

# Biosecurity Training

An Introduction to Biosecurity for  
VHA Research Laboratory Staff

# Overview of Presentation

- Part I: Basic Concepts of Biosecurity
- Part II: Components of a Biosecurity Program
- Part III: Laboratories Requiring Increased Security
- Part IV: Employee Responsibilities for VHA Biosecurity



Part I

Basic Concepts of  
Biosecurity

# What Is Biosecurity?

- Biosecurity is preventing unauthorized
  - Entry into laboratories
  - Removal or misuse of microbiological agents or hazardous agents
  - Removal or misuse of sensitive materials
    - Data, equipment, computers
  - Disruption of laboratories
    - Terrorist incident, natural disaster, destructive events

# Why Is Training Necessary?

- To increase awareness of security concerns
- To increase employee understanding of required security measures that are designed to protect staff and VA resources
- To prevent materials found in research laboratories from being used for unintended purposes such as bioterrorism

# Biosecurity vs. Biosafety

- Biosecurity: Protection of materials, data, equipment & sites against theft or misuse
- Biosafety: Administrative polices, work practices, safety equipment, lab design that protects the worker and the environment

# Definitions

- Bioterrorism: Use of biologic, pathogenic agents for terrorist activities
- Risk: Measure of potential loss based on
  - Probability of occurrence of an event
  - Effectiveness of protection
  - Consequence of loss
- Threat: Capability and intention of an adversary or others to undertake malicious actions

## Definitions (2)

- **Vulnerability:** A security weakness or deficiency; a susceptibility for malicious actions to occur; the capacity to suffer harm

# Definitions (3)

- Vulnerability assessment: A systematic evaluation process that identifies:
  - Potential threats to security
  - The impact of an event
  - How current security measures would prevent an incident
  - Potential solutions/protections
  - Resources required to implement solutions/protections

# Definitions (4)

- Select agents & toxins: Specifically regulated pathogens and toxins that are defined by HHS and USDA regulations that require specific security
  - [www.cdc.gov/od/sap](http://www.cdc.gov/od/sap)
  - [www.aphis.usda.gov](http://www.aphis.usda.gov)
- Exempt quantities of toxins: Permissible amounts of toxins that a PI is allowed to store or use that are not subject to select agents regulations.
  - Listed on the Centers for Disease Control & Prevention (CDC) website

# Definitions (5)

- Hazardous Agents: VHA has defined select agents & toxins plus other chemicals and radiation sources as hazardous and having the potential to be used as tools for bioterrorist.
  - See Handbook 1200.6, Appendix A

# Related Policies and Regulations

- VHA Handbook 1200.6 Control of Hazardous Agents in VA Research Laboratories
- 38 CFR 72 & 73, 9 CFR 121, 7 CFR 331 regarding select agents and toxins
- 10 CFR 19 & 30 regarding Nuclear Regulatory Commission and use of radiation
- VA Handbook and Directive 0710 (Personnel Suitability) & 0730 (Security)
- Other policies listed in Handbook 1200.6 Paragraph 10



Part II  
Components of a  
Biosecurity Program

# Components of a Biosecurity Program

- Institutional Policies
- Security Plan
- Training
- Evaluation

# Institutional Policies

- Facility specific policies based on
  - VA and VHA central office policies
  - Other Federal regulations including
    - Occupational Safety & Health Adm. (OSHA)
    - CDC
    - US Dept. of Agriculture (USDA)
    - Dept. of Transportation (DOT)

# Institutional Policies (2)

- Facility policies serve as the basis for SOPs
  - Policies tell us what must be done
  - Procedures tell us how to do it
- Specific laboratories may also develop policies and procedures that are specific to the agents present and the research that is conducted in the laboratory

# Components of a Biosecurity Plan

- Physical security
- Personnel security & access control
- Information security
- Material control & accountability
- Vulnerability assessment
- Emergency response plans

# Physical Security

- Objective: To deter or detect unauthorized activities such as theft, destruction or misuse of property, equipment, materials, data etc.
- Deter by use of physical barriers
  - Building: locks, limited access points, construction (windows, doors, etc.), lighting, unobstructed views of entrances, fences
  - Interior: self-closing doors, locks to individual rooms, cabinets, refrigerators, etc.
- Detect: Intrusion alarms, security patrols, video monitors etc.

# Personnel Security

- Justification for hiring new personnel
- Formal application and background checks for compensated and uncompensated personnel
  - Qualifications and experience
  - Background check dependent on the sensitivity level of the position & determined by Human Resource Management
- Ensuring:
  - References have been contacted
  - Qualifications have been verified
  - Background checks completed
  - Training in safety & security completed

# Personnel Security (2)

- Maintaining a comprehensive list of all persons who have been granted access to:
  - “Regular” labs
  - Labs containing hazardous agents
  - Labs containing select agents & toxins
  - BSL-3 labs
- Maintaining records of keycard/key assignments

# Access Control

- Access control is 24 hours/day, 7 days a week
- Photo identification badges issued and displayed at all times
- Specific levels of access and authorization are defined depending on risk assessment for laboratories such as:
  - Labs without hazardous agents
  - Labs with select agents or toxins
  - Labs with radiation sources
  - BSL-3 labs
- Keycards or other control mechanisms coded to allow access to areas the person is authorized to enter
- Procedures for immediately deactivating keycards when lost or stolen & when employees leave

# Access Control (2)

- Marking all non-public areas as restricted
  - All laboratories are restricted areas
- Procedures for challenging unauthorized persons who enter or attempt to enter restricted areas
- Procedures must be in place for reporting and removing unauthorized persons
- Procedures for escorting persons who have not been approved to enter restricted areas
  - Delivery persons, repair technicians, maintenance, housekeeping and visitors
  - Access should be limited to when approved laboratory staff are present

# Access Control (3)

- Develop mechanisms to track who enters research areas
- For Biosafety Level-3 (BSL-3) laboratories: a mechanism to track when persons both enter and exit the laboratory
- Ensuring physical security measures are not compromised
  - Doors are not propped open
  - Cabinets/refrigerators/cold storage rooms are locked when not in use or under direct observation
  - Intrusion alarms, video cameras are not disabled

# Information Security

- Pertains to information regardless of storage mechanism (paper, electronic, audio or visual) and to IT systems
- Sensitive information & data are