United States
Department of
Agriculture

Agriculture Research Service

DM 9610-1

USDA Security Policies and Procedures for Biosafety

Level – 3 Facilities

USDA SECURITY POLICIES AND PROCEDURES
FOR BIOSAFETY LEVEL-3 FACILITIES

TABLE OF CONTENTS

		Page
TABLE OF CONTENTS		i
SECTIONS		
1	Purpose	1
2	Special Instructions	1
3	Introduction	1-3
4	Abbreviations	3-4
5	Definitions	4-8
6	Responsibilities	9
7	Authorities, References, and Organizations	9-12
8	Inventory Control Procedures	13-16
9	Physical Security Systems	16-24
10	Cybersecurity Systems	24-28
11	Personnel Suitability	29-30
12	Biosecurity Incident Response Plan	30

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

DEPARTMENTAL MANUAL	Number: 9610-001
SUBJECT: USDA Security Policies and Procedures for Biosafety Level-3 Facilities	DATE: August 30, 2002
	OPI: Agricultural Research Service

1 PURPOSE

The purpose of this Manual is to define U.S. Department of Agriculture (USDA) requirements to secure pathogens held at USDA Biosafety Level-3 (BSL-3) facilities. Security of pathogens held at non-BSL-3 facilities is covered in another technical facility security USDA manual entitled, "Security Policies and Procedures for USDA Laboratories and Technical Facilities Excluding BSL-3 Facilities."

2 SPECIAL INSTRUCTIONS

a This Manual contains a uniform set of USDA policies and procedures which are intended to cover USDA laboratories that work with or have the capacity to work with BSL-3 pathogens and other facilities as deemed appropriate.

b The policies and procedures described herein are subject to review on a 5-year basis unless conditions warrant earlier review.

3 INTRODUCTION

This Manual defines USDA requirements to secure USDA-held pathogens at BSL-3 facilities. Each BSL-3 biocontainment facility shall create or modify an existing plan for biosecurity that is distinct from their own biosafety plan. The biosecurity plan shall have the following elements:

a Inventory Control Procedures
b Physical Security Systems
c Cybersecurity Systems
d Personnel Suitability
e Biosecurity Incident Response Plan

The biosecurity plan is the responsibility of the Agency and will be approved by the Administrator. The USDA conducts research and regulatory activities, including detection and diagnosis, to protect American agriculture, forestry, and human health from pathogens. USDA scientists utilize pathogens in their research and diagnostic activities that could constitute a threat to either human health or productivity of the agriculture system if purposely or inadvertently released into the environment.

Not all pathogens constitute an equal risk of threat to humans. The Centers for Disease Control and Prevention (CDC) provide a classification scheme (see Definitions) describing the level of containment that must be used to protect researchers from the pathogens. In addition, agricultural scientists utilize a parallel set of standards for managing agricultural pathogens to protect researchers and minimize the risk of a release into the environment (see Definitions). Pathogens of concern are those needing BSL-3 or BSL-4 containment.

USDA scientists work with crop pathogens that do not pose a direct threat to human health but may indirectly pose a threat through the production of toxins. The major concern with exotic crop pathogens is the potential for harm to American crops.

USDA scientists work with animal pathogens that need containment to prevent their release into the environment. An example of such a pathogen is foot-and-mouth disease virus that does not pose a health threat to humans but would cause significant loss among impacted animal populations.

USDA scientists work with zoonotic pathogens that cause disease in animals and in humans. Avian influenza virus is such a pathogen that causes illness in birds but can also cause serious illness and even death in humans.

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. USDA scientists work with *E. coli* O157:H7 to develop means to prevent its contamination of the food supply.

In light of legislation and the urgency to address security at USDA laboratories, in the interim and absent any criteria, all BSL-3 agents as currently defined will be treated as High Consequence Pathogens (HCPs). Pathogens classified at the

BSL-2 level and held with BSL-3 pathogens will be treated as HCPs, including brucellosis species**,** Bacillus anthracis, etc. The Department will develop and maintain a HCPs list.

All USDA personnel at BSL-3 facilities are responsible for biosafety. The USDA-Agricultural Research Service (ARS) employs a Biosafety Officer responsible for managing and directing the biosafety program of USDA BSL-3 laboratories. Line managers in USDA are responsible for implementing operational biosafety programs, with direct oversight assigned to researchers and diagnosticians. Line managers provide resources for training, implementation, and monitoring of biosafety policies and programs. Individual researchers or diagnosticians play the primary role for day-to-day biosafety practices related to inventory management and security. Researchers and diagnosticians also oversee utilization of pathogens by technicians and other support staff. USDA collateral duty biosafety officers serve as a resource for biosafety program implementation, quality control, biosafety inspections, and training.

This Manual specifically establishes a biosecurity program that charges all those responsible for biosafety with parallel responsibilities for biosecurity. This biosecurity program will outline individual responsibilities to deter, detect, and respond to any security threat to ensure that pathogens are not removed illegally from the biocontainment facilities.

4 ABBREVIATIONS

ARS - Agricultural Research Service
APHIS - Animal and Plant Health Inspection Service
CDC - Centers for Disease Control and Prevention
CFR - Code of Federal Regulation
DOC - Department of Commerce
HCPs - High Consequence Pathogens
IATA - International Air Transport Association
ICAO - International Civil Aviation Organization
IDS - Intrusion Detections System
IRC - Incident Response Chief
ISSP - Information System Security Plan
LAN - Local Area Network
NACI - National Agency Check with Inquiry
NPI - National Pathogen Inventory
OSHA - Occupational Safety and Health Administration
OCIO - Office of Chief Information Officer
PSL - Personnel Security Level
USDA - U.S. Department of Agriculture

USPHS - U.S. Public Health Service
VPN - Virtual Private Network

4 DEFINITIONS

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

b Agency. A major program (non-administrative) organization within the Department (USDA) headed by an administrator who reports to the Secretary, Deputy Secretary, or an Under Secretary.

c Biosafety Level (BSL). A combination of work practices and physical containment requirements designed to reduce the risk of laboratory infection when working with infectious material. The degree of protection recommended is proportional to the risk associated with an agent. There are four biosafety levels. Biosafety Level 3-Agriculture (BSL-3Ag) contains an agriculture modification of BSL-3. Vaccine strains that have undergone multiple *in vivo* passages should not be considered avirulent simply because they are vaccine strains.

(1) BSL-1. Practices, safety equipment, and facility design and construction are appropriate for undergraduate and secondary educational training and teaching laboratories, and for other laboratories in which work is done with defined and characterized strains of viable microorganisms not known to consistently cause disease in healthy adult humans. *Bacillus subtilis*, *Naegleria gruberi*, infectious canine hepatitis virus, and exempt organisms under the National Institutes of Health Guidelines for Research Involving Recombinant DNA Molecules are representative of microorganisms meeting these criteria. Many agents not ordinarily associated with disease processes in humans are, however, opportunistic pathogens and may cause infection in the young, the aged, and immunodeficient or immunosuppressed individuals.

(2) BSL-2. Practices, equipment, and facility design and construction are applicable to clinical, diagnostic, teaching, and other laboratories in which work is done with the broad spectrum of indigenous moderate-risk agents that are present in the community and associated with human disease of varying severity. With good microbiological techniques, these agents can be used safely in activities conducted on the

open bench, provided the potential for producing splashes or aerosols is low. Hepatitis B virus (HBV), the salmonellae, and *Toxoplasma* spp. are representative of microorganisms assigned to this containment level. BSL-2 is appropriate when work is done with any human-derived blood, body fluids, tissues, or primary human cell lines where the presence of an infectious agent may be unknown. (Laboratory personnel working with human-derived materials should refer to the Occupational Safety and Health Administration (OSHA) *Bloodborne Pathogen Standards* [(2)] for specific required precautions.)

Primary hazards to personnel working with these agents relate to accidental percutaneous or mucous membrane exposures, or ingestion of infectious materials. Extreme caution should be taken with contaminated needles or sharp instruments. Even though organisms routinely manipulated at BSL-2 are not known to be transmissible by the aerosol route, procedures with aerosol or high splash potential that may increase the risk of such personnel exposure must be conducted in primary containment equipment, or in devices such as a biological safety cabinet or safety centrifuge cups. Other primary barriers should be used as appropriate, such as splash shields, face protection gowns, and gloves.

Secondary barriers such as hand washing sinks and waste decontamination facilities must be available to reduce potential environmental contamination.

(3) BSL-3. Practices, safety equipment, and facility design and construction are applicable to clinical, diagnostic, research, or production facilities in which work is done with indigenous or exotic agents with a potential for respiratory transmission, and which may cause serious and potentially lethal infection. *Mycobacterium tuberculosis*, St. Louis encephalitis virus, and *Coxiella burnetii* are representative of the microorganisms assigned to this level. Primary hazards to personnel working with these agents relate to autoinoculation, ingestion, and exposure to infectious aerosols.

At BSL-3, more emphasis is placed on primary and secondary barriers to protect personnel in contiguous areas, the community, and the environment from exposure to potentially infectious aerosols. For example, all laboratory manipulations should be performed in a biological safety cabinet or other enclosed equipment, such as a gas-tight
aerosol generation chamber. Secondary barriers for this level include controlled access to the laboratory and ventilation requirements that

minimize the release of infectious aerosols from the laboratory.

(4) BSL-3-Ag. There is a special concern for reducing the risk of environmental exposure to pathogens of consequence to agriculture. Therefore, USDA defined BSL-3-Ag criteria enhances containment described for BSL-3 by adding filtration of supply and exhaust air, sewage decontamination, exit personnel showers, and facility integrity testing. BSL-3-Ag is treated the same as BSL-3 for biosecurity purposes of this document.

(5) BSL-3 Facility. A facility constructed to provide containment for BSL-3 pathogens.

(6) BSL-4. Practices, safety equipment, and facility design and construction are applicable for work with dangerous and exotic agents that pose a high individual risk of life-threatening disease, which may be transmitted via the aerosol route and for which there is no available vaccine or therapy. Agents with a close or identical antigenic relationship to BSL-4 agents also should be handled at this level. When sufficient data are obtained, work with these agents may continue at this level or at a lower level. Viruses such as Marburg or Congo-Crimean hemorrhagic fever are manipulated at BSL-4.

The primary hazards to personnel working with BSL-4 agents are respiratory exposure to infectious aerosols, mucous membrane or broken skin exposure to infectious droplets, and autoinoculation. All manipulations of potentially infectious diagnostic materials, isolates, and naturally or experimentally infected animals, pose a high risk of exposure and infection to laboratory personnel, the community, and the environment.

The laboratory director is specifically and primarily responsible for the safe operation of the laboratory. His/her knowledge and judgment are critical in assessing risks and appropriately applying these recommendations. The recommended biosafety level represents those conditions under which the agent can ordinarily be safely handled. Special characteristics of the agents used, the training and experience of personnel, and the nature or function of the laboratory may further influence the director in applying these recommendations.

(7) BSL-3 Pathogens. For purpose of this Manual, all BSL-3 agents will be considered as HCPs.

d Chain of Custody. The serial holders of a pathogen, each of who is responsible for securing the pathogen and are accountable for its documentation.

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

f Incident Response Chief (IRC). USDA Center Director or Laboratory Director responsible for incident control.

g Infectious Biological Material. Infectious substances (also referred to as etiologic agents) as defined by the U.S. Public Health Service (USPHS):

A substance containing or suspected of containing an infectious virus, prion, or a viable microorganism, such as a bacterium, rickettsia, parasite, fungus, or protozoan that is known or reasonably believed to cause disease in humans. Toxins known to be pathogenic to humans are to be packaged and shipped as infectious substances.

For purposes of USDA policy, this includes any subunits or genetic elements of BSL-3 pathogens if those subunits or genetic elements, if inserted into an appropriate host system, are reasonably believed capable of causing disease or toxicosis in livestock, poultry, and crops.

h "Select Agents" as defined by USPHS:

Prior to the shipment of any biological material to any destination within the United States, the designated shipper must first check to see if the biological material is classified as a Select Agent under the updated 42 CFR Part 72.6, Additional Requirements for Facilities Transferring or Receiving Select Agents. Select Agents are listed in Appendix A, to Part 72 -- Select Agents (http://www.cdc.gov/od/ohs/lrsat/42cfr72.htm# Appendix A). If the agent is classified as a Select Agent, the designated shipper must receive authorization from the USDA designee before shipping. All rules outlined in 42 CFR 72 must be followed. It is the responsibility of the USDA designee to assure that the transfer of any USPHS Select Agents from USDA facilities is accomplished in adherence with the current regulations.

i Organisms. All cultures or collections of organisms or their derivatives that introduce or disseminate any contagious or infectious disease of animals including poultry.

j Vectors. Vector- A carrier, usually an arthropod in biology, that transfers an infective 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.

k Intrusion Detection System. A system designed to detect unauthorized entry and to send an alarm.

l Guard Post Orders and Special Instructions. Detailed 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.

m Personnel Security Level (PSL). Designation assigned to positions that are located at BSL-3 facilities. The designations are commensurate with low, moderate, and high-risk levels of public trust and have similar investigative requirements.

(1) PSL-1. Personnel assigned to positions with BSL-3 facility/center/complex, but whose duties do not involve access to BSL-3 pathogens shall, at a minimum, be determined to encumber low risk public trust positions.

(2) PSL-2. Personnel assigned to positions that have access to or work with BSL-3 facilities or that have access to or work with BSL-3 pathogens shall, at a minimum, be determined to encumber moderate risk public trust positions.

(3) PSL-3. Personnel who are assigned to leadership/supervisory positions and who plan, report, and control research and access to BSL-3 facilities and pathogens shall be determined to encumber high risk public trust positions.

6 RESPONSIBILITIES

a All USDA personnel at BSL-3 facilities are responsible for security of USDA assets. Line managers in USDA are responsible for implementing and managing biosecurity programs with direct oversight assigned to researchers and diagnosticians.

The biosecurity program will outline individual responsibility to deter, detect, and respond to any security threat to ensure that pathogens are not removed illegally from the biocontainment facilities. The following agency positions have responsibility for ensuring biosecurity procedures and policies are implemented:

b Agency Biosafety Officer or Equivalent. Must ensure USDA biosafety and biosecurity policies are adhered to at all agency locations.

c Agency Heads. Agency heads are responsible for ensuring that their organizations adhere to USDA biosafety and biosecurity policies and procedures as outlined in this Manual.

d Deputy Administrators. Must ensure USDA biosafety and biosecurity policies are implemented at all sub-agency levels.

e Center Director, Laboratory Chief or Director, or Research Leader. Must ensure effective biosafety and biosecurity implementation at their facility or institute.

f Location Biosafety/Biosecurity/Quarantine Officer. Must work with local line managers to ensure laboratories are adhering to agency policy on pathogen inventories.

g Scientists. Must ensure that all pathogens used in their laboratories are entered in the repository database and that repository records are current and reflect the materials on hand.

7 AUTHORITIES, REFERENCES, AND ORGANIZATIONS

a Authorities. All Code of Federal Regulation (CFR) citations can be accessed via the Internet at http://www.access.gpo.gov/nara/cfr/cfr-table-search.html#page1

b Biosafety Levels, Risk Assessment, and Agent Summary Statements.

Biosafety in Microbiological and Biomedical Laboratories,
4th Edition
Published by the Office of Biological Safety, CDC,
Stock Number 017-040-00547-4 available from: U.S. Superintendent of Documents
U.S. Government Printing Office Washington, D.C. 20402 202-275-3318

c Control List.

9 CFR 122, APHIS Veterinary Services, National Center for Import and Export.

USDA, APHIS
Veterinary Services, National Center for Imports and Exports,
Products Program
4700 River Road, Unit 40
Riverdale, Maryland USA 20737
http://www.aphis.USDA.gov/OA/imexdir.html

7 CFR 330.200 Subpart M-Movement of Plant Pests Regulated; permits required.

USDA, APHIS
Plant Protection and Quarantine
4700 River Road, Unit 133
Riverdale, Maryland USA 20737
http://www.aphis.USDA.gov/ppq/permits

d Personnel Suitability/Security.

The National Security Act of 1947, dated July 26, 1947, as amended.

Executive Order 12968 access to classified information, August 4, 1995.

5 CFR 731, suitability regulations, revised March 19, 2001.

5 CFR 732, national security positions, revised January 1, 2001.

32 CFR 147, adjudicative guidelines for determining eligibility for access to classified information, July 1, 1999.

Executive Order 10450 security requirement for Government employees, April 27, 1953.

e Physical Security.

41 CFR Chapter 101, Federal Property Management Regulations.

7 CFR Part 2, Delegations of Authority by the Secretary of Agriculture and general officers of the Department.

Interagency Security Committee Security Design Criteria,
May 28, 2001.

f Shipping.

9 CFR 122, APHIS, Veterinary Services, National Center for Import and Export.

USDA, APHIS
Veterinary Services, National Center for Imports and Exports,
Products Program
4700 River Road, Unit 40
Riverdale, Maryland USA 20737
http://www.aphis.USDA.gov/OA/imexdir.html

7 CFR 330.200 Subpart M-Movement of Plant Pests Regulated; permits required.

USDA, APHIS
Plant Protection and Quarantine
4700 River Road, Unit 133
Riverdale, Maryland USA 20737
http://www.aphis.USDA.gov/ppq/permits

49 CFR 171-180, U.S. Department of Transportation hazardous materials regulations.

49 CFR 173.143, Division 6.2, Definitions, exemptions, and packing group assignments.

42 CFR 72, Interstate Shipment of Etiologic Agents.
smtp://www.cdc.gov/od/ohs.biosfty/shipregs.htm

15 CFR 742, 744, and 774, DOC Control Policy and Commerce.

International Air Transport Association (IATA) Dangerous Goods

Regulations, 40th Edition, 1999.

39 CFR 111, U.S. Postal Service Domestic Mail Manual.

42 CFR 71, USPHS Foreign Quarantine.

42 CFR 71.54, Etiologic agents, hosts, and vectors.

IATA Dangerous Goods Regulations, 36th Edition, 1995
IATA Publications Assistant
2000 Peel Street
Montreal, Quebec, Canada H3A 2R4
514-844-3611 or 800-716-6326 (phone); 514-844-9089 (fax)
http://www.iata.org

International Civil Aviation Organization (ICAO) Technical Instructions for the Safe Transport of Dangerous Goods by Air,
1995-1996 Edition
ICAO Document Sales Unit
1000 Sherbrooke Street
Montreal, Quebec, Canada H3A 2R2
514-285-8022 (phone); 514-285-6769 (fax)
http://www.icao.int

Guidelines for the Safe Transport of Infectious Substances and Diagnostic Specimens
World Health Organization, 1997
http://www.who.int/emc/biosafety.html

g Work Practices, Training.

29 CFR 1910.1030, OSHA, Blood Borne Pathogen Standard.

8 INVENTORY CONTROL PROCEDURES

a Purpose. The purpose of this section is to set policy on the handling, storage, shipping, disposal, record keeping, and monitoring of all biological agents. The intent of this section is also to ensure proper chain of custody procedures are utilized.

(1) Accountability Records. Three types of accountability records are required: (a) a summary inventory at USDA agency headquarters, i.e., National Pathogen Inventory (NPI) system; b) a detailed inventory of repository materials to be kept at the research or diagnostic facility; and (c) materials accountability for experimental or working samples. Records in the first two systems 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 pathogens are present, or have been present in its facilities, to ensure the accountability of scientists for the pathogens they store and use, and to know the final disposition of pathogens, including destruction or shipping to another facility. The NPI will allow an agency to rapidly identify the facilities at which particular agents are in use. The format for each is described below:

(a) NPI. Agencies will maintain a summary inventory database, consisting of the limited fields listed below, to provide management with the capability to rapidly determine pathogens in use at each facility. USDA agencies will use an NPI system for this purpose.

Inventory records must include:

1 Agent name
2 Agency/Location/Laboratory
3 Person responsible for pathogenic material (laboratory supervisor)
4 Contact information

(b) Facility Inventory of Repository Materials. Each USDA facility that stores or uses any pathogen must maintain a current detailed inventory as outlined below. The information shall be maintained in a standard database format. Each facility will maintain a current master database reflecting the cumulative

pathogens of all management units at the facility. The database will not only serve as a record of current inventory but will also serve as a historical record of pathogens use at the facility. Placing records no longer in use in an inactive file rather than deleting them will accomplish this. Inactive records will be kept for at least 5 years. The Center or Laboratory Director for retention of BSL-3 pathogens in the inventory must review records annually.

Information to be included in the database is as follows:

1 Agent (scientific and common name and strain where applicable);

2 Amount (number of vials or contains inventoried);

3 Biosafety Level, Agent Type (bacteria, virus, etc.)

4 Storage location (building, room number, freezer number);

5 Storage conditions (refrigerator, freezer, -70^{o}C, -20^{o}C, liquid $N_{2.}$, etc.);

6 Date of change of status, i.e., removal, change of custody, etc.;

7 Site of usage (pinpoint to discrete locations such as building numbers and possibly room numbers);

8 Disposition including shipping when removed from inventory, including method of destruction, when applicable;

9 Scientist with contact information (telephone number and address of researcher or diagnostician).

Any working cultures that become new repository stocks must be added to the inventory. New pathogens (not already in inventory) identified in diagnostic or experimental samples or generated through recombinant technologies must be added to the repository and inventory database.

(c) 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 (laboratory notebooks, electronic systems, etc.). The location of material use must be included. At the conclusion of each experiment, the disposition of the infectious material, including the means of disposal, must be verified by the signature of the researcher or diagnostician, or their designee.

(2) Packaging and Shipping of Infectious Material. Packing and shipping of pathogens will meet current national and international regulations and guidelines, which are referenced in this Manual under Section 7, AUTHORTIES, REFERENCES, AND ORGANIZATIONS.

Shipping and receiving of pathogens will meet applicable guidelines and be tracked by each agency. Organisms and vectors may require an APHIS permit for transport (9 CFR Part 122 for Animal Pathogens and 7 CFR 330.200 for Plant Pathogens).

USDA laboratories employ a small number of agents designated by the CDC as select agents. Shipping and tracking of these agents will be done in accordance with CDC regulations found in 42 CFR Part 72.

The DOC regulations, including requirements for export permits, must be met for the export of pathogenic materials. The Biosafety Officer will review shipping records in the database on at least an annual basis to ensure compliance.

(3) Physical Review of Accountability Records. Scientists working with pathogens 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 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 is responsible for ensuring the physical reviews are accomplished. Random reviews shall be conducted on an annual basis by the agency Biosafety Officer to ensure compliance at the locations.

(4) Pathogen Security. All pathogens shall be stored in secure freezers within the facility. BSL-3 pathogens must be secured within the high containment facility. Only personnel with the appropriate PSL will

have access to freezer keys and codes. The biosafety level risk group or biosafety category of the storage unit will be determined by the highest risk pathogen within the storage unit.

(5) Sample Labeling. All sample vials in the inventory shall be labeled in a permanent manner so that all information is readable.

(6) Inactivation and Disposal of Pathogens. 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. All pathogens and contaminated supplies will be treated.

(7) Internal Transfer. A BSL-3 pathogen 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 pathogen database and all required records must be updated to document such transfers.

9 PHYSICAL SECURITY SYSTEMS

a Purpose. This sections sets policy to:

(1) Ensure appropriate levels of protection against unauthorized access, theft, diversion, or loss of custody of BSL-3 pathogens; loss or theft of information related to BSL-3 pathogens and other acts that may cause unacceptable adverse impacts on national security or on the health and safety of USDA employees, the public, or the environment;

(2) Provide levels of protection in a graded manner in accordance with the potential consequences;

(3) Ensure effective planning of graded protection levels and prudent application of resources.

BSL-3 pathogens are ubiquitous, existing both in nature and in laboratories around the world. However, it is prudent to limit access to BSL-3 pathogens and information related to BSL-3 pathogens to authorized individuals, and to deter and detect unauthorized access.

b Risk Assessment. The physical security system shall be designed according to a site-specific risk assessment, which will evaluate targets, adversary capabilities, consequences, and vulnerabilities. The risk assessment shall be developed by qualified individuals who have expertise in physical and biological security. The objectives and performance of the physical security system shall be reviewed regularly, but no less than every 5 years, by qualified individuals who have expertise in physical and biological security.

c Site-Specific Considerations. The physical security systems will be tailored to address site-specific characteristics and requirements, ongoing programs, and operational needs, and to achieve acceptable protection levels using current technology in a cost-effective manner. The protection strategy may be tailored to address varying circumstances and may range from prevention to pursuit.

d Graded Protection. Physical security systems shall provide graded protection in accordance with the importance of the asset. That is, USDA intends that the highest level of protection be given to security interests whose loss, theft, compromise, and/or unauthorized use will seriously affect the national security, and/or the health and safety of USDA employees, the public, the environment, or USDA programs. Therefore, protection of BSL-3 pathogens will be given the highest level of protection. Protection of other interests will have lower levels of protection.

It should be recognized that risks must be accepted (i.e., that actions cannot be taken to reduce the probability or consequences of all malevolent events to zero); however, an acceptable level of risk should be determined based on evaluation of a variety of facility-specific goals and considerations. Protection-related plans shall describe, justify, and document the graded protection provided to BSL-3 pathogens and information related to BSL-3 pathogens. The plans shall be reviewed and updated annually.

The nature of the threat, the vulnerability of the asset, and the potential consequences of an adversarial act shall be considered in determining the appropriate level of protection against risk. Accordingly, physical security systems shall provide graded protection in accordance with the importance of the asset.

Consequently, facilities shall consolidate BSL-3 pathogens, concentrate intrusion detection and assessment systems at the remaining locations where the BSL-3 pathogens are kept, and control access to these locations. To

maintain the continuity of operation, the protection strategy shall be to mitigate the severity of the event through response and recovery option planning.

e Security and Restricted Access Areas. Unescorted access shall be limited to authorized individuals. Any unauthorized individual will be escorted at all times by an authorized individual. Local authorities shall establish appropriate escort-to-visitor ratios.

Controls shall be established to detect, assess, and deter unauthorized access to security areas. Access control requirements may be layered as appropriate for the situation. At succeeding boundaries, access controls may be increased. Means shall be provided to deter and detect unauthorized intrusion into limited and exclusion areas as defined below. Means include: use of intrusion detection sensors and alarm systems, random patrols, and/or visual observation. The protection program shall include suitable means to assess alarms.

f 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 shall be identified, and signs prohibiting trespassing shall be posted. Physical barriers, where determined to be necessary by local authority, shall be used to protect property and facilities.

All buildings in the property protection area must be locked and security keys shall be protected. An accountability system for security keys shall be implemented.

g Limited Area--Intermediate Level of Protection. A limited area shall 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 that contains an exclusion area.

Access to a limited area shall require a unique item (i.e., proximity card) and an appropriate level of intrusion detection. Sufficient exterior lighting should be provided to allow the protective force to detect and assess intrusions.

h Exclusion Area--Highest Level of Protection. An exclusion area shall 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 BSL-3 pathogens or information related to BSL-3 pathogens.

Access to an exclusion area shall require a unique item (i.e., proximity card) and unique knowledge (i.e., personal identification number), and an appropriate level of intrusion detection. Access control and intrusion detection shall be administered by protective personnel and/or automated systems.

i Storage. BSL-3 pathogens and information related to BSL-3 pathogens shall be stored in an exclusion area and secured within a locked security container or locked room.

j Access Control and Entry/Exit Inspections. Access control points shall be designed to provide positive control over pedestrian traffic. The access control points shall provide a barrier to personnel entering limited areas and exclusion areas until such time as entry is requested and/or authorized. Automated access control systems shall read data entered by the person requesting access, and if the data are successfully validated, the portal shall be electrically unlocked.

A security badge that electronically stores information relevant to the badge and badge holder shall be used for automated access control systems. The access authorization list shall be updated when an individual's access authorization has changed or when an individual is transferred or reassigned. Badge readers shall be equipped with anti-pass back protection.

Door locks opened by badge readers shall be designed to relock immediately after the door has closed to deter another person from opening the door without following procedures.

The system shall record all transactions--authorized access (for tracking purposes) and attempted unauthorized access.

Keypad devices shall have a visual shielding device mounted so that an unauthorized person in the immediate vicinity cannot observe the numbers entered.

k Intrusion Detection and Assessment Systems. Intrusion detection systems

shall be installed to provide reasonable assurance that breaches of security boundaries are detected and that assessment information is provided to protective personnel.

A means for timely detection of intrusion shall be provided by the use of intrusion detection systems and/or protective force fixed posts and/or mobile patrols. Assessment of intrusion detection system alarms shall be provided by patrols and/or closed circuit television. When used for detection, patrols shall be conducted at random intervals at a documented frequency.

Intrusion detection systems shall provide operable coverage in all local environmental conditions.

There shall be an effective method by which to assess intrusion detection system alarms (e.g., intrusion, false, nuisance, and tamper).

Response capability to intrusion detection system alarms shall be provided to protect USDA BSL-3 pathogens and information related to BSL-3 pathogens. The response capability may be provided by assigned protective personnel or by the local law enforcement agency, as applicable. Response times shall be appropriate for the protection strategy employed at the site.

The intrusion detection systems shall be: (1) monitored continuously by assigned personnel to assess alarms and initiate appropriate responses; (2) operated and maintained in a manner ensuring that the number of false and nuisance alarms does not reduce the system credibility; and (3) tamper-resistant or tamper-alarmed. A facility possessing BSL-3 pathogens shall have line supervision for security sensors. The security sensors shall not be connected to an open computer network.

Compensatory measures shall 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.

Records shall be kept on each actual and/or false nuisance alarm. The record shall be reviewed, analysis performed, and corrective measures taken to correct system malfunctions. The record shall contain, at a minimum: date and time of the alarm, cause of the alarm or a probable cause if definite cause cannot be established, and the identity of the recorder or the operator on duty.

Alarm monitoring systems shall be self-checking and shall enunciate system failure in the alarm station. Systems shall indicate the type and location of

the alarm source.

Systems shall be functionally tested in accordance with established procedures at a frequency that is documented.

Doors and hatches which provide access to limited and exclusion areas shall be equipped with intrusion detection system devices. A balanced magnetic switch, or other equally effective device, shall be used on each door to provide detection of attempted or actual unauthorized access.

Panic hardware or emergency exit mechanisms used on emergency doors located in limited and exclusion areas shall be operable only from inside the building or room and shall meet all applicable life safety codes.

Windows which provide access to exclusion areas shall have intrusion detection sensors or 18-gauge expanded metal securely fastened on the inside. This also applies to doors with windows. All windows shall be closed and locked during non-working hours to preclude surreptitious entry.

Video recorders, when used, shall be activated by alarm signals operated automatically and sufficiently rapid to record an actual intrusion.

When used as the principal means of alarm assessment and to determine response level, closed-circuit television cameras shall have tamper-protection, loss-of-video alarm enunciation, and adequate lighting.

l Protection of Access Control and Intrusion Detection Systems.
Security-related equipment shall be protected from unauthorized access in a graded manner consistent with its importance; all detection/alarm devices and access control system components, including transmission lines to enunciators, shall be tamper-indicating in both the access and secure modes. System components used for protection of other interests shall be protected, consistent with a cost/benefit analysis determined by each facility. Electronics enclosures and junction boxes shall be: under lock and key control; have tamper switches; have tamper-resistant hardware; or be welded shut. Line supervision is required. Access to records and information concerning encoded data and personal identification numbers shall be restricted to authorized individuals. Records reflecting active assignments

of badges, personal identification numbers, levels of access, and similar system-related records shall be maintained. All records for access control and intrusion detection systems, including personnel removed from the system, shall be retained for 1 year.

m Auxiliary power sources**.** Auxiliary power shall be available and shall be capable of maintaining full operation of the intrusion detection and assessment system for 8 hours, or for such time as would be needed to implement contingency plans. The period of time necessary to implement contingency plans shall be documented. Auxiliary power sources shall have the capability to facilitate operational testing or routine maintenance.

Transfer to auxiliary power shall be automatic upon failure of the primary source and shall not effect operation of the security system or device. The alarm station shall receive an alarm indicating failure of the security system power and transfer to the auxiliary power source.

n Maintenance. Security-related subsystems and components shall be maintained in an operable condition. A regularly scheduled testing and maintenance program is required. Corrective maintenance shall be initiated within 72 hours of the indication of malfunction. The local cognizant USDA or agency authority for physical security systems shall determine if compensatory measures are necessary.

The following system elements shall be included in a preventive maintenance program: intrusion detection and assessment systems, central alarm station alarm enunciators, protective force equipment, personnel access control and inspection equipment, security lighting, and security system-related emergency power or auxiliary power supplies.

Personnel who test, maintain, or service security system elements shall have access authorization consistent with the protection level where the maintenance is being performed.

Records of testing shall be retained for 1 year.

o Performance Testing. Performance assurance programs shall provide for operability and effectiveness tests of security systems and/or components of systems. Testing frequencies shall reflect site-specific conditions, operational needs, and threat levels. However, at least annually, a performance test encompassing protection systems associated with a

comprehensive site or facility threat scenario shall be conducted to demonstrate overall facility physical security system effectiveness. This includes: integrated systems of equipment and hardware, administrative procedures, protective forces, and other staff.

The performance assurance program shall 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 BSL-3 pathogens and information related to BSL-3 pathogens.

p Response Forces. Response to intrusion detection alarms shall be by protective personnel, private security firms, or local law enforcement personnel, as documented in approved biosecurity incident response plans. If the response time by local law enforcement is inappropriate for the protection strategy, the on-site security force shall be armed.

q Duress Systems. Activation of duress alarms shall be accomplished in as unobtrusive a manner as practicable. Duress alarms shall not enunciate at the post initiating the duress alarm. Mobile duress alarms shall enunciate at the central alarm station.

r Radios. A continuous electronic recording system shall be provided for all security radio traffic. The logging recorder shall be equipped with a time track and shall cover all security channels. Portable radios shall be capable of two-way communication on the primary security channel from within critical buildings and structures--or an alternate means of communication shall be provided. Portable radios shall 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.

s Exit Inspections for Limited and Exclusion Zones. Personnel, vehicles, and hand-carried items, including packages, briefcases, purses, and lunch pails, shall be subject to random exit inspections to deter and detect unauthorized removal of BSL-3 pathogens and information related to BSL-3 pathogens from security areas.

t Prohibited Articles. The following articles are prohibited from BSL-3 areas, unless approved by the cognizant USDA local authority for physical security systems: any dangerous weapon, explosive, or other dangerous instrument

or material likely to produce substantial injury or damage to persons or property. Sites shall, at a minimum, employ administrative procedures to prohibit these articles.

u Visitor Logs. Visitor logs are required for limited areas and exclusion areas and shall be retained for 1 year.

10 CYBERSECURITY SYSTEMS

a Purpose. The purpose of this section is to set policy to:

(1) Ensure that the required and appropriate level of confidentiality, specifically information related to BSL-3 pathogens, is preserved by the system that is used to acquire, store, manipulate, manage, move, control, display, switch, interchange, receive, or transmit that information;

(2 Protect the physical, technical, and administrative controls and risk management processes that secure USDA information and information related to BSL-3 pathogens;

(3) Require that each USDA high-containment laboratory tailors the protection mechanisms, implementation, and security planning for its cybersecurity program to suit its environment, missions, and threats, while maintaining consistency and interoperability with USDA's overall cybersecurity policies and procedures;

(4) Ensure prudent application of resources.

The Department and its contractors shall systematically integrate cybersecurity into management and work practices at all levels so that missions are accomplished while protecting electronic information and electronic information systems. This is to be accomplished through effective integration of cybersecurity management into all facets of work planning and execution. In other words, the overall management of cybersecurity functions and activities shall become an integral part of mission accomplishment.

b Following are the general policies:

(1) Cyber Resource Protection. Each agency shall ensure that all USDA information resources, including USDA information related to high-consequence pathogens under its purview, are protected in a manner that is consistent with its threats and missions at all times.

(2) Risk Management. Each agency shall use a risk-based approach to identify information resources and specifically those that are related to BSL-3 pathogens. A documented risk assessment process shall be used to make informed decisions related to the adequacy of protection, cost implications of further enhanced protection, and acceptance of residual risk.

(3) Resources. Each agency shall plan, budget, allocate, and execute resources sufficient to ensure comprehensive implementation and maintenance of that organization's computer security program.

(4) Cybersecurity Program Plan. Each agency shall document its cybersecurity program in an Information System Security Plan (ISSP). The ISSP shall be approved by the organization's local director, field office, and the Office of the Chief Information Officer (OCIO), Cybersecurity. USDA agencies may revise their ISSPs as required by new operational considerations, risks, vulnerabilities, etc. Each agency shall submit the revised ISSP to its local director, field office, and to OCIO, Cybersecurity, for approval.

(5) ISSP Assessment and Review. To ensure that the ISSP is properly implemented, it shall be subject to the following reviews:

1 Implementation of the ISSP shall be internally reviewed no less frequently than once every year.

2 The appropriate field office shall review the ISSP at least once every 3 years.

3 Finally, the USDA Chief Information Officer shall maintain a continuous program of independent oversight for cybersecurity. The independent oversight program will include announced and unannounced cybersecurity inspections, follow-up reviews, remote testing for network vulnerabilities (network scanning), and penetration testing.

(6) Corrective Action Plans. Each agency shall draft and implement corrective action plans to address security shortfalls revealed as a result of the oversight review process. The corrective action plans shall include actions to be taken, responsible organizations and individuals for each action, the schedule (including key milestones), actions to address

root causes and generic applicability, a process for tracking actions to

closure, and steps to verify effectiveness of actions prior to closure.

(7) User Authentication. Each agency shall employ user authentication techniques before allowing users to access systems that support multiple-user accounts or that contain hard-to-replace or sensitive data. The organization's ISSP shall indicate the systems or enclaves that require authentication and the type of authentication that shall be employed.

(8) Access Protection. Access to each agency's information resources shall be protected commensurate with the risks and threats of its environment. The ISSP shall specify the information resources to be protected and the protective mechanisms to be used.

(9) Auditing. Each agency shall be capable of recording and maintaining in an audit trail information regarding access to and modifications of all information resources, where this is identified as appropriate by risk and vulnerability analysis, and such capability is technically feasible. The ISSP shall state the systems or enclaves that shall be audited, what information shall be captured in that audit trail, and how long the audit trail shall be maintained.

(10) Continuity of Service. Each agency shall employ procedures and mechanisms to curtail or recover from activities that can disrupt or otherwise interfere with system availability, where operationally necessary and technically feasible. The ISSP shall identify the organization's systems and enclaves that require such mechanisms and procedures and shall detail the procedures and mechanisms employed.

(11) Security Monitoring and Reporting. Each agency shall report security incidents to the OCIO, Cybersecurity. In addition, each agency shall provide 24-hour-a-day, 7-day-a-week monitoring of cybersecurity activities. The ISSP shall specify the type of events that require monitoring, the enclaves and systems that will be subject to monitoring, how the 24x7 monitoring will be handled, and the composition of the organization incident response team.

(12) Training. Personnel from agencies and contractors shall be appropriately trained in cybersecurity vulnerabilities, threats, protection strategies, and respective organizational and personal responsibilities. The ISSP shall specify the details of the training program.

(13) Malicious Code. Each agency shall establish procedures and mechanisms consistent with the threat environment, to limit (as

technically feasible) the introduction of malicious code into its information systems. The ISSP shall specify the mechanisms used to detect and deter the installation of malicious code and the frequency of updating such mechanisms.

(14) System Administrator. Each USDA organization shall have a system administrator, who is responsible for developing, updating, and implementing the ISSP; monitoring cybersecurity activities locally; responding to cyber incidents in coordination with the appropriate headquarters oversight office; and ensuring that there is local understanding of USDA cybersecurity policies and procedures.

c The following are the specific policies that should be documented in the ISSP:

(1) Modem Use. All connections to the outside world, including modems, shall go through a firewall. Modems that are not needed for day-to-day work shall not be plugged into the phone system. If a modem is needed for outbound traffic only, the internal call-in ability shall be disabled. Systems with modems that are both on the Local Area Network (LAN) and are used for day-to-day dial up to additional networks shall have a personal firewall installed to deny access from one network to the other.

(2) Anti-Virus Software. All systems shall have a virus scanner installed. This virus scanner shall be enabled to automatically update either directly or via a virus-scanner proxy. All E-mail shall be virus checked before it is delivered in or out of the LAN.

(3) Password Policy. Passwords cannot be dictionary words or common names, and they cannot be the same as the login name. They shall be eight characters or more. If the system is in an open or public area, the system shall also be protected by a boot-up password. Passwords shall not be kept anywhere near the system or anywhere in the open. Passwords for networked computers shall be changed every 60 days. Systems in open or public areas shall have a locking screensaver; systems in locking offices should have a locking screensaver.

(4) External Network. Servers that are open to the public (such as external Web servers, E-mail servers, File Transfer Protocol servers) shall be on an isolated (external) network segment. A firewall shall be used and/or each system shall be secured to the maximum level possible at both the operating system and application level. Only public data can be on this network.

All Web servers shall have the Web content reviewed before public

release. This is to ensure that details about the laboratory's facility and security system are not openly available, and information related to personnel and those who work with BSL-3 pathogens is kept to an absolute minimum.

(5) Internet Network. The internal systems and servers shall be on an isolated (internal) network that is fire walled. There shall be very little to no traffic entering this network segment. If the internal network needs to be open to an outside individual, an encrypted tunnel such as a Virtual Private Network (VPN) shall be used. Only select traffic shall be allowed to travel from the external network to the internal network.

(6) Remote Access. If a user needs to access the internal network from a remote location, a VPN transport or equivalent solution shall be utilized. The system at the user's end shall use "VPN client" or an equivalent. The network end can use VPN tunneling or an equivalent. Systems on both ends of the VPN shall comply with this security policy.

(7) E-mail Policy. All E-mail sent and received from an outside network shall be treated as open to public view. Sensitive data traveling on the Internet shall be encrypted; this includes E-mail and work performed by remote network users.

(8) Outbound Access. Only necessary traffic shall be permitted to leave the internal network. Necessary traffic may include: Web browsing, E-mail, File Transfer Protocol servers, and other standard Internet applications.

(9) Intrusion Detection. Intrusion detection on the network is critical to verify the security measures are working. An Intrusion Detections System (IDS) shall be installed on the internal network. An IDS system shall also be installed on the external network. The System Administrator shall review the IDS's logs and monitor unusual network traffic. Constant analysis is critical to securing and maintaining the security on a network.

11 PERSONNEL SUITABILITY

a Purpose. This section sets policy on suitability requirements for USDA and non-USDA personnel requiring access to BSL-3 facilities.

(1) Background Investigations. Following Office of Procurement Policy Management instructions, the following investigations will be conducted

to determine the personnel suitability:

(a) PSL1-National Agency Check with Inquiry (NACI) - [Low Risk Public Trust]

(b) PSL-2-Limited Background Investigation – [Moderate Risk Public Trust]

(c) PSL-3-Background Investigation – [High Risk Public Trust]

(2) Pre-employment**.** Recruitment announcements will notify all candidates for permanent and non-permanent positions that the position is located within a BSL-3 facility and appointment to the position is subject to a background investigation.

A pre-employment Special Agency Check must be completed for all PSL-2 and PSL-3 selectees prior to appointment. An appointee to PSL-1 positions may have the NACI completed after entering on duty.

(3) USDA Employees. Appointees to PSL-2 and PSL-3 positions must have a completed and favorably adjudicated background investigation prior to assuming duties with the BSL-3 facility. New appointees may be assigned duties outside the BSL-3 area or may have access to a BSL-3 area only if escorted into the BSL-3 facility by a staff member who has a completed background investigation and appropriate facility authorization.

Note: Personnel who have been granted a secret or top secret clearance level may be authorized unescorted access to the BSL-3 facility upon receipt of their security clearance.

(4) Non-USDA Personnel. Includes personnel from universities, cooperators, contractors, students, visiting scientists, laboratory visitors, seminar attendees, etc. Non-USDA personnel will be escorted all times by staff members who have a completed background investigation and appropriate facility authorization.

Note: Facility managers may authorize non-USDA personnel unescorted access if the non-USDA personnel have appropriate background investigations.

12 BIOSECURITY INCIDENT RESPONSE PLAN

a Purpose**.** This section sets policy for responses to specific types of incidents in order to protect personnel and secure pathogen holdings.

b The biosecurity plan must include responses to the following types of incident:

(1) Biocontainment breach
(2) Biocontainment security breach
(3) Inventory violation
(4) Non-biological incident such as violence
(5) Cybersecurity breach

c The plan must address the following issues:

(1) Personnel safety and health
(2) Containment
(3) Inventory control
(3) Notification of managers and responders

d Each organizational level responsible for a BSL-3 facility will submit a biosecurity incident response plan to headquarters for review.

The determination of a biosecurity incident is by the Incident Response Chief (IRC) who must be notified by phone call or in person of a potential incident. The IRC, after investigation, will determine if a biosecurity incident has occurred. If a potential threat exists to either facilities or personnel, the IRC will notify the Federal Protective Service, local police, and the USDA Office of Inspector General.