data or information intended for publication or public reporting must be correct (moderate integrity) but confidentiality and availability impacts would be low, leading to an overall categorization of moderate. In the case of high and maximum containment or select agent facilities, the physical security and environmental control systems are protecting repositories of select agents or HCBA. Therefore, the information that these systems generate, transmit, and store must similarly be protected from compromises such as tampering, unauthorized disclosure, or disruption.

(10) More controls are required for high systems than moderate systems; the required controls are identified in NIST, SP 800-53, Revision 5, *Security and Privacy*

*Controls for Information Systems and Organizations*. Based on the assessment of risk, the baseline set of controls can be supplemented with additional controls as well. For example, controls for tamper protection on physical access devices, incident handling of insider threats, or information spillage are not required in the high impact baseline, but depending on the outcome of the risk assessment, the facility may add these controls to the baseline. Each facility will establish their baseline set of information security controls tailored to site-specific considerations after performing a site-specific information security risk assessment and categorizing the various types of information and information systems.

d. Standards for Cybersecurity Controls.

While each facility will tailor the selected set of NIST, SP 800-53 controls resulting from the information and information system categorization and risk assessment, specific attention must be paid to the following topics and the controls associated with the topic.

e. Access control, Identification, and Authentication.

Each facility must implement controls to manage access to information and information systems, ensuring that only authorized personnel are permitted access. Each user must be uniquely identified and must employ multi-factor authentication in accordance with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*. Actions taken by privileged users such as system administrators will be logged. Remote access to moderate and high impact systems will be limited or denied, depending on the risk decision of the designated approving authority or information System Owner (SO).

f. Auditing.

Information systems will generate audit records that can support investigations of events and cybersecurity incidents. Audit records will be reviewed regularly, and anomalies will be investigated. Audit records will be protected from modifications.

g. Configuration Management and Maintenance.

The configuration of hardware and software will be properly controlled and managed. There will be an inventory and a baseline configuration for each element of the system. Systems will be hardened by, for example, applying more stringent configuration settings following guidelines such as NIST, SP 800-70, Revision 4, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*, NIST, Computer Security Resource Center (CSRC), *United States Government Configuration Baselines* (USGCB), and the Defense Information Systems Agency Security (DISA) Technical Implementation Guides (STIG). All maintenance on facility systems will be properly controlled.

h. System and Network Protections.

Tools and processes will be implemented to monitor systems and networks used by the facility, including physical and environmental control systems. Vulnerability scanning and mitigation of identified weaknesses on all systems must follow current guidance as established by DR3530-006, *Scanning and Remediation of Configuration and Patch Vulnerabilities*. Systems will also be scanned to ensure all devices on the network are accounted for inventory. Systems will be protected from malicious code using USDA-approved automated mechanisms. The network will be engineered to provide protection to information and IT assets, ensuring proper segmentation and other controls to minimize the risk of weaknesses or compromises of one information system allowing compromise of other systems. Depending on the security categorization of an information type, the information at rest and in transit will be protected with encryption technologies that meet FIPS PUB 140-3, *Security Requirements for Cryptographic Modules*.

i. Contingency Planning.

Each facility will develop and maintain contingency plans for system disruptions and designate and train responsible personnel to implement the plans. The contingency plans will be exercised annually, and updates and improvements made to the plans. In support of contingency plans, regular backups of important information such as the inventories of repository materials will be performed. The backed-up information will be stored apart from the system, preferably at a secure off-site location.

j. Incident Response.

Each facility must develop and maintain cybersecurity incident response plans consistent with the USDA's plan. Each facility must designate and train responsible personnel to implement the plans. The incident response plans will be exercised annually, and updates and improvements made to the plans.

k. Responsibility.

Consistent with RMF, SP 800-37 Revision 2, a SO must be identified and ultimately responsible for the laboratory information security; however, the physical security specialist, information technology specialists and information system security officer must support the SO on effectively implementing and managing a risk management framework to protect the confidentiality, integrity, availability, privacy, and non-repudiation of information and information assets.

l. Information Security Documentation.

USDA high and maximum containment laboratories must develop information security documents that include:

(1) This must include provisions to facilitate the flow, transfer, and dissemination of data deemed for public consumption (e.g., research data), and restriction of data deemed not for public consumption.

(2) Classification of data type – research or diagnostic and regulatory, in order to assign the correct protection scheme to different data that may be co-mingled on a single system.

(3) Laboratory Configuration Management Plan – the configuration management plan will inventory the specific high and maximum containment laboratory configuration items and describe the secure configuration and patching process used to effectively maintain the configuration items (i.e., operating system, applications, and database) to minimize the risk of compromise due to misconfiguration.

(4) Laboratory Incident Response Plan – DR 3505-005, *Cybersecurity Incident Management Procedures*, provides the specifications for USDA compliant Incident Response Plans. The incident response plan will outline the specific procedures related to the resolution of an information security event involving the compromise of high and maximum containment laboratory information and information assets.

(5) USDA high and maximum containment laboratory networks may be segmented: physically via a firewall; or virtually in its own virtual local area network. Networks that may be accessible to the Internet, whether directly or indirectly, must employ intrusion detection and prevention, data transmission encryption, network access control and application access control at a minimum. Security configuration for network devices will conform to NIST, SP 800-70 Revision 4.

m. High and Maximum Containment Laboratory and Laboratory Information Management Systems.

High and maximum containment LIMS operating systems will employ NIST, SP 800-70 Revision 4, where feasible to secure the operating system without compromising information system operations. Multi-factor authentication (e.g., USDA LincPass or approved USDA logical access alternative) will be used for logical access control to the information system and anti-virus software will be installed on the information systems. Systems that connect internally or externally will connect using FIPS PUB 140-3. Multi-tier LIMS (i.e., web tier, application tier, database tier) must communicate over a FIPS 140-3 connection.

n. Building Automation, Environmental, and Supervisory Control and Data Acquisition (SCADA) Information Systems.

(1) BSAT building automation, environmental, and SCADA information systems must employ NIST SP 800-70 where feasible to secure the operating system without compromising information system operations.

(2) Building automation and environment information systems that can be managed remotely represent a higher level of risk, therefore all remote access must be via Virtual Private Network (VPN) and use multi-factor authentication (e.g., USDA LincPass or approved USDA logical access alternative) for logical access. Additional elements of a graded information security protection plan may be implemented after a site-specific risk assessment.

o. CCTV, Cameras, and Digital Video Recorders.

Transmitting requirements and records retention for high and maximum containment spaces would be consistent with known and current standards derived from the NIST SP 800-70 Revision 4, the National Archives and Records Administration (NARA), *General Records Schedule (GRS), Transmittal 31*.

(1) Video footage would be transmitted using FIPS PUB 140-3 encryption.

(2) Storage to retain video footage would be provided to be compliant with the NARA, Office of Chief Records Officer, GRS 5.6: *Security Management Records*, Section 090, *Facility security management operations records*.

(3) In consideration of the above standards, 30 calendar days retention time of security camera video is required.

p. Laboratory Equipment.

High and maximum containment facility laboratory equipment (or the computers that control them) that is connected to the network would be maintained in accordance with all Departmental and Government standards. The system would have an Authorization to Operate (ATO) following RMF, SP 800-37 Revision 2 guidance, including annual reviews and assessments of security controls, and reauthorized following a 3-year cycle. If the equipment (or computers) cannot be effectively secured against identified threats and vulnerabilities, the vendor must be contacted, advised of the Federal high and maximum containment laboratory information security requirements, and required to provide a corrective action plan and roadmap for the remediation of the identified threats and vulnerabilities. Until resolved, the system would be isolated from the Local Area Network (LAN) where network traffic is blocked, preventing any Internet communication.

q. Physical Access Control Systems.

(1) High and maximum containment facility PACS would be maintained in accordance with all Departmental and Government standards. This system would be Authorized following RMF, SP 800-37 Revision 2 guidance, and reauthorized following an annual cycle.

(2) If the PACS cannot be effectively secured against identified threats and vulnerabilities, the vendor must be contacted, advised of the Federal high and maximum containment laboratory information security requirements, and required to provide a corrective action plan or roadmap for the remediation of the identified threats and vulnerabilities. Until resolved the system would be isolated from the LAN and any Wide Area Network Internet access.

(3) Basic safety and biosafety principles generally prohibit mobile devices, laptops, tablets, cellular phones, smartphones, and other electronic storage devices from entering high and maximum containment space. Because of their information security risks, this prohibition also includes peripheral devices such as Universal Serial Bus (USB) storage devices (commonly referred to as flash or thumb drives). However, laboratory management officials can approve and document such devices on a case-by-case basis (for example, smart phones may be kept under Personal Protective Equipment (PPE) for emergency communications, electronic notebooks, tablets, or cameras can be retained for inspection purposes).

(4) Additionally, authorized system administrators and laboratory management officials must work together to establish objective procedures, with clear classification criteria, that facilitate the flow of research data from protected systems to and from external systems.

r. At a minimum, the below situations must be addressed:

(1) Sending pre-publication information (e.g., presentation slides, images) to collaborators, conference organizers, or other concerned parties when the files exceed email size limitations.

For example, a USDA-authorized secure Federal Risk and Authorization Management Program (FedRAMP) certified cloud platform for registered users to transfer large files to external users.

(2) Interchanging raw research data with external servers securely for archiving or external analysis (e.g., sequence data to GenBank (See Appendix B, *Definitions*), microarray data to private pathway analysis companies).

For example, establishing an interconnection security agreement process that facilitates data transfers to external servers.

(3) Receiving data on a USB storage device for downloading to a United States Government (USG) computer system (i.e., a USB from a conference with both valuable data as well as a virus on it).

(a) For example, a pre-scan station for virus cleaning of external devices for connection to the network.

(b) Any other locally applicable issues at the intersection of data protection and data flow that are identified during the site-specific risk assessment.

9. PERSONNEL SECURITY PROCEDURES

a. This section describes the personnel security program requirements for USDA and non-USDA personnel requiring access to specific high and maximum containment, Limited or Exclusion Areas within a facility where work at BSL3 or higher level of containment is conducted.

b. The name was also changed to "personnel security" to reflect this new focus, and also to remove confusion with the "pre-access suitability assessment of persons" required in FSAP for workers with access to T1 select agents and toxins.

