United States Department of Agriculture

Agricultural Research Service

DM 9610-2

USDA Security Policies and Procedures For Laboratories and Technical Facilities (Excluding Biosafety Level (BSL)-3 Facilities)

USDA SECURITY POLICIES AND PROCEDURES FOR LABORATORIES AND TECHNICAL FACILITIES (EXCLUDING BIOSAFETY LEVEL (BSL)-3 FACILITIES)

TABLE OF CONTENTS

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

DEPARTMENTAL MANUAL Number 9610-2

SUBJECT: USDA Security Policies and Procedures For Laboratories and Technical Facilities (Excluding Biosafety Level (BSL)-3 Facilities)

Date: April 30, 2003

OPI: Agricultural Research Service

1. PURPOSE

This Departmental Manual establishes the U.S. Department of Agriculture (USDA) policy for the security of critical assets (e g , equipment, facilities, functions, personnel, and/or research or regulatory material/projects) with the exception of Biosafety Level (BSL)-3 facilities, which are covered in USDA policies and procedures, USDA Security Policies and Procedures for Biosafety Level-3 Facilities, and can be found at http://www.usda.gov/ocio/directives/DM/DM9610-001.htm

This Manual includes guidance on the risk management approach and assigns responsibilities for implementation to protect USDA assets. The risk management approach is a systematic process to analyze threats, risks, and criticality of assets; to assess consequences and vulnerabilities; and to recommend security countermeasures to support key decisions linking resources with prioritized efforts for the most effective results.

2. SCOPE

This Departmental Manual applies to all USDA organizational elements and their employees. This Manual also applies to USDA facilities operated on behalf of the USDA by State and local government, universities, contractors, or other private organizations to accomplish a USDA function. Finally, human reliability standards apply to anyone involved in the design, development, acquisition, installation, operation, maintenance and use of USDA security systems and countermeasures. It does not apply to purely administrative facilities.

3. INTRODUCTION

It is the policy of USDA to ensure appropriate levels of protection against unauthorized access to USDA facilities; prevent the theft, diversion, or loss of USDA property; and prevent 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.

To accomplish this, USDA intends to use a "Risk Management Approach" to address USDA physical security requirements. As defined by the General Accounting Office (GAO), Risk Management is a systematic and structured process to consider the likelihood that a threat will endanger an asset (e.g., a structure, individual, or function) and to identify actions that reduce the risk and mitigate the consequences of an adverse action /security breach.

The process begins with the identification of the assets to be protected. For pathogens, this includes an identification of pathogens. Also, this includes an identification of the risk involved if there is a release of the pathogen into the environment, either accidental or deliberate.

An effective Risk Management Plan consists of a threat, vulnerability, and criticality assessment. A threat assessment identifies and evaluates various threats and the probability of their occurrence; a vulnerability assessment identifies weakness that may be exploited and suggests countermeasures to eliminate or mitigate these weaknesses; and a criticality assessment provides the basis for prioritizing assets when resources for addressing vulnerabilities are insufficient.

4. ABBREVIATIONS

APHIS	- Animal and Plant Health Inspection Service
AGPMR	- Agriculture Property Management Regulations
BI	- Background Investigation
BMBL	- Biosafety in Microbiological and Biomedical Laboratories
BSL	- Biosafety Level
CDC	- Centers for Disease Control and Prevention
CFR	- Code of Federal Regulations
CIP	- Chemical Inventory Program
DOC	- Department of Commerce
GAO	- General Accounting Office
GSA	- General Services Administration
IATA	- International Air Transport Association
IDS	- Intrusion Detection System
IRC	- Incident Response Chief
ISC	- Interagency Security Committee
ISSP	- Information System Security Plan
LAN	- Local Area Network
LBI	- Limited Background Investigation
NACI	- National Agency Check and Inquiry
NPI	- National Pathogen Inventory
NRC	- Nuclear Regulatory Commission
OCIO	- Office of Chief Information Officer
OIG	- Office of Inspector General

OPM	- Office of Personnel Management
OSHA	- Occupational Safety and Health Administration
PSL	- Personnel Suitability Levels
PTP	- Public Trust Position
SOPS	- Standard Operating Procedures
USDA	- U.S. Department of Agriculture
USDOT	- U.S. Department of Transportation
USPHS	- U.S. Public Health Service
USPS	- U.S. Postal Service
VPN	- Virtual Private Network