(1) Purpose.

(a) Describe the personnel security program requirements for USDA and non-USDA personnel requiring access to high and maximum containment locations, facilities, biological agents, and BSAT to;

(b) Ensure appropriate levels of protection against unauthorized access, theft, diversion, or loss of custody of biological agents or BSAT at high and maximum containment laboratories, or registered select agent space, as regulated by the FSAP. This includes loss or theft of information related to these biological agents or BSAT and other acts that may cause unacceptable adverse impacts on national security or on the health and safety of USDA employees, the public, U.S. animal and plant health or products, or the environment;

(c) Ensure, based on a site-specific personnel security risk assessment, effective planning, and prudent application of resources to establish graded protection, including operational procedures and administrative controls;

(d) Provide guidance, based on a site-specific personnel security risk assessment, to develop a written security plan that addresses the provisions of this DM; and

(e) Instruct those entities that possess, use, or transfer BSAT to comply with applicable regulations (7 CFR § 331 (Plant); 9 CFR § 121 (Animal) and 42 CFR § 73 (Human)).

(2) The "Tier" designations for background investigations below come from the *Federal Investigative Standards* (revised in 2012 by Office of Personnel Management (OPM). They are not equivalent to the T1 designation defined in the select agent regulations.

(3) In accordance with 5 CFR § 1400, *Designation of National Security Positions* and 5 CFR § 731, *Suitability*, all positions must be evaluated for impact to national security or impact to integrity.

(4) An adjudicated National Security background investigation evaluates an individual's potential to impact National Security. In addition, the National Security investigations ensure eligibility for access to classified national security information (CNSI) and include a "continuous evaluation" component, consistent with Office of the Director of National Intelligence (ODNI) Security Executive Agent Directive 6, *Continuous Evaluation*).

c. Tier Designations.

T1 is the minimum background requirement for all employees and contractors. T2 and 4 background investigations are considered Public Trust and address the personnel suitability and character. T3 and 5 background investigations fall into the national security classification.

Tier categories:

(1) T1 is the investigation for positions designated as low-risk, non-sensitive. It is also the minimum level of investigation for a final credentialing determination for physical and logical access. T1 investigations are requested using the Standard Form (SF) 85;

(2) T2 is the investigation for non-sensitive designated as moderate risk Public Trust positions. T2 investigations are requested using the SF 85P. It is recommended that all employees and contractors requiring access to containment facilities undergo a T2 investigation at a minimum;

(3) T3 is the investigation required for positions designated as non-critical sensitive or requiring eligibility for "L" access or access to Confidential or SECRET information. T3R is the reinvestigation product required for the same positions. The SF 86 is used to conduct these investigations;

(4) T4 is the investigation required for positions solely designated as high risk Public Trust. The T4R is the reinvestigation product required for the same positions. The SF 85P is used to conduct these investigations; and

(5) T5 is the investigation required for positions designated as critical sensitive, special sensitive, or requiring eligibility for "Q" access or access to TOP SECRET or Sensitive Compartmented Information. The T5R is the reinvestigation product required for the same positions. The SF 86 is used to conduct these investigations.

d. Personnel Security Investigations and Position Designations.

Following OPM's instructions, the following investigations will be conducted as described for the position designation.

(1) At a minimum, a T1 investigation (formerly a National Agency with Inquiry) is required by all USDA workers, with or without access or potential access to HCBA, regardless of their job classification or duty station. Results must be released to DCSA before the work start date. A fingerprint check alone is not sufficient.

(a) Additionally, all workers with unescorted access to BSAT must submit information and successfully complete a SRA conducted by the FBI-CJIS before access approval is granted. The SRA approval must be renewed every 3 years, is conducted by the FBI, but is granted by the FSAP.

(b) This designation, along with the SRA granted by the FSAP for all select agent workers, and the additional personnel suitability program requirements for workers with access to T1 BSAT, are the baseline requirements for USDA personnel.

(c) Certain job classifications or duty stations who have the authority to influence or direct the work of others, may have additional need to see sensitive or classified information may be deemed higher risk by local leadership. However, all employees must successfully complete this level of background investigation before access is granted to biological agents that require high and maximum containment (Biosafety Level (BSL) 3 or higher) or the space where they are stored or manipulated. For example, office workers, janitors or other support personnel who do not have access to the high and maximum containment laboratory (but could potentially access such spaces as insiders) would be classified at this level as well.

(2) A T2 Investigation (formerly a Moderate Background Investigation) may be required for some personnel at the discretion of the local management team (e.g., Laboratory Director, Center Director, or Research Leader). This level of investigation is not sufficient for access to classified information, but may be used for access to spaces, areas, or agents that local leadership deems sensitive. The focus of such an investigative process is personnel suitability and not initial and ongoing access to sensitive information.

(3) A T3 Investigation (which may be adjudicated to a National Security Clearance at the SECRET level) may be required for certain work duties that involve access to CNSI. For example, second-line supervisors, Laboratory Directors, Center Directors, and similar management officials that need access to classified information would require this clearance level. Additionally, a T3 investigation subjects the employee to continuous evaluation of certain sensitive information that could make them susceptible to coercion (e.g., financial information, criminal

activity). Local leadership may deem such elements of this clearance level desirable for those personnel who have the authority to influence or direct the work of others.

(4) A T4 investigation (formerly a Background Investigation (BI)) is a higher-level examination that is similar in character to a T2 investigation such that it is focused on a "point in time" assessment of suitability and does not involve any third-party continuous monitoring. For example, second-line supervisors, Laboratory Directors, Center Directors, and similar management officials may be classified here by local leadership.

(5) A T5 investigation (eligible for adjudication to a National Security Clearance at the TOP SECRET level) may be required for certain work duties that involve access to CNSI. For example, Laboratory Directors, Center Directors, Administrators or their staff, and similar management officials that need access to classified information would require this clearance level. Additionally, a T5 investigation subjects the employee to continuous monitoring of certain sensitive information that could make them susceptible to coercion (e.g., financial information, criminal activity).

e. Pre-employment.

(1) Recruitment announcements will notify all candidates for permanent and non-permanent positions that the position is located within a high and maximum containment area and appointment to the position is subject to a favorably adjudicated background investigation, and possibly ongoing evaluation as well.

(2) A favorably adjudicated pre-employment Special Agency Check must be completed for all positions with access to high and maximum containment biological agents (including BSAT) prior to appointment.

f. Location Considerations for T2 and 4 Decisions.

This section describes the variables that locations should consider as they decide on positions and background investigations based on position designations. Similar to the graded protection model used in physical security, it is helpful in creating a site specific risk assessment approach that is reviewed by the agency and Department. Modifications should account for the operational realities at the location or entity level while allowing review processes to input high level considerations as necessary and potentially harmonizes these procedures with the physical security requirements.

(1) All USDA employee positions with access to HCBA (including BSAT) will be evaluated by Human Resources (HR) to provide an initial determination of clearance requirements.

(2) HR will send initial determination to the local management Security Review Committee (SRC; individual agency locations with oversight for that respective agency, e.g., Laboratory or Center Directors, Associate Directors, Safety and Security staff, or supervisors). That committee will assess the initial determination and either validate it so that HR can proceed or provide a justification for either a downgrade or upgrade in the determination based upon a graded protection approach (similar to physical security) as well as the site-specific risk assessment. HR will attach such justifications to the (PD) to be used in future determinations as personnel turn over.

(3) Factors that must be considered in this assessment include the following: whether personnel have unescorted physical access to HCBA (i.e., defined as the ability to hold, touch, or manipulate HCBA); and whether that access could potentially affect the public reputation, integrity, or efficiency of services offered or delivered from the location, agency, or Department. Local physical security measures and other local or operational factors can and would inform this assessment.

(4) The assessment will generally be considered specific to the position type, physical access potential, and the work conducted, and need not be re-evaluated if personnel leave employment and others are hired for similar duties and work. However, any significant change in the safety or security risk of the work performed (e.g., work with a new HCBA, new facilities with physical security elements, moving from in vitro studies to in vivo studies) would trigger a re-evaluation of the risk classification of the position.

(5) Additionally, any member of the SRC, or the agency or Departmental review authorities, can re-open an assessment at any time with or without cause to re-evaluate the classification of any position with access to HCBA.

(6) New appointees may be assigned duties outside the high and maximum containment area or may have access to a high and maximum containment area only if escorted into the high and maximum containment area by a staff member who has a favorably adjudicated security investigation and appropriate facility authorization.

(7) Personnel security risk assessments would be grouped rationally (e.g., by access potential and type of work) and submitted for agency review. Agency level review may be structured independently by each location, and may include the following members of security, safety, and upper management:

(a) APHIS:
Security – Security Branch (301) 436-3144
Biosafety – (301) 436-3117
Personnel Security – (612) 336-3560

(b) ARS:
Security – HSD (202) 441-6543 or

ARSHomelandSecurityDivision@usda.gov
Biosafety – Office of National Programs (301) 504-4700 or
AgencyBiosafeyProgram@usda.gov
Personnel Security – (301) 504-1338 or
ARSPersonnelSecurity@usda.gov

(c) FSIS:
Security – Security and Emergency Preparedness (202) 690-6606
Biosafety – (706) 546-2380
Personnel Security – (612) 659-7054

(8) Personnel who have been granted a SECRET or TOP SECRET clearance level may be authorized unescorted access to the high and maximum containment areas within the facility upon receipt of their security clearance if approved by an institutional official or designee who controls access to HCBA other than BSAT, or the RO for the entity who controls access to BSAT (if those personnel have an appropriate SRA-approval).

(9) However, personnel with a SECRET or TOP SECRET clearance will not be granted unescorted access to areas where viable HCBA (including BSAT) are stored or used (e.g., laboratory spaces) unless authorized by the institutional official or designee who controls access to HCBA other than BSAT, or the RO for the entity who controls access to BSAT. Such access would require an SRA-approval before such access to BSAT was granted.

g. Investigative Standards.