5. DEFINITIONS

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

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

c. Asset. Any USDA property or resource, the loss or theft of which could pose potential harm or threat to the general public.

d. Biological Agent. Any microorganism (including, but not limited to, bacteria, viruses, fungi, rickettsiae, or protozoa), or infectious substance, or any naturally occurring, bioengineered, or synthesized component of any such microorganism or infectious substance, capable of causing:

(1) Death, disease, or other biological malfunction in a human, an animal, a plant or a another living organism;
(2) Deterioration of food, water, equipment, supplies, or material of any kind; or;
(3) Deleterious alteration of the environment.

e. Biocontainment. Work practices and construction designed to reduce the risk of an agent escaping into the environment.

f. Biosafety. Development and implementation of administrative policies, work practices, facility design, and safety equipment to prevent transmission of biologic agents to workers, other persons, and the environment.

g. 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. Only non-BSL-3 pathogens are covered by this Manual.

h. 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.

i. 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 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,

j. 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.

k. Biosecurity. Protection of high-consequence microbial agents and toxins, or critical relevant information, against theft or diversion by those who intend to pursue intentional misuse.

l. Chain of Custody. The serial holders of an asset, each of whom are responsible for securing the asset and are accountable for its documentation.

m. Chemical Agent. Any element, chemical compound or mixture of elements and/or compounds. (29 CFR Part 1200)

n. Concentric Rings. Defined physical boundaries delineating increased security requirements.

o. Gap Analysis. An evaluation to determine the void or difference that exists between the optimal requirements and the existing security processes.

p. Guard Post Orders and Special Instructions. Detailed instructions to the guard force detailing 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.

q. High-Security Facility. Refers to a USDA facility that has, by nature of the pathogens, programs, or materials housed therein, been determined by the Department to require special security measures to ensure the integrity of the facility, including the suitability of all individuals having access to the facility.

r. Incident Response Chief (IRC). A USDA designated agency official responsible for incident control.

s. Infectious Biological Material. Infectious substances (also referred to as etiologic agents) 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, protozoan, or fungus, that is known or reasonably believed to cause disease in humans. Toxins known to be hazardous to humans are to be packaged and shipped as infectious substances.

For purposes of USDA policy, this includes any subunits or genetic elements of pathogens if those subunits or genetic elements, if inserted into an appropriate host system, are reasonably believed to be capable of causing disease or toxicosis.

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

u. Pathogen. Synonymous with Biological Agent.

v. Public Trust Position (PTP). A position that can potentially affect public confidence in the government's integrity, efficiency, and effectiveness, whether or not the actual damage occurs, based on the action or inaction of the incumbent. Public Trust positions are designated Low Risk, Moderate Risk, and High Risk. Public trust classifications do not substitute for National Security Clearances and do not provide access to classified information. In the P&P for BSL-3 facilities, these are referred to as Personnel Suitability Levels (PSL).

(1) Low Risk. Positions that involve duties with the potential for limited impact on agency or program mission, or on the integrity and efficiency of the service.

(2) Moderate Risk. Positions with duties that are of considerable importance to the agency or program mission with significant program responsibility or delivery of service. Positions with the potential for moderate to serious impact on the integrity and efficiency of the service including:

- Investigative or law enforcement responsibilities; duties require carrying a firearm;
- assistants to policy development and implementation;
- mid-level management duties;
- responsibility for independent or semi-independent action; and/or
- delivery of service positions that demand public confidence or trust.

(3) High Risk**.** Positions with duties that have a broad scope of responsibility and authority which are especially critical to the agency or program mission. Positions with potential for exceptionally serious impact on the integrity and efficiency of the service including:

- policy-making, policy-determining, and policy-implementing;
- higher level management duties/ assignments, or major program responsibility; and/or
- independent spokesperson or non-management positions with authority for independent action.

w. Radioactive Material. A substance that emits ionizing radiation in the form of alpha particles, beta particles, neutrons, x-rays, or gamma rays. (USDA Safety and Health Manual -Radiation Safety Program Section)

x. Risk Management. A systematic and structured process to consider the likelihood that a threat will endanger an asset (e.g., a structure, individual, function, or item) and to identify actions that reduce the risk and mitigate the consequences of an attack.

y. Select Agents. In accordance with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (PUB. L. 107-188) CDC and USDA have established a "Select Agent" listing of biological agents and toxins and established regulations and requirements for handling these agents. Select Agents, which are human pathogens, are handled according to USPHS requirements. Agricultural Select Agents are handled according to APHIS requirements. Agricultural select agents are defined by the Secretary under the authority of the Agricultural Bioterrorism Protection Act of 2002, which is a subtitle of the Public Health Security and Bioterrorism Preparedness and Response Act. These Select Agents are not restricted to BSL-3 laboratories but, are nevertheless, deemed of particular sensitivity by the USDA--*Bacillus anthracis* is an example. A list of Select Agents can be found in 7CFR 33 1.3 for plant biological agents and toxins, 9 CFR 121.3 for animal biological agents and toxins, and 42 CFR 73 for human biological agents.

z. Suitability. An individual's character, reputation, trustworthiness, and fitness for overall employment as related to the efficiency of the service.

aa. Vectors. 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.

6. RESPONSIBILITIES

All USDA personnel are responsible for security of USDA assets. Line managers in USDA are responsible for implementing and managing security and biosafety programs. The Agency security program will outline individual responsibility to deter, detect, and respond to any security threat. Each USDA laboratory and technical facility shall create or modify an existing plan for security. That plan must include inventory control

procedures, physical security systems, cybersecurity systems, personnel suitability, and incident response plans. Where applicable, the security plan shall also include or reference a biosecurity plan, a chemical security plan and a radiological plan.

a. The following Agency positions have responsibility for ensuring security procedures and policies are implemented:

(1) Agency Biosafety Officer or Equivalent - Must ensure adherence to USDA security and biosafety policy at all agency, or equivalent locations.
(2) Agency Heads or Equivalent - Agency heads are responsible for ensuring that their organizations adhere to USDA security and biosafety policies and procedures as outlined in this Manual. Agency Heads will approve the security plan.
(3) Center Director, Laboratory Chief or Director, or Research Leader or Equivalent - Must ensure effective security and bio-safety implementation at their facility or institute.
(4) Deputy Administrators of Equivalent - Must ensure USDA security and biosafety policy is implemented at all sub-agency levels.
(5) Location Biosafety/Biosecurity/Quarantine Officer - Must work with local line managers to ensure laboratories adhere to agency policy on security and pathogen inventories.
(6) Scientists - Must ensure that all security procedures are followed and all assets used in their laboratories are entered into the repository database and that repository records are current and reflect the materials on hand also to ensure chain of custody is not compromised.

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 (BMBL), 4th Edition
Published by the Office of Biological Safety, Centers for Disease Control and Prevention (CDC)
Stock number 0 17-040-00547-4 available from: U.S. Superintendent of Documents
US. Govt. Printing Office Washington, D.C. 20402 202-275-3318

c. Control List.

7 CFR 330.200 Subpart M-Movement of Plant Pests Regulated; permits required;
7 CFR 331, Possession, Use, and Transfer of Biological Agents and Toxins.

USDA, APHIS
Plant Protection and Quarantine
4700 River Road, Unit 133
Riverdale, Maryland USA 20237-1236
http://www.aphis.USDA.gov/ppq/permits

9 CFR 121, Possession, Use, and Transfer of Biological Agents and Toxins; 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 20737-3277
http://www.aphis.USDA.gov/OA/imexdir.html

42 CFR 73, Possession, Use and Transfer of Select Agents and Toxins

HHS, CDC
Office of Health and Safety, Center for Disease Control & Prevention
1600 Clifton Road, N.E.
Atlanta, GA 30333

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 (ISC) Security Design Criteria, May 28, 2001
GAO - Testimony Before Congress -Homeland Security, A Framework for Addressing the Nation's Efforts - GAO-01-115ST

Agriculture Property Management Regulations (AGPMR 104.50.1)

Building Safety/Security Occupant Emergency Program, Departmental Regulation 1650-002

10 CFR Part 20, "Standard Protection Against Radiation"

f. Property.

AGPMR 104.50.1

S 104-50.301-1 Accountable Property

S 104-50.001-10 Sensitive Personal Property

g. Shipping.

49 CFR 171-180, U.S. Department of Transportation (USDOT) 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.html

Animal and Plant Health Inspection Service
7 CFR Part 331, "Possession of Biological Agents and Toxins"
9 CFR Part 121, "Possession of Biological Agents and Toxins"

15 CFR 742,744, and 774, Department of Commerce (DOC) Control Policy and Commerce

39 CFR 111. USPS Domestic Mail Manual

42 CFR 71, USPHS Foreign Quarantine

42 CFR 71.54, Etiologic agents, hosts, and vectors

IATA Dangerous Goods Regulations, latest edition
IATA Publications Assistant
2000 Peel Street
Montreal, Quebec, Canada H3A 2R4
514-844-361 1 or 800-716-6326 (phone); 514-844-9089 (fax)
http://www.iata.org

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

h. Work Practices, Training.

29 CFR 1910.1030, OSHA, Blood Borne Pathogen Standard

8. ASSET ACCOUNTABILITY

a. Purpose. The purpose of this section is to set policy on the handling, storage, shipping, disposal, record keeping, and monitoring of assets that may pose biological, chemical, radiological, or physical threat. The intent of this section is also to ensure that proper chain of custody procedures are utilized for Select Agents.

(1) Accountability Records for Pathogens. Three types of accountability records are required: (1) a summary inventory at USDA agency headquarters, i.e., National Pathogen Inventory (NPI) system; (2) a detailed inventory of repository materials to be kept at the research or diagnostic facility which should be updated yearly; and (3) materials accountability for Select Agent pathogens in experimental or working stocks. In this Manual, the term "Select Agents" refers to those Select Agents that are classified at a BSL-2 level. 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 or equivalent, is aware 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 be aware of 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) National Pathogen Inventory (NPI). Agencies or equivalent will maintain a summary inventory database, consisting of the limited fields listed below, to provide management with the capability to rapidly determine biological materials in use at each facility or equivalent. 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 biological agents 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 used at the facility. This will be accomplished by placing records no longer in use in an inactive file rather than deleting them.

Information to be included in the database is as follows:

1 Name of the organism, BSL, number of vials or other containers;
2 Storage location (building, room number, freezer number);
3 Storage condition (refrigerator, freezer, -70°C, -2O"C, liquid nitrogen, lyophilized and stored at room temperature or refrigerator temperature;
4 Date of change of status, i.e., removal, change of custody disposal, transfer;
5 Site of usage (pinpoint to discrete locations such as building numbers and room numbers);
6 Disposition including shipping when removed from inventory, method of destruction, when applicable;
7 Scientists 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 for pathogens in Experimental or Working Stocks. Experimental samples and repository stock aliquots used for working stocks or experimental purposes are tracked by laboratory records (laboratory notebooks, electronic systems). The location of material use must be included (building and room number). The accountability for Select Agents will be greater than for other biological agents. The disposition of the infectious material, including the means of disposal, must be addressed in Standard Operating Procedures (SOPS).

(2) Packaging and Shipping of Infectious Material. Packing and shipping of infectious material or biological agents will meet current national and international regulations and guidelines, which are referenced under Authorities, References, and Organizations.

Shipping and receiving of infectious material or biological agents will meet applicable guidelines and be tracked by each agency. Organisms and vectors may require APHIS permits for transport (9 CFR Part 122 for Animal Pathogens and 7 CFR 330.2 for Plant Pathogens). USDA laboratories utilize a small number of agents designated by the CDC as Select Agents. Shipping and tracking of these agents designated such by CDC 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 infectious material or biological agents are responsible for the accuracy of electronic databases and laboratory notebook records which are subject to review by their supervisor, laboratory director, or other authorized agency personnel. Physical review will be on an annual basis for biological agents and toxins and more frequent for Select Agents. Methods used during physical review or reconciliation may include counts of entire inventory or sampling of records and repository materials. The Center Director or Laboratory Director or equivalent is responsible for ensuring the physical reviews are accomplished. Random reviews shall be conducted on an annual basis by a designated official (not employed at that specific laboratory) to ensure compliance at the locations.

(4) Pathogen Security. All pathogens shall be stored in secure areas within the facility. Select Agents must be secured in locked containers within exclusion areas which are restricted buildings or rooms within the facility. Only personnel with the appropriate Public Trust designations will have access to freezer keys and codes. The biosafety level, risk group or biosafety category of the storage unit will be determined by 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. Bar coding may be used when practical.

(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. Procedures should be spelled out in Location Biosafety Manual.

(7) Internal Transfer. A pathogen can be transferred to another scientist 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.

(8) Chemical & Radiological Assets. Regulatory requirements necessitate keeping track of the hazardous materials found within USDA facilities or equivalent. The department Chemical Inventory Program (CIP) tracks and reports storage and use of hazardous materials to meet federal, state, and local regulatory requirements. The inventory assists emergency responders, provides USDA employees with specific hazard and storage information, aids in sharing of chemicals, and reminds users to dispose of sensitive chemicals before they become unsafe. The implementation of a CIP can also minimize opportunities for intentional removal of any hazardous materials from the facility.

The department's guidance can be found in the USDA Safety and Health Manual, Chapter 3, Specialized Programs. Section 1, Radiation Safety Programs, outlines program requirements for using radioactive materials and equipment that produces ionizing radiation. Section 2, Hazard Communication, Laboratory Chemical Hygiene and Biological Safety Program, sets policies and program elements to manage chemical and biological agents. Both programs require the annual identification of chemical, and biological health hazards associated with the respective USDA Agency mission operations.

All radiological assets will be kept in compliance with 10 CFR Part 20, "Standard Protection Against Radiation." Part 20 includes Agency requirements for dose limits for radiation workers and members of the public, monitoring (inventorying) and labeling of radioactive materials, posting radiation areas, reporting the theft or loss of radioactive material, penalties for not complying with Nuclear Regulatory Commission (NRC) regulations, and tables of individual radionuclide exposure limits. Subpart I---Storage and Control of Licensed Materials, Section 20.1801 outlines security procedures for stored materials, and Section 20.1802 mandates controls for materials not in storage.

(9) Property. Assets that pose a risk of physic .I threat include certain property with value in excess of $5,000 and other sensitive items. Inventory of property greater than $5,000 in value is regulated by AGPMR 104.50.1. Sensitive items as identified by each Agency, shall be inventoried according to AGPMR 104.50.1 and Agency policy.

9. PHYSICAL SECURITY

It is the policy of USDA to ensure appropriate levels of protection against unauthorized access, theft, diversion, or loss of assets, loss or theft of information related to these assets, 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.

The physical security assessment shall be designed according to risk management principles, which will evaluate targets, adversary capabilities, consequences, and vulnerabilities. Risk management principles acknowledge that while risk generally cannot be eliminated; enhancing protection from known or potential threats can reduce it.

Qualified individuals who have expertise in physical security shall develop this assessment. The assessment shall be reviewed regularly, but at least once every 5 years. The development of this physical security assessment is to reduce and mitigate the risk to the Department's mission and critical assets utilizing the following procedures:

a. Development of a Threat Assessment. This will be utilized to evaluate the likelihood of an attack against a given asset. It will identify and evaluate each threat on the Basis of various factors, including capability, intention, and impact of an attack. In characterizing the threat, USDA agencies or equivalent will examine the historical record of security and safety breaches and obtain location-specific threat information from governmental organizations and other sources.

b. Development of a Criticality Assessment. This will be utilized to systematically identify and evaluate important assets and infrastructure in terms of various factors, such as when the asset is at its most critical state and the mission and significance of a target. The assessment provides information to prioritize assets and allocate resources. These assessments consider factors such as the importance of the asset to accomplish the mission, the ability to reconstitute this capability, and the potential cost to repair or replace the asset.

c. Performance of a Gap Analysis. To determine the appropriate security countermeasures needed to protect assets and eliminate/mitigate the risk/threat, a gap analysis must be performed. The gap analysis will determine the difference between existing security countermeasures and the risk that was identified through the assessments.

d. Development of Vulnerability Assessment. This will be utilized to identify weaknesses in the protection of a given asset that may be exploited by a criminal or environmental threat and may suggest options to eliminate or mitigate those weaknesses.

e. Development of a Menu List for Suggested Security Countermeasures. This list will be recommended utilizing the concentric rings of security (perimeter security countermeasures) starting from the asset and working out toward the perimeter.

f. Site Assessment. The physical security system shall he 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.

g. 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.

h. 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.

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 the identified assets. 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.

i. 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 or equivalent. 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.

j. 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 security 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.

k. 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. This is sometimes referred to as a high containment area. Access to an exclusion area shall require a unique security 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.

l. 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 is 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.

m. Intrusion Detection and Assessment Systems. Intrusion detection systems appropriate for the risk 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, closed circuit television, alarm monitoring centers, or any combination of the above. 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 critical assets.

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 or equivalent possessing critical information 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 with a description of actions taken.

Alarm monitoring systems shall be self-checking and shall annunciate 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, be alarmed, 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 annunciation, and adequate lighting.

n. 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 annunciators, 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 3 years.

o. Auxiliary Power Sources. Auxiliary power shall have the availability and shall be capable of maintaining full operation of the intrusion detection and assessment system for 8 hours or for such a 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.

p. 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 equivalent 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 annunciators, protective farce 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 3 years.

q. 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. The most significant elements are those that provide protection for Select Agents, information related to physical security, and aircraft security.

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

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

t. 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.

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

v. Prohibited Articles. The following articles are prohibited from security areas, unless approved by the cognizant USDA local authority for physical security systems: any dangerous weapon, explosive, or other dangerous instrument or material capable of producing substantial injury or damage to persons or property. Sites shall, at a minimum, employ administrative procedures to prohibit these articles.

w. Visitor Logs. Visitor logs are required for limited areas and exclusion areas and shall be retained for 1 year. Information on the visitor logs, should include but not be limited to, visitor's name, agency, office telephone number, office to be visited with point of contact, time/date in and out, and purpose of visit.

10. CYBERSECURITY

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

(1) To ensure that the required and appropriate level of confidential specific information related to assets, is preserved by the system that is used to acquire, store, manipulate, manage, move, control, display, switch, interchange, receive, or transmit that information;
(2) To protect the physical, technical, and administrative controls and risk management processes that sec-re USDA information and information related to assets;
(3) To require that each USDA 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) To 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. The following are the general policies:

(1) Cyber Resource Protection. Each USDA organization or equivalent shall ensure that all USDA information resources, including USDA information related to Select Agents under its purview, are protected in a manner that is consistent with its threats and missions at all times.

(a) Risk Management. Each USDA organization or equivalent shall use a risk-based approach to identify information resources and specifically those that are related to Select Agents. 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.

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

(3) Security Program Plan. Each USDA organization or equivalent shall document its cybersecurity program in an Information System Security Plan (ISSP) following NIST Special Publication 800-18. The ISSP shall be approved by the organization's local director, field office, and the Office of the Chief Information Officer.

(OCIO)-Cybersecurity. USDA organizations may revise their ISSPs as required by new operational considerations, risks, vulnerabilities, etc. Each USDA organization shall submit the revised ISSP to its local director, field office, and to OCIO--Cybersecurity for approval.

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

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

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

Finally, the Headquarters Cybersecurity Office 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.

(5) Corrective Action Plans. Each USDA organization or equivalent 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. Each USDA organization shall submit their corrective action plans to OCIO Cyber Security and provide quarterly updates on progress.

(6) User Authentication. Each USDA organization or equivalent 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.

(7) Access Protection. Access to each USDA organization'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.

(8) Auditing. Each USDA organization or equivalent 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.

(9) Continuity of Service. Each USDA organization or equivalent 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 system and enclaves that require such mechanisms and procedures and shall detail the procedures and mechanisms employed.

(10) Security Monitoring and Reporting. Each USDA organization or equivalent shall report security incidents to the OCIO--Cybersecurity. In addition, each USDA organization shall provide 24-hours-a-day, 7-days-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.

(11) Training. Personnel from USDA organizations 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.

(12) Malicious Code. Each USDA organization or equivalent 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.

(13) System Administrator. Each USDA organization or equivalent shall have a system administrator, who is responsible for developing, updating, and implementing the ESP; 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 electronic connections from USDA systems to non-USDA or external systems, 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 by software on the email server. Each email client system shall have viral scanner software installed which scans the system on a regular schedule determine by unit policy.

(3) Password Policy. Passwords cannot be the same as the login name. They shall be six (6) characters or more. If the system is in an open or public area, the system shall also be protected by a boot-up password. Password shall not be kept anywhere in the open or in a fashion where unauthorized individuals can detect them. Passwords for network accounts shall be set to expire by administrative software at a period determined by the unit according to security needs, research flexibility, and physical accessibility to the network. 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 physical facility and security system are not openly available, and information related to personnel and those who work with Select Agents is kept to an absolute minimum.

(5) Internet Network. The internal systems and servers shall be on an isolated (internal) network that is strongly 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 Detection 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. HUMAN RELIABILITY

a. Purpose.

This section sets forth policy on human reliability requirements for USDA and non-USDA personnel who work in USDA laboratories including collaborators, cooperators, University personnel and contractors.

(1) Position Risk Designation. Following Office of Personnel Management (OPM) public trust designation model, agencies are responsible for designating each position High, Moderate, or Low Risk based upon the documented duties and responsibilities of the position.

(2) Background Investigations. Following Office of Procurement Policy and Management instructions, the following investigations will be conducted to determine the personnel suitability.

(a) Low Risk - National Agency Check With Inquiries (NACI)
(b) Moderate Risk – ANACI to a Limited Background Investigation (LBI)
(c) High Risk - Background Investigation (BI)

(3) Vacancy Announcement. Recruitment announcements will notify all candidates for permanent and non-permanent positions designated Moderate or High Risk that the appointment is subject to a background investigation.

(4) Pre-employment. A pre-employment Special Agency Check (SAC) must be completed for the selectees of Moderate and High Risk positions prior to appointment. Appointees to low risk positions must have the NACI completed after entering on duty.

12. RESPONSE PLANS

a. Purpose. This section sets policy for responses to specific types of incident in order to protect personnel and secure pathogen chemical, and radiological holdings.

b. Biosecurity Plan. The biosecurity plan will 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

The plan will address the following issues:

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

The determination of a biosecurity incident is by the 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 R C will notify the Federal Protective Service, local police, and the USDA Office of Inspector General (OIG).

c. Chemical & Radiology Security Plan. The plan will include responses to the following types of incidents:
(1) Containment/vessel/container breach
(2) Containment/storage area/cabinet security breach
(3) Chemical/Radiological agent inventory violation
(4) Workplace violence incident
(5) Cybersecurity breach
(6) Environment Releases

This plan will address the following issues:

(1) Personnel safety and health
(2) Storage/handling/treating/shipping materials and agents
(3) Proper labeling/signage
(4) Inventory Control
(5) Cleanup Procedures
(6) Notification of manager and responders
(7) Education/training requirements
(8) Environmental Releases

Anyone involved in any chemical/radiological related incidents, regardless of the severity, will immediately notify their supervisor or designee. The notification will be by phone or in person. Once an investigation of the situation is completed, the supervisor, will report the findings through the normal management communication structure, and to the IRC if the incumbent is not part of the structure. The appropriate Federal/State/local regulatory official must be contacted if there is an environmental release, a hospitalization of one or more employees, a property damage incident, a fire, a major accident/injury/ illness, a motor vehicle accident or a death.

d. Occupant Emergency Plans. In accordance with Departmental Regulation 1650-002, an Occupant Emergency Program shall be established for all USDA facilities to safeguard lives and property during emergencies such as fire, explosions, bomb threats, and natural disasters.

All employees must be given a copy of the Occupant Emergency Plan and they shall fully cooperate with the Designated Official in the implementation of an Occupant Emergency Plan and the staffing of an Occupant Emergency organization. The Designated Official is the official in charge, or his or her designee, at that location. At General Services Administration (GSA) leased sites, the Designated Official is the official in charge in the lead agency at that facility. The Designated Official is to be named in the Occupant Emergency Plan.

When there is immediate danger to persons or property such as fire, explosion, or the discovery of an explosive device, occupants shall be evacuated or relocated in accordance with the Occupant Emergency Plan. This shall be accomplished by sounding the fire alarm system or by other appropriate means.

When there is advance notice of an emergency, the Designated Official shall initiate appropriate action in accordance with the established Occupant Emergency Plan.

After normal duty hours, the senior official present shall represent the Designated Official and shall initiate action to cope with emergencies in accordance with the established Occupant Emergency Plan.