In accordance with the 5 CFR Part 731, *Suitability* and 5 CFR Part 732, *National Security Positions,* individuals occupying a moderate, high, critical sensitive, or special sensitive, position will be reinvestigated at least once every 5 years and as event-driven, and subject to implementing guidance.

h. Non-USDA Personnel.

Includes personnel from universities, collaborators, contractors, students, visitors, and seminar attendees, etc. If these individuals meet the same standards that apply to USDA employees (as outlined above), they may have unescorted access to areas where HCBA (including BSAT) are stored upon written approval by the RO (for access to BSAT) or the institutional official or designee for access to viable HCBA other than BSAT. Non-USDA personnel without the appropriately adjudicated background investigation must be escorted at all times in areas where HCBA are stored or used by staff members who have a favorably adjudicated personnel security investigation and appropriate facility authorization.

i. Reporting Requirements.

(1) Individuals, coworkers, and supervisors of persons with access to viable HCBA, (including viable BSAT) are required to report issues or situations that could pose a threat to the health and security of personnel, the community, or the environment, or the integrity of the research or diagnostic activities. Reports must be made (at a minimum) to the next level supervisor, and to the RO (for BSAT).

(2) It is the responsibility of all personnel to ensure reports are communicated to the appropriate response personnel, not necessarily to complete the reporting themselves. For example, leaving a phone message for a supervisor who is out of town is not sufficient to this duty, but talking to them in person or on the phone is sufficient because each supervisor would be trained to pass that information to the appropriate office or official. Reportable events include (but are not limited to) observation or knowledge of the following:

(a) Unlawfully carrying weapons (or carrying weapons in violation of institutional rules);

(b) Providing false information on applications or other formal institutional documents;

(c) Unauthorized work performed by the individual in the facility during off-hours;

(d) Intentional sabotage of research;

(e) Physical violence or threats toward another co-worker;

(f) Acts of vandalism or property damage;

(g) Intentional violation of safety or security procedures;

(h) Suspicious activities that may be criminal in nature; and

(i) Other safety or security incidents or violations.

(3) Individuals (including visitors with unescorted access to high and maximum containment areas) who do not report behaviors of concern may be subject to disciplinary action up to and including removal of access to restricted areas and termination of employment. Visitors who are not USDA employees but have unescorted access to high and maximum containment areas must be informed of this requirement during their facility training.

(4) Nothing in this policy precludes Agency Heads, Administrators, Center Directors, Laboratory Chiefs or Directors, Research Leaders, Lead Scientists or Supervisors

from implementing additional reporting requirements as appropriate for the work situation under their leadership.

j. Insider Threat Awareness.

(1) Insider threat awareness is a critical component of our country's National Security Program, particularly with respect to classified information. From a practical standpoint, it could also include proprietary information or trade secrets that refer to the BSAT itself as well as non-classified information, physical items, or equipment. The Select Agent Program also references a requirement for Insider Threat Awareness training for those with access to T1 Agents.

(2) Development and implementation of these programs at USDA locations is complex and far-reaching. This section does not attempt to make you an expert, but rather to give you general information and references. If at any time you have any concerns or questions, please contact either your RO or consult the FSAP CDC document on *Suitability Assessment Program Guidance*.

(3) Similar to the terminology that crosses over above (e.g., T1 personnel security investigation versus T1 select agents), there are many conflicting and confusing terms in this area. Officials from OPM discuss continuous evaluation of personnel from a human resource, workplace, violence, personnel, and suitability perspective.

(4) Representatives of the USDA OHS oversee USDA's insider threat program related to information and materials classified for national security reasons. Personnel from the FSAP provide guidance on suitability assessment programs for those with access to T1 select agents.

(5) There are many similar requirements related to personnel security and suitability that may or may not overlap, may or may not have contradictory requirements or initiatives, and may or may not have agency or Departmental level resources for Location staff to access. Personnel needing support in this area would contact their agency's security, biosafety, or personnel security staff members for advice and guidance in these matters.

(6) Keep in mind that there could be unanticipated elements of personnel security that need to be addressed in the development of local standard operating procedures (SOP) to ensure adequate response to incidents. For example, management officials would define the ability of contracted security guards (versus Federal Protective Services personnel) to detain or arrest employees or visitors that may be committing crimes. Contacts with other resources include:

(a) APHIS-EMSSD:
Security – Security Branch: (301) 436-3144
Biosafety: (301) 436-3117
Personnel Security: (612) 336-3560

(b) ARS:
Security – HSD: (202) 441-6543 or
ARSHomelandSecurityDivision@usda.gov
Biosafety – Office of National Programs: (301) 504-4700 or
AgencyBiosafeyProgram@usda.gov

Personnel Security: (301) 504-1338 or
ARSPersonnelSecurity@usda.gov

(c) FSIS:
Security – Physical Security: (202) 603-2048
Biosafety: (706) 546-2380
Personnel Security: (612) 659-7054

(7) While a national security clearance is not required for access to HCBA (including BSAT), if personnel hold a security clearance, they may have additional reporting requirements. These requirements can be found at OHS, *Cleared Employee Reporting Requirements*.

(8) Reporting requirements for national security clearance holders are described in DR 3440-001, *USDA Classified National Security Information Program* and its associated DM 3440-001, *USDA Classified National Security Information Program*. According to the USDA Insider Threat Program, DR 4600-003, *USDA Defensive Counterintelligence and Insider Threat Programs* concerning classified information must be reported to cnsis@usda.gov and insider@usda.gov . Further information on both reporting requirements can be found on the OHS, *Personnel and Document Security Division's (PDSD)* home page. Individuals can report potential insider threat issues online at OHS *Insider Threat Program* home page. For additional information, you may email the Insider Threat Coordinator at insider@usda.gov.

## 10. INCIDENT RESPONSE PLAN

a. Purpose.

This section describes the requirements for responses to specific types of incidents in order to protect personnel and facilities, as well as secure biological agent holdings. The CDC, *Incident Response Plan Guidance*, *7 CFR Part 331, 9 CFR Part 121, 42 CFR Part 73*, available from FSAP and will be a useful resource in developing a viable Incident Response Plan (IRP).

b. Assessment Criteria.

(1) Measurement of the success or failure of an incident response plan will necessarily be performance based, as each location will have a variable set of threats assessed, response resources identified, and appropriate response protocols defined.

(2) Performance metrics for a successful IRP would include the following criteria:

(a) Focus on protecting human life before property; then a focus on protecting animal life before other assets;

(b) Focus on impact to the high and maximum containment laboratory and other high-hazard areas in the context of the overall facility;

(c) Documented collaboration between entity leadership and local responders;

(d) Location staff and local responder joint participation in entity training, drills, and exercises, including consultation during the planning stages of such activities; and

(e) Comprehensive scope of response that considers the primary effect of the hazard, secondary effects that can be reasonably predicted, and the effect of the hazard on the people who work at the facility.

c. Required Incident Response Plan Elements.

(1) Site Specific. The incident response plan must be site-specific, which means that each section of the written plan must reflect a risk identified in a site-specific risk assessment. Also, the plan must accurately reflect the entity's current policies and procedures related to incident response.

(2) In developing the written incident response plan, the entity needs to factor in specific consequence assessments for all hazards present, including (but not limited to) high and maximum containment biological agents, volatile or reactive chemicals, environmental hazards (e.g., oil or propane tanks for emergency generators (Note: This is not an exhaustive list and each facility may have different hazards)), or the sociopolitical sensitivities surrounding animal and plant care and use (e.g., "animal rights and anti-Genetically Modified Organism activists" as a threat).

Note: Documents required by FSAP would be acceptable to meet this requirement.

(3) The incident response plan must include responses to the following types of incidents:

(a) Biocontainment and facility incidents, including but not limited to a loss of negative airflow;

(b) Spill response procedures, including small and large spills;

(c) Security breach, suspicious activity, suspicious person, alarm activation, or civil disturbance;

(d) Inventory discrepancy;

(e) Theft, loss, or release of a high and maximum containment biological agent;

(f) Cybersecurity breach (i.e., Information systems breach);

(g) Animal emergencies (if applicable), including escape of infected animals or arthropods;

(h) Pollen or spore drift;

(i) Workplace violence, including "active shooter" planning;

(j) Bomb threats;

(k) Suspicious packages;

(l) Severe weather, natural disasters, minimally including a risk assessment for: earthquake, hurricane, flood, tornado, severe storms; and

(m) Other emergencies identified during the site-specific risk assessment, minimally including fire, gas leak, explosion, and power outage.

(4) The plan must include the following categories as relevant to site-specific risk:

(a) Personnel safety and health;

(b) Containment (including "secure or destroy" provisions for incidents during laboratory work;

(c) Inventory control during and after an incident (e.g., audit requirements);

(d) Initial notification of managers and responders;

(e) Site security and control;

(f) Drills and exercises, and documentation of response and follow-up;

(g) Implementation of the Incident Command System at the entity (i.e., roles and responsibilities, contact information, authorities to trigger response events such as gross decontamination). See the Federal Emergency Management Agency (FEMA), *National Incident Management System (NIMS)*, Third Edition;

(h) Coordination during the incident with local first responders;

(i) Procedures for entity personnel performing rescue or medical duties (e.g., training, protocols for emergency evacuation from high and maximum containment laboratories);

(j) Emergency medical treatment and first aid, especially in the high and maximum containment laboratory;

(k) Decontamination procedures following an incident (e.g., whole room or gross decontamination protocols); and

(l) Required notifications of Departmental, Mission Area, and agency leadership via line management reporting procedures, and other local or Federal agencies (e.g., the FSAP), and other applicable reports (e.g., DHS, Federal Protective Service, the USDA Office of the Inspector General (OIG)).

11. TRAINING

All training results outlined below must be tracked in the agency training database (i.e., AgLearn).

a. Line Responsibilities.

(1) Center Director, Laboratory Chief or Director, or Research Leader.

These personnel must individually or collectively ensure implementation and confirm the effectiveness of biosafety and security at their facility or institute. Must provide resources for training, implementation, and monitoring of safety and security policies and programs. Must determine the level of competency of trained individuals on a regular basis, using a combination of mentorship reporting or performance verification standard testing.

(2) Location Biosafety, Biosecurity, Quarantine Officer, Collateral Duty, or Biosafety Officer.

These personnel must individually or collectively ensure and verify effective biosafety implementation at their facility or institute. They must work with local line managers to ensure laboratories have validated biosafety programs and laboratory personnel are adhering to the Department, agency, or local site policy on

biosafety programs and biological agent inventories. Primary or collateral duty biosafety officers serve as a resource for biosafety program implementation, quality control, biosafety inspections, and training.

(3) Location Information Management Director System Administrator.

These personnel must individually or collectively provide resources for training, implementation, and monitoring of cybersecurity and information security policies and programs. Must coordinate with the ISSM on all information security issues.

(4) Location Physical Security Specialist, Manager, or Collateral Duty Security Specialist.

These personnel must individually or collectively ensure effective security implementation at their facility or institute. They must work with local line managers to ensure laboratories are adhering to Department, agency, and local site on security. They must act as a resource for security program implementation, quality control, security inspections, and training.

(5) Scientists.

These personnel must individually or collectively ensure effective safety and security implementation at their facility or institute. They must ensure that all biological agents used in their laboratories are entered in the repository database and that repository records are current and accurate reflect the materials on hand. They must ensure the responsible use of biological agents and BSAT. They must act as a resource for safety, biosafety, and security program implementation, quality control, safety and security inspections, and training.

(6) Supervisors and Managers.

They must provide resources for training, implementation, and monitoring of biosafety and security policies and programs.

(7) Escort.

They must be capable of executing appropriate safety and security protocols. Must provide (or verify that training was provided in the last year) visitor training to the unapproved person on the safety and security risks they will encounter, commensurate to their exposure to such risks.

b. HQ Roles and Responsibilities.

(1) Department, Agency, and HQ ISSM.

The ISSM will specify the details of a training program inclusive of appropriate training in vulnerabilities, threats, protection strategies, and respective organizational and personal responsibilities in relation to cybersecurity. They will be responsible for developing tools (e.g., training modules) for use by location staff to institute the mandated training programs.

(2) Department, Agency, and HQ Leadership.

These personnel must individually or collectively ensure implementation and confirm the effectiveness of the training programs and activities described in this section. They must provide resources for training, implementation, and monitoring of safety and security policies and programs.

c. Safety, Biosafety, and Related Issues.

The site's safety staff must work collaboratively to establish training programs that:

(1) Inform and educate individuals regarding their responsibilities regarding safety, biosafety, and other required elements within the laboratory and institution;

(2) Includes principles of containment, biological and agricultural risk assessment, PPE donning and doffing, etc.;

(3) Conduct annual performance assurance (drills) or performance testing (exercises) that addresses issues such as:

(a) A variety of scenarios such as release of materials, spills, etc.;

(b) Emergency response to incidents such as accidents and injuries;

(c) Incident reporting methods; and

(d) Criteria for identification of (and response to) biocontainment breaches.

(4) Provide training to affected personnel on the implementation and ongoing management of the recommendations of the site specific biological and agricultural risk assessment; and

(5) Ensure that employees attend other (i.e., Occupational Safety and Health Administration (OSHA)) required trainings with biosafety elements before work is begun:

(a) Bloodborne biological agents;

(b) Respiratory Protection Program; and

(c) Hazard Communication and Chemical Hygiene.

d. Inventory.

The site's biosafety officer and physical security manager (and RO, where applicable) must collaborate to establish training programs that:

(1) Inform and educate individuals regarding their responsibilities within the laboratory and institution;

(2) Includes criteria for initiating an inventory audit, how to conduct audits, required depth of audits in different situations, etc.; and

(3) How to report results of inventory, including maintaining USDA-HQ level inventory databases (e.g., NBATI).

e. Physical and Operational Security.

(1) Physical Security.

The site's physical security manager (and RO, where applicable) must establish training programs that:

(a) Inform and educate individuals regarding their responsibilities within the laboratory and institution; and

(b) Conduct annual performance assurance (drills) or performance testing (exercises) that addresses issues such as:

1 A variety of scenarios such as loss or theft of material;

2 Emergency response to incidents such as accidents and injuries;

3 Incident reporting methods;

4 Criteria for identification of (and response to) security breaches; and

5 Provide training to affected personnel on the implementation and ongoing management of the recommendations of the site-specific security assessment.

(2) Access Control.

Access control and intrusion detection will be managed by authorized USDA personnel qualified and trained on the local access control system.

(3) Operational Security.

Personnel must be adequately trained and familiar with regulatory and institutional procedures. The roles and responsibilities of all levels of management and programs will be clearly defined. Guards or protective forces must be trained in location procedures specific to their roles and responsibilities.

(4) High and Maximum Containment Laboratory Information Security Training.

All users of Government-owned computer must complete Annual Information Security Awareness training, see DR 3545-001, *Information Security Awareness and Training Policy*. High and maximum containment Information Security Training for all formally authorized system administrators must also be conducted. This training must be provided by the Laboratory Director, or designee, to affected staff – there is no agency-level training that covers these elements. This training is in addition to other high and maximum containment training.

(5) Cybersecurity.

The specialized training for system administrators would include the following sections at a minimum:

(a) Basic IT Security Awareness training (AgLearn);

(b) DM 9610-001 high level overview;

(c) Information asset security categorization;

(d) Physical security of high and maximum containment information and information assets;

(e) Physical Access Control to high and maximum containment secured space;

(f) Logical Access Control – Protecting access credentials, reporting lost or compromised credentials;

(g) Personnel Security – Reporting of suspicious person or activities;

(h) Inventory control – Prevention of unauthorized alteration or compromise of inventory records;

(i) Information systems control;

(j) Formal agreements to control external connections to facility security systems;

(k) Processes to grant authorized and authenticated users to access information, files, and equipment;

(l) Implement malicious code preventative controls; and

(m) General training for laboratorians (e.g., end users) and management officials.

(6) Training content will be decided annually by the ISSM, system administrators, and laboratory management officials to ensure adequate flow of information on needs and requirements for systems from an end user's perspective.

At a minimum, training for laboratorians would include:

(a) Basic IT Security Awareness training (AgLearn);

(b) DM 9610-001, high level overview; and

(c) USDA Insider Threat Awareness.

(7) The site's biosafety officer and physical security manager (and RO, where applicable) must collaborate to establish training programs that:

(a) Inform and educate individuals regarding their responsibilities within the laboratory and institution;

(b) Include criteria for initiating an incident response, initial response expectations, etc.;

(c) Include FEMA training modules on Incident Command System (if applicable); and

(d) Include procedures for entity personnel performing rescue or medical duties (e.g., training, protocols for emergency evacuation from high and maximum containment laboratories);

(e) Conduct annual performance assurance (drills) or performance testing (exercises) that addresses issues such as:

1 A variety of scenarios such as power loss, loss of primary containment, spills, etc.;

2 Incident reporting methods; and

3 Incident follow-up and review procedures.

f. Performance Verification or Mentoring in the Laboratory or Laboratory Support Function.

(1) The level and type of performance verification required for training activities will be decided with a risk-based criticality assessment. This assessment must allow for the practicality of testing on the tasks, information, and skills addressed in training. Each institution that has BSL3 equivalent or above facilities would institute a performance-based verification of knowledge, skills, and abilities needed for high and maximum containment operations.

(2) Examples of performance verification activities include but are not limited to:

(a) Regular review of competencies (e.g., Morbidity and Mortality Weekly Report(s) on Competencies);

(b) Development of performance verification methods such as mentorship, hands-on testing, observation, and reporting by supervisor or designee;

(c) Required review and retraining after any incident or near-miss or deviation from SOP; and

(d) Specified number of hours required in high and maximum containment laboratory before unescorted access.

12. ROLES AND RESPONSIBILITIES

a. The USDA Agency Administrator, or their delegated responsible staff, will:

(1) Develop, publish, and actively maintain policies, regulations, and compliance requirements for biosafety, biosecurity, physical security, incident response, personnel suitability, and information security, including actively providing channels for agency input into and approval of the same.

(2) Provide management and oversight activities as required to ensure effective biosafety, biosecurity, physical security, incident response, personnel suitability, and information security program implementation:

(a) Reviewing and monitoring compliance to established policy requirements and standards with minimal disruption to business functions or mission requirements; and

(b) Reporting compliance and deviations to OMB as necessary.

b. Agency and Staff Office officials will:

(1) Implement the policies and procedures required to implement by this DM;

(2) Develop internal procedures and controls in support of this policy and reviewing existing internal procedures and controls for support of this policy;

(3) Establish effective communication between internal stakeholders and an identified Point of Contact in the Department and agencies;

(4) Incorporate the policies, requirements, and standards into agency and staff office Capital Planning and Investment Control processes;

(5) Provide resources for appropriate training programs, including developing tools (e.g., training modules) for use by location staff to institute the mandated training programs; and

(6) Direct random reviews of materials accountability records.

c. Center Director, Laboratory Chief or Director, Research Leader, or their delegated responsible staff (as appropriate) will:

(1) Individually or collectively ensure effective biosafety, security, and incident response implementation at their facility or location, including access control;

(2) Provide resources for implementation of a robust safety and security program, including, but not limited to, training on, and monitoring of, safety and security policies and programs;

(3) Determine and document the level of competency of trained individuals on a regular basis;

(4) Maintain a current, centralized master database for materials accountability;

(5) Ensure applicable Departmental, agency, and required regulatory reporting requirements are completed in a timely fashion; and

(6) Assume or delegate the role of Incident Commander (IC) when necessary, consistent with HSPD-5, *Management of Domestic Incidents*, and HSPD-8, *National Preparedness*.

d. PIs, Lead Scientists, or their delegated responsible staff as appropriate will:

(1) Individually or collectively ensure effective safety, biosafety, security, and incident response implementation at their facility or institute, including access control;

(2) Maintain materials inventory and accountability records and ensure that such records are verifiable in a timely fashion; and

(3) Ensure applicable Departmental, agency, and required regulatory reporting requirements are completed in a timely fashion.

e. Any and all location staff with programmatic duties for safety or security such as Location Biosafety, Biosecurity, Quarantine Officer, Collateral, Duty Safety Officer, Personnel Suitability (Human Resources) Specialist, Physical Security Specialist, Information Management Director, and System Administrator will:

(1) Individually or collectively ensure effective biosafety, biosecurity, personnel suitability, physical security, incident response, and information security implementation at their facility or location;

(2) Work with local line managers to ensure laboratories are adhering to Department, agency, and site policy on biosafety, biosecurity, personnel suitability, physical security, incident response, information security programs; and

(3) Serve as a resource for biosafety, biosecurity, personnel suitability, physical security, incident response, information security program implementation, quality control, inspections, and training.

f. All USDA staff will:

(1) Adhere to and actively participate (as appropriate) to the requirements outlined in this DM to ensure effective biosafety, biosecurity, personnel suitability, physical security, incident response; and information security implementation at their facility or location; and

(2) Work with local line managers as appropriate to support their locations adherence to Department, agency, or site policy on biosafety, biosecurity, personnel suitability, physical security, incident response, and information security programs.

## 13. INQUIRIES

Address inquiries concerning this DM to the ARS HSD, via email to the ARSHomelandSecurityDivision@usda.gov mailbox.

-END-

# APPENDIX A

## ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| A&A | Assessment and Authorization |
| ABSL | Animal Biosafety Level |
| APHIS | Animal and Plant Health Inspection Service |
| ARS | Agricultural Research Service |
| ATO | Authorization to Operate |
| BI | Background Investigation |
| BMBL | Biosafety in Microbiological and Biomedical Laboratories |
| BSAT | Biological Select Agents and Toxins |
| BSC | Biological Safety Cabinet |
| BSL | Biosafety Level |
| CCL | Commerce Control List |
| CCTV | Closed Circuit Television |
| CDC | Centers for Disease Control and Prevention |
| CFR | Code of Federal Regulations |
| CJIS | Criminal Justice Information Services (FBI component) |
| CNSI | Classified National Security Information |
| CSRC | Computer Security Resource Center |
| CUI | Controlled Unclassified Information |
| DG | Departmental Guidebook |
| DHS | Department of Homeland Security |
| DISA | Defense Information Systems Agency |
| DM | Departmental Manual |
| DNA | Deoxyribonucleic Acid |
| DR | Departmental Regulation |
| EMSSD | Emergency Management, Safety, and Security Division (APHIS component) |
| EO | Executive Order |
| ePACS | Enterprise Physical Access Control System |
| FBI | Federal Bureau of Investigation |
| FedRAMP | Federal Risk and Authorization Management Program |
| FEMA | Federal Emergency Management Agency |
| FIPS PUB | Federal Information Processing Standards Publication |
| FISMA | Federal Information Security Modernization Act |
| FSAP | Federal Select Agent Program |
| FSIS | Food Safety and Inspection Service |
| FSL | Facility Security Level |
| GenBank | Genetic Database |
| GRS | General Records Schedule |
| HCBA | High Containment Biological Agent |
| HCPNA | High Containment Pathogenic Nucleic Acids |
| HEPA | High Efficiency Particulate Air |
| HQ | Headquarters |

| | |
|---|---|
| HSD | Homeland Security Division (ARS component) |
| HSPD | Homeland Security Presidential Directive |
| IC | Incident Commander |
| IDS | Intrusion Detection System |
| IRP | Incident Response Plan |
| ISC | Interagency Security Committee |
| ISSM | Information Systems Security Manager |
| IT | Information Technology |
| LAN | Local Area Network |
| LIMS | Laboratory Information Management System |
| NA | Nucleic Acid |
| NARA | National Archives and Records Administration |
| NBATI | National Biological and Toxin Inventory (formerly the National Pathogen Inventory) |
| NIH | National Institutes of Health |
| NIMS | National Incident Management System |
| NIST | National Institute of Standards and Technology |
| ODNI | Office of the Director of National Intelligence |
| OHS | Office of Homeland Security |
| OIG | Office of the Inspector General |
| OMB | Office of Management and Budget |
| OPM | Office of Personnel Management |
| OSHA | Occupational Safety and Health Administration |
| OSSP | Office of Safety, Security, and Protection |
| PACS | Physical Access Control System |
| PDSD | Personnel and Document Security Division (OHS component) |
| PI | Principal Investigator |
| PIN | Personal Information Number |
| PIV | Personal Identity Verification |
| P.L. | Public Law |
| PPD | Presidential Policy Directive |
| PPE | Personal Protective Equipment |
| PPQ | Plant Protection and Quarantine |
| recNA | Recombinant Nucleic Acid |
| RG | Risk Group |
| RMF | Risk Management Framework |
| RMP | Risk Management Process |
| RNA | Ribonucleic Acid |
| RO | Responsible Official |
| SCADA | Supervisory Control and Data Acquisition |
| SO | System Owner |
| SOP | Standard Operating Procedure |
| SP | Special Publication |
| SRA | Security Risk Assessment |
| SRC | Security Review Committee |
| STIG | Security Technical Implementation Guide |

| | |
|---|---|
| synNA | Synthetic Nucleic Acid |
| T | Tier |
| UL | Underwriters' Laboratories |
| UPS | Uninterruptible Power Supply |
| USA PATRIOT | Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism |
| USB | Universal Serial Bus |
| U.S.C. | United States Code |
| USDA | United States Department of Agriculture |
| USG | United States Government |
| USGCB | United States Government Configuration Baseline |
| USPHS | United States Public Health Service |
| VPN | Virtual Private Network |
| VS | Veterinary Service |
| WAN | Wide Area Network |
| WHO | World Health Organization |

APPENDIX B

DEFINITIONS

Administrator. Head of an agency within the USDA regardless of the actual title used, e.g., Chief of the Forest Service.

Agency. Organizational units of the Department, other than staff offices, whose head reports to officials within the Office of the Secretary, Deputy Secretary, Under Secretaries, Assistant Secretaries, and Assistant to the Secretary. (Source: Departmental Guidebook (DG) 0100-002, *USDA Departmental Definitions Glossary*)

Agent Type. Limit categories to: Arthropods (non-indigenous arthropods and disease vectors or pests), Bacteria and Rickettsiae, Fungi; Oomycetes; Nematodes; Parasites; Parasitoids; Prions; Toxins; Viroids; Viruses; and others not Taxonomically Classified. This list of categories of agent types will allow the database to be searchable. Future distinctions may be appropriate or relevant as necessary to encompass the varied activities of the USDA as a whole and will be reviewed on an annual basis.

Animal Biosafety Levels (ABSL). Encompass a combination of practices, safety equipment, and facilities for experiments with vertebrate animals involved in infectious disease research and other related studies that require containment.

The CDC, *Biosafety in Microbiological and Biomedical Laboratories (BMBL)*, 6th Edition, describes 4 combinations, designated ABSL-1 through 4, which provide increasing levels of protection to the worker and the environment. In addition to the 4 ABSLs, the USDA has developed parameters and work practices for working with specific high consequence livestock biological agents in livestock hosts to include an enhanced ABSL-3 facility (known as BSL-3Ag) which incorporates many of the enhancements found within an ABSL-4 facility, with the exception of the chemical decontamination shower and the infrastructure associated with a fully encapsulated suit.

Animal Biosafety Level 1 (ABSL-1). Suitable for work in animals involving well-characterized, low-risk agents that are not known to cause disease in immunocompetent adult humans or animals, and present minimal potential hazard to personnel and the environment. However, many agents not ordinarily associated with disease processes in humans are opportunistic biological agents that may cause infection in the young, the aged, and immunocompromised individuals.

a. ABSL-1 facilities would be separated from the general traffic patterns of the building and restricted as appropriate. Special containment equipment or facility design may be required as determined by appropriate risk assessment; and

b. Personnel must have specific training in animal facility procedures and standard microbiological techniques and must be supervised by an individual with adequate

knowledge of potential hazards and experimental animal procedures. These facilities are typical of university or industry research farms.

Animal Biosafety Level 2 (ABSL-2). Builds upon the practices, procedures, containment equipment, and facility requirements of ABSL-1. ABSL-2 is suitable for work involving laboratory animals infected with agents associated with human disease and pose moderate hazards to personnel, animals or agriculture, and the environment.

a. It also addresses hazards from ingestion as well as from percutaneous and mucous membrane exposure. These agents are generally endemic, cause illness of varying degree in either humans or animals and are typically treatable or preventable.

b. ABSL-2 requires that:

(1) Access to the animal facility is restricted;

(2) Personnel must have specific training in animal facility procedures, the handling of infected animals and the manipulation of biological agents;

(3) Personnel must be supervised by individuals with adequate knowledge of potential hazards, microbiological agents, animal manipulations and husbandry procedures;

(4) Biological Safety Cabinets (BSC) or other physical containment equipment is used when procedures involve the manipulation of infectious materials, or where aerosols or splashes may be created;

(5) Appropriate personal protective equipment must be utilized to reduce exposure to infectious agents, animals, and contaminated equipment; and

(6) Implementation of employee occupational health programs would be considered.

c. Most research and diagnostic vivaria that work with food-borne biological agents and domestic diseases are designed to perform work at this level.

Animal Biosafety Level -3. Animal Biosafety Level 3 (ABSL-3) involves practices suitable for work with laboratory animals infected with indigenous or exotic agents, agents that present a potential for aerosol transmission, and agents causing serious or potentially lethal disease. ABSL-3 builds upon the standard practices, procedures, containment equipment, and facility requirements of ABSL-2. The ABSL-3 facility has special engineering and design features. ABSL-3 requires that in addition to the requirements for ABSL-2, all procedures are conducted in BSCs or by use of other physical containment equipment. Inward airflow at the containment boundary is maintained. Handwashing sinks are capable of hands-free operation. Appropriate PPE is worn to reduce exposure to infectious agents, animals, and contaminated equipment.

Animal Biosafety Level 3 (ABSL-3Ag). Facilities required for activities involving the use of hazardous biological agents designated as High Consequence Foreign Animal Diseases and Pests by USDA APHIS in animals that are loose-housed or in open penning.

a. ABSL-3Ag containment incorporates standard practices, procedures, containment equipment, and facility design features common to ABSL-3 and ABSL-2Ag facilities, but also incorporates many of the facility features usually reserved for ABSL-4 facilities as enhancements. This level of containment is required for animals that must be housed in open cages or pens and that have been infected with specific transboundary livestock or wildlife pathogens defined by USDA APHIS Veterinary Services (VS). The agents involved may either be animal pathogens that pose significant economic risk to the agricultural sector or agents with zoonotic potential that are classified as Risk Group (RG)-1, RG-2, or RG-3 pathogens. USDA APHIS VS *Select Agent Regulations* (9 CFR Part 121) will specify required facility enhancements that exceed standard ABSL-3 requirements for research involving agricultural pathogens that pose significant economic risk to local, regional, or national agricultural sectors.

b. Because large animals and wildlife species involved in research and diagnostic activities cannot be housed in primary containment isolators, the room perimeter serves as the primary containment barrier. The containment zone may consist of a single room, a suite of rooms within a larger facility, or may occupy an entire building. The area of containment functions as a "box within a box" and is completely isolated from non-containment areas. Access is strictly controlled and is limited to personnel who have been properly trained and cleared. Special physical security features often associated with ABSL-4 facilities may be incorporated to safeguard against unauthorized entries.

c. A site-specific risk assessment would be completed with documents the various ABSL-3 and ABSL-2Ag enhancements considered for implementation. Supplemental enhancements would be based on the results of this risk assessment and on any specific conditions or requirements stipulated by USDA APHIS, other relevant regulatory entities, or local policies and procedures.

d. At minimum, ABSL-3Ag containment facilities must meet requirements associated with ABSL-3 and ABSL-2Ag containment; and incorporate the majority of enhancements usually found in ABSL-4 facilities. Potential enhancements to increase the safety of ABSL-3Ag containment facilities designed for in vivo work with large animals are listed in the BMBL, 6$^{th}$ Edition, Appendix D. USDA APHIS VS, other relevant regulatory entities, or local policies and procedures will determine which enhancements are required based on the specific details of the proposed work.

Animal Biosafety Level 4 (ABSL-4). Also called "Maximum Containment". Required for work with animals infected with dangerous and exotic agents that pose a high individual risk of aerosol-transmitted laboratory infections and life-threatening disease in humans that is frequently fatal, or for which there are no vaccines or treatments; or a related agent with unknown risk of transmission.

a. Agents with a close or identical antigenic relationship to agents requiring (A)BSL4 containment must be handled at this level until sufficient data are obtained either to confirm continued work at this level, or to re-designate the level. This standard would have all the features of a BSL-3-Ag facility with added worker protection(s).

b. While there is no BSL-4 requirement solely for agricultural agents, some viruses are lethal for agricultural species and for humans (e.g., Rift Valley fever virus, Nipah virus encephalitis). Animal care staff must have specific and thorough training in handling extremely hazardous, infectious agents and infected animals. Animal care staff must understand the primary and secondary containment functions of standard and special practices, containment equipment, and laboratory design characteristics.

c. All animal care staff and supervisors must be competent in handling animals, agents and procedures requiring (A)BSL4 containment. The animal facility director or laboratory supervisor control access to the animal facility within the (A)BSL4 laboratory in accordance with institutional policies.

d. There are two models for (A)BSL-4 laboratories:

   (1) Cabinet Laboratory: All handling of agents, infected animals, and housing of infected animals must be performed in Class III BSCs, and

   (2) Suit Laboratory: Personnel must wear a positive pressure protective suit; infected animals must be housed in ventilated enclosures with inward directional airflow and HEPA filtered exhaust; and infected animals would be handled within a primary barrier system such as a Class II BSC or other equivalent containment system.

e. (A)BSL-4 builds upon the standard practices, procedures, containment equipment, and facility requirements of (A)BSL-3. However, (A)BSL-4 cabinet and suit laboratories have special engineering and design features to prevent microorganisms from being disseminated into the environment and personnel.

f. The (A)BSL-4 cabinet laboratory is distinctly different from an (A)BSL-3 Laboratory containing a Class III BSC.

<u>(A)BSL-4Ag</u>. Facilities for Conducting Work with Animals that are Loose-Housed or in Open Penning. ABSL-4Ag containment incorporates standard practices, procedures, containment equipment, and facility design features common to ABSL-4 and ABSL-3Ag facilities (see previous sections). This level of containment is required for animals infected with zoonotic pathogens that would ordinarily require:

a. Facilities and procedures commensurate with ABSL-4 containment as determined by relevant regulatory authorities, or; and

b. A comprehensive local risk assessment, which also assesses the cross-contamination risk, for animals that cannot be housed in primary containment isolators (e.g., open

caging units inside flexible film isolators with inward-directional airflow that is separate from the facility's Heating, Ventilation, and Air Conditioning system. Personnel working in the ABSL-4Ag containment zone must wear positive pressure suits.

c. Agents studied in ABSL-4Ag containment can pose a significant economic risk to the agricultural sector and are also zoonotic pathogens consistent with RG-3 or RG-4 classification, for which effective treatments or preventative measures are not available for humans. Animals used in this research are housed loosely or in open penning, so the room perimeter serves as the primary containment barrier. The containment zone may consist of a single room, a suite of rooms within a larger facility, or an entire building. The area of containment functions as a "box within a box" and is completely isolated from non-containment areas. Access is strictly controlled and limited to personnel who have been properly trained and cleared. Special physical security features that are required for standard ABSL-4 facilities must be incorporated to safeguard against unauthorized entries.

d. A site-specific risk assessment would be completed with various ABSL-4 and ABSL-3Ag enhancements being considered. Supplemental enhancements would be based on the results of this risk assessment and would be implemented with specific conditions or requirements stipulated by USDA APHIS VS, other relevant regulatory entities, or local policies and procedures.

e. At minimum, ABSL-4Ag containment facilities must meet requirements associated with ABSL-4 and ABSL-3Ag containment. Potential enhancements to increase the safety of ABSL-4Ag containment facilities designed for in vitro procedures and in vivo work with animals may be found in Appendix D of the *BMBL*, 6th Edition.

Biohazard. Materials containing infectious agents (including pathogenic microbes) or hazardous materials that present a risk or potential risk to the health of humans, animals, or the environment. The risk can be direct through infection or indirect through damage to the environment. Biohazardous materials include certain types or recombinant DNA, organisms, and viruses infectious to humans, animals, or plants (e.g., parasites, viruses, bacteria, fungi, prions, and rickettsia), and biologically active agents (e.g., toxins, allergens, and venoms) that can cause disease in living organisms or cause significant impact to the environment or community. Although, many viral vectors (e.g., replication defective adenoviruses) are prepared in such a way to be reasonably safe to work with, they should still be listed as biohazardous. Potentially biohazardous agents that may produce latent (silent or subclinical) infections must be considered biohazardous. Materials that may harbor infectious agents (e.g., human blood, body fluids, tissues, cells, and various environmental diagnostic samples) must also be considered biohazardous.

Biological Agent Name. Minimum genus name; species if identified to that level. Provision of strain information is recommended, if known. Note name changes for agents in annual updates in the inventory record; do not relabel tubes unless scientifically necessary (as long as they are uniquely identified and traceable using the inventory record).

Biological Select Agents and Toxins (BSAT). Biological agents and toxins that have the potential to pose a severe threat to public health and safety, animal health and safety, plant health and safety, or to the safety of animal or plant products, regulated under 9 CFR § 121, 7 CFR §331, and 42 CFR § 73.

Biosafety Levels and Animal Biosafety Levels ((A)BSL). A classification system including a combination of work practices and physical containment requirements designed to reduce the risk of laboratory infection and environmental release when working with infectious materials. The BMBL, 6th Edition provides relevant insights.

Biosafety Level 1 (BSL-1). Suitable for work involving well-characterized, low-risk etiologic agents not known to consistently cause disease in immunocompetent adult humans or healthy animals, that represent no potential economic loss to agricultural industries, and that present an overall minimal potential hazard to laboratory personnel and the environment. BSL-1 laboratories are not necessarily separated from the general traffic patterns in the building.

a. Work is typically conducted on open bench tops using standard microbiological practices. Laboratory personnel must have specific training in the procedures conducted in the laboratory and must be supervised by a scientist with training in microbiology or a related science.

b. Facilities would be easily cleanable, have a sink for hand washing, and conform to the facility requirements described in the BMBL for BSL-1.

c. These laboratories are typical of undergraduate or secondary education teaching laboratories, laboratories working with plant biological agents that are not a risk to humans or the environment or work with exempt organisms under *The National Institutes of Health (NIH), Guidelines for Research Involving Recombinant or Synthetic NA Molecules* (NIH Guidelines).

d. However, many agents not ordinarily associated with disease processes in humans are opportunistic biological agents that may cause infection in the young, the aged, and immunocompromised individuals.

Biosafety Level 2 (BSL-2). Builds upon BSL-1. BSL-2 is suitable for work involving agents that pose moderate hazards to personnel, animals or agriculture, and the environment. These agents are generally endemic, cause illness of varying degree in the relevant host and are typically treatable or preventable.

a. It differs from BSL-1 in that:

(1) Laboratory personnel have specific training in handling biohazardous agents and are supervised by scientists competent in handling infectious agents or toxins and associated procedures; and

(2) Access to the laboratory is restricted when work is being conducted.

b. All procedures in which infectious aerosols or splashes may be created are conducted in Biological Safety Cabinets (BSC) or other physical containment equipment. Most research and diagnostic laboratories that work with food-borne biological agents and domestic diseases are designed to perform work at this level. Many biotechnological diagnostic procedures on more hazardous (e.g., BSL-3) agents are performed at this level due to the low level of the organism in samples, the lack of concentration or culture steps in the tests, and the destructive nature of the process (e.g., Enzyme-Linked Immunosorbent Assay Polymerase Chain Reaction).

Biosafety Level 3 (BSL-3). Applicable to clinical, diagnostic, teaching, research, or production facilities where work is performed with indigenous or exotic agents that may cause serious or potentially lethal disease in humans through the inhalation route of exposure, or those that may have grave economic consequences to agriculture if released.

a. Laboratory personnel must receive specific training in handling biological agents and potentially lethal agents and must be supervised by scientists competent in handling infectious agents and associated procedures.

b. All procedures involving the manipulation of infectious materials must be conducted within BSCs or other physical containment devices.

c. A BSL-3 laboratory has special engineering and design features, such as inward directional airflow, separation from non-laboratory areas, requirements for special laboratory protective clothing, and systematic decontamination of laboratory waste with specialized equipment (e.g., autoclave) or specialized treatments (e.g., chemical inactivation procedures).

d. For in vitro work with some highly infectious agriculture agents, a risk assessment for the agent and planned manipulations would be conducted. BSL-3 laboratories may be modified further with enhancements specifically designed to protect the environment such as HEPA filtration of supply or exhaust air, laboratory liquid effluent sewage decontamination, personnel exit showers (at the room or facility level), and facility integrity testing.

Biosafety Level 4 (BSL-4). Also called "Maximum Containment." Required for work with dangerous and exotic agents that pose a high individual risk of aerosol transmitted laboratory infections and life-threatening disease that is frequently fatal to humans, for which there are no vaccines or treatments, or a related agent with unknown risk of transmission.

a. While there is no BSL-4 requirement when solely considering the animal or agricultural risk of an agent, this classification could apply to etiologic agents that cause serious disease in both humans and animals (e.g., Henipaviruses), and for which there are no vaccines. Agents with a close or identical antigenic relationship to agents requiring BSL-4 containment must be handled at this level until sufficient data are obtained either to confirm continued work at this level or re-designate the level.

b. Laboratory staff must have specific and thorough training in handling extremely hazardous infectious agents. Laboratory staff must understand the primary and secondary containment functions of standard and special practices, containment equipment, and laboratory design characteristics.

c. All laboratory staff and supervisors must be competent in handling agents and procedures requiring BSL-4 containment.

d. The laboratory supervisor, in accordance with institutional policies strictly control access to the laboratory.

e. There are two models for BSL-4 laboratories:

(1) Cabinet Laboratory. Manipulation of agents must be performed in a Class III BSC; and

(2) Suit Laboratory. Personnel must wear a positive pressure supplied air protective suit.

f. BSL-4 cabinet and suit laboratories have special engineering and design features to protect laboratory personnel and prevent microorganisms from being disseminated into the environment.

Chain of Custody. The protection of evidence by each responsible party to ensure it against loss, breakage, alteration, or unauthorized handling. This protection also includes properly securing, identifying, and dating evidence. Individuals place their initials and date on the container when the evidence is stored in a container or on the evidence in such a way that no damage is incurred.

Escort. Any USDA employees with unrestricted access to HCBA, high and maximum containment laboratory support space, or critical infrastructure, with a completed and favorably adjudicated background investigation and appropriate facility authorization, who accompany an unapproved person into a secure area. The escort must be knowledgeable of the institution's security requirements and the biosafety, chemical, and physical risks of the agent(s) or toxin(s) in the areas where the escorted person is being allowed to enter. The escort must be capable of executing appropriate safety and security protocols. The escort is responsible for providing visitor training to the unapproved person on the safety and security risks, they will encounter, commensurate to their exposure to such risks.

a. These presentations must account for items such as (but not limited to): administrative access controls, security of critical assets, safety considerations for physical, chemical, or biological risks, and evacuation during incidents.

b. Procedures for handling any exceptions to these requirements, such as for ad-hoc training events must be outlined in location-level policy. If an agency is unable to meet any of these requirements, they may request, in writing, a waiver from OHS.

Exclusion Area. The area that houses the critical asset(s). This area could be (or contain) the high and maximum containment area, or anything else that the location or other rules and regulations defines as a critical asset worthy of the highest level of maximum protection. Exclusion area access requires unique item and unique knowledge.

Facility. The brick and mortar building, greenhouse, glasshouse, or screen house within the location that houses regulated high and maximum containment assets. Again, subject to design and the security risk assessment, could be contained in either the Property Protection Area (e.g., have semi-public sections), or define the Limited Area, or both. Facilities are "containment facilities" when the whole building is dedicated to high and maximum containment laboratory or animal space, or support structures; however, this term is not necessarily appropriate for buildings that house spaces with other non-containment functions.

Federal Select Agent Program. A program with shared responsibility by the Animal and Plant Health Inspection Service, Agricultural Select Agent Services and the Centers for Disease Control and Prevention Division of Select Agents and Toxins.

Foreign Animal Disease. A contagious, infectious, or communicable animal disease exotic to the United States.

Genetic Database (GenBank). A comprehensive database that contains publicly available nucleotide sequences for more than 300,000 organisms named at the genus level or lower.

Guard Post Orders and Special Instructions. Detailed written instruction to the guard force detailing use of force frequency of patrols, hours of operation, special needs of the facility, and outlining changes in protocols to address specific incidents. To the maximum extent permissible under the law, USDA will exercise available authority to arrest and detain.

High Containment Area. The actual room or rooms (e.g., actual laboratory, inventories, growth chamber) within the facility, or connected to it, that houses a regulated mission critical asset that requires maximum control and protection. Referred to as the Exclusion Area.

High Containment Biological Agent (HCBA). Those biological agents, inclusive of "biological agents" and "Foreign Animal Diseases" that require BSL-3 or higher biological containment for possession, use, or transfer.

High Containment Pathogen . Those biological agents, inclusive of "biological agents" and "Foreign Animal Diseases" that require BSL-3 or higher biological containment for possession, use, or transfer. Pathogens are bacteria, viruses or microorganisms that specifically can cause disease. For purpose of this DM, all pathogens that require work to be conducted in a High or Maximum Containment facility will be considered as HCBA.

Incident. An occurrence, natural or manmade, that requires a response to prevent compromise of the high and maximum containment laboratory facilities, security, inventory, personnel, or to protect human life, and animal and plant health.

Incident Commander (IC). HSPD-5 mandates that Federal agencies use the FEMA, NIMS. IC mirrors local responder (Fire, Police, Emergency) and NIMS models and requirements. The USDA Center Director, Laboratory Director, or Research Leader directly involved in High Containment Biological Agent management would assume or delegate this role.

Intrusion Detection System (IDS). A system designed to detect unauthorized entry and to send an alarm.

Limited Area. All but local, facility employees are excluded. Agency employee credentials will not open the barriers from semi-public areas to limited areas, but access can be granted to certain personnel (e.g., agency or Federal employees, long-term visitors, contractors) that have a successfully-adjudicated security clearance appropriate to their access by authorized management officials. Members of the public, or those not granted unrestricted access, must be escorted in limited areas. Access requires unique item or unique knowledge. If a keycard (i.e., unique item) is required to enter the perimeter fence, the Property Protection Area can be (but is not necessarily) the same as the Limited Area security barrier.

LincPass. HSPD-12 mandates that Federal agencies screen their employees and contractors and issue credentials that adhere to NIST FIPS PUB 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors.* FIPS PUB 201-3 was issued by the NIST and outlines the requirements for Federal credentials. Here at USDA, this Federal credential, or Smartcard, has been named the "LincPass," (see DR 4620-002, *Common Identification Standard for U.S. Department of Agriculture*).

Location and Entity. The overall geographic footprint of the business. Subject to the design of the grounds and the security risk assessment, could be defined as the Property Protection Area. Property protection areas require a perimeter fence, roadway with signage, or some sort of notification that the general public is entering restricted space. Also referred to by the FSAP as an "entity."

Nucleic acid (NA). NA are polymeric macromolecules, which include DNA and RNA that are made from monomers known as nucleotides. The term "nucleic acid" is the overall name for DNA and RNA and is synonymous with "polynucleotide." The basic component of biological NA is the nucleotide, each of which contains a pentose sugar backbone (ribose or deoxyribose), a phosphate group, and a nucleobase. NA are fundamental to biological processes and can be manipulated and generated within the laboratory by many methods.

Pathogen. A bacterium, virus or other microorganism that can cause disease.

Position Risk Designation. Agency heads must designate every covered position, contract positions, or visitor within the agency as to the level of personnel security investigation that will be required based on the needs of their work.

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

program. For select agents, the PI can only designate SRA approved and registered personnel to act on their behalf in "delegation of authority" type standard operating policies or procedures.

Recombinant nucleic acids (recNA). Molecules that are constructed by joining NA molecules and that can replicate in a living cell (i.e., recombinant NA), or molecules that result from the replication of recNA would be named such that a layman can assess the risk of the material and would include (at a minimum) the name of the parent organism of the gene or NA sequence, and the common name of the disease or intoxication it causes. For example, the products experiment that use of enzymes designed to cut or combine DNA and RNA (e.g., endonucleases and ligases) or introduce isolated or manipulated DNA or RNA into cells are generally described as "recombinant NA" or "recombinant organisms."

Space. Areas of concern are classified at several different levels.

Synthetic nucleic acids (synNA). Molecules that are chemically or by other means synthesized or amplified, including those that are chemically or otherwise modified but can base pair with naturally occurring NA molecules (i.e., synthetic NA) or molecules that result from the replication of synNA, would be named such that a layman can assess the risk of the material and would include (at a minimum) the name of the parent organism of the gene or NA sequence, and the common name of the disease or intoxication it causes.

a. For example, the products experiment that use of enzymes designed to amplify or generate DNA and (DNA and RNA polymerases and solid-phase chemical synthesis) or introduce amplified or generated DNA or RNA into cells are generally described as "synthetic NA" or "synthetic organisms."

b. Additionally, some chemical methods also enable the generation of altered NA that are not found in nature. Artificial NA analogs have been designed and synthesized by chemists and can include peptide NA, morpholino-NA, and locked-NA, among others. Each of these is distinguished from naturally occurring DNA or RNA by changes to the backbone of the molecule and would be considered "synthetic NA" as well.

Tailgating. A process where the electronic lock will reengage after a valid entry or within 12-20 seconds after a valid card read, to prevent unauthorized access for persons not authorized to enter the secure area.

Toxin. Toxic material or products of plants, animals, microorganisms (including, but not limited to, bacteria, viruses, fungi, or protozoa), or recombinant or synthesized molecules, or other substances whatever their origin and method of production, and includes any poisonous substance or biological product that may be engineered as a result of chemistry or biotechnology, produced by a living organism, or any poisonous isomer, biological product, homolog, or active derivative or subunit of such a substance. This excludes chemical poisons or intoxicants not of a natural biological origin.

Vectors. A carrier, usually an arthropod in biological systems that transfers an infectious agent from one host to another. Transmission can be either mechanical, where no replication occurs in

the vector or biological (the usual case with viruses), where replication in the vector is required for transmission.

Visitor. Any person not physically assigned to the high and maximum containment location or facility.

APPENDIX C

AUTHORITIES AND REFERENCES

5 CFR Part 731, *Suitability Regulations*

5 CFR Part 732, *National Security Positions*

5 CFR § 1400, *Designation of National Security Positions*

7 CFR § 2, *Delegations of Authority by the Secretary of Agriculture and General Officers of the Department*

7 CFR § 2.95, *Director, Office of Homeland Security*

7 CFR § 330.200, Subpart B – *Movement of Plant Pests, Biological Control Organisms, and Associated Articles*

7 CFR § 331.16, *Transfers*

7 CFR § 331.17, *Records*

7 CFR § 331.19, *Notification of Theft, Loss, or Release*

9 CFR § 121, *Possession, Use and Transfer of Select Agents and Toxins*

9 CFR § 122, *Organisms and Vectors*

15 CFR § 742, *Control Policy – Commerce Control List, (CCL) Based Controls*

29 CFR § 1910.1030, OSHA, *Bloodborne Pathogens*

32 CFR § 147, *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*

39 CFR § 111, *General Information on Postal Service*

40 CFR § 792, *Good Laboratory Practice Standards*

41 CFR § 101, Subtitle C – *Federal Property Management Regulations*

42 CFR § 70, U.S. Public Health Service, *Interstate Quarantine*

42 CFR § 71, *Foreign Quarantine*

42 CFR § 71.54, *Import Regulations for Infectious Biological Agents, Infectious Substances, and Vectors*

42 CFR § 73, *Select Agents and Toxins*

49 CFR § 171-177, 178-180, Subchapter C – *Hazardous Materials Regulations*

49 CFR § 173.134, Class 6, Division 6.2, *Definitions, and Exceptions*

CDC, FSAP, *Annual Report of the Federal Select Agent Program,* 2020

CDC, *Guidance on the Inventory of Select Agents and Toxins, 7 CFR § 331, 9 CFR § 121, 42 CFR § 73*, December 2020

CDC, *Incident Response Plan Guidance*, *7 CFR Part 331, 9 CFR Part 121, 42 CFR Part 73, August 2021*

CDC, *Suitability Assessment Program Guidance*, *42 CFR §73.11, 7 CFR § 331.11,and 9 CFR § 121.11*, March 2017

*Code of Federal Regulations*, (Annual Edition)

DHS, ISC, *Best Practices for Armed Security Officers in Federal Facilities*, 2nd Edition, April, 2013

DHS, ISC, *Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors*, 1st Edition, September 2012

DHS, ISC, *Items Prohibited from Federal Facilities*, 2022 Edition

DHS, ISC, *The Risk Management Process, An Interagency Security Committee Standard*, 2021 Edition

DISA, *Security Technical Implementation Guides* (STIG) website

EO 12923, *Continuation of Export Control Regulations*, June 30, 1994; continuation of the *Export Administration Act of 1979*

EO 14028, *Improving the Nation's Cybersecurity,* May 12, 2021

FEMA, *National Incident Management System* (NIMS), Third Edition, October 2017

Health and Human Services, Publication No. (CDC) 21-1112, *Biosafety in Microbiological and Biomedical Laboratories (BMBL),* 6th Edition, Revised June 2020

HSPD-5, *Management of Domestic Incidents*, February 28, 2003

HSPD-8, *National Preparedness*, December 17, 2003

HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004

International Air Transport Association, *Dangerous Goods Regulations*, 40th Edition, 1999

International Civil Aviation Organization, *Technical Instructions for the Safe Transport of Dangerous Goods by Air*, 2017-2018 Edition

NARA, Office of Chief Records Officer, General Records Schedule 5.6: *Security Management Records*, Section 90, *Facility security management operations records,* March 2022

NARA, *General Records Schedule (GRS), Transmittal 31*, April 2020

*National Security Act of 1947*, dated July 26, 1947, as amended

National Institutes of Health (NIH), *Guidelines for Research Involving Recombinant or Synthetic Nucleic Acid Molecules*, April 2019

National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication (FIPS PUB) 140-3, *Security Requirements for Cryptographic Modules*, March 22, 2019

NIST, FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

NIST, FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006

NIST, FIPS PUB 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, January 2022

NIST, Computer Security Resource Center (CSRC), Glossary website

NIST, CSRC, *United States Government Configuration Baseline (USGCB)*, website, retrieved March 24, 2022

NIST, SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*, *A System Life Cycle Approach for Security and Privacy*, December 2018

NIST, SP 800-39, *Managing Information Security Risk: Organization, Mission , and Information System View*, March 2011

NIST, SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* September 2020, includes updates as of December 10, 2020

NIST, SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008

NIST, SP 800-70, Revision 4, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers,* February 2018

Office of the Director of National Intelligence, Security Executive Agent Directive 6, *Continuous Evaluation,* January 12, 2018)

OMB, Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

OPM, *Federal Investigative Standards*, 2012

Presidential Decision Directive - 12, *Security Awareness and Reporting of Foreign Contacts*, August 5, 1993

Presidential Policy Directive - 21, *Critical Infrastructure Security and Resilience*, February 12, 2013

*Public Health Security and Bioterrorism Preparedness and Response Act of 2002*, P.L. 107-188, June 12, 2002

U.S.C., §§ 3551-3559, Subchapter II, *Information Security*

USDA, APHIS, *Import Export Services* website

USDA, APHIS, *Plant Health (PPQ)* website

USDA, DG 0100-002, *USDA Departmental Directives Definitions Glossary*, September 26, 2018

USDA, DM 3440-001, *USDA Classified National Security Information Program Manual*, June 9, 2016

USDA, DM 3510-000, *Information Technology (IT) Restricted Space*, August 19, 2004

USDA, DM 3510-001, *Physical Security Standards for Information Technology (IT) Restricted Space*, Chapter 2, Part 1, August 19, 2004

USDA, DM 4620-002, *Common Identification Standard for U.S. Department of Agriculture (USDA)*, December 9, 2021

USDA, DM 9610-002, *Security Policies and Procedures for Laboratories and Technical Facilities (Excluding Biosafety Level (BSL)-3 Facilities)*, April 30, 2003

USDA, DR 1650-002, *Building Safety/Security Occupant Emergency Program*, October 7,1992

USDA, DR 1800-001, *Incident Preparedness, Response, and Recovery*, February 9, 2022

USDA, DR 3300-001, *Telecommunications & Internet Services and Use*, March 18, 2016

USDA, DR 3440-001, *USDA Classified National Security Information Program*, June 9, 2016

USDA, DR 3440-002, *Control and Protection of "Sensitive Security Information,"* January 30, 2003

USDA, DR 3440-003, *Controlled Unclassified Information (CUI)*, September 13, 2021

USDA, DR 3441-001, *Sensitive Compartmented Information Security Program*, January 18, 2012

USDA, DR 3500-3599, *Cybersecurity*

USDA, DR 3505-003, *Access Control for Information and Information Systems*, July 17, 2019

USDA, DR 3505-005, *Cybersecurity Incident Management Procedures*, November 30, 2018

USDA, DR 3520-002, *Configuration Management*, July 17, 2019

USDA, DR 3530-006, *Scanning and Remediation of Configuration and Patch Vulnerabilities*, June 5, 2019

USDA, DR 3540-003, *Security Assessment and Authorization*, August 12, 2014

USDA, DR 3545-001, *Information Security Awareness and Training Policy*, October 22, 2013

USDA, DR 3565-003, *Plan of Action and Milestone Policy*, September 25, 2013

USDA, DR 4000-4999, *Human Resources Management*

USDA, DR 4030-001, *Section 508 Program*, September 8, 2014

USDA, DR 4070-735-001, *Employee Responsibilities and Conduct*, October 4, 2007

USDA, DR 4400-007, *Biorisk Management Policy*, September 3, 2020 (Maximum Containment)

USDA, DR 4600-003, *Defensive Counterintelligence and Insider Threat Programs*, July 12, 2021

USDA, DR 4600-004, *Foreign Visits and Assignments Vetting*, May 27, 2021

USDA, DR 4610-001, *Security Screening Unit Procedures*, December 12, 2021

USDA, DR 4620-002, *Common Identification Standard for U.S. Department of Agriculture*, June 24, 2021

USDA, DR 9610-xxx, *Security, Suitability, and Incident Response for High and Maximum Containment Facilities*, forthcoming

USDA, DR 9630-001, *Policies and Procedures on Biohazardous Waste Decontamination, Management, and Quality Controls at Laboratories and Technical Facilities*, June 18, 2009

USDA, OHS, *Cleared Employee Reporting Requirements*

USDA, OHS, *Insider Threat Program*, home page

USDA, OHS, *Personnel and Document Security Division's (PDSD)* home page

U.S. Department of Commerce, Bureau of Industry and Security, *Commerce Control List (CCL)* website

*United States Government Configuration Baseline*, website

*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001*, Public Law (P.L.) 107-56, October 26, 2001

World Health Organization (WHO), *Guidelines for the Safe Transport of Infectious Substances and Diagnostic Specimens*, 1997

WHO, *Laboratory Biosafety Manual*, 4th Edition, 2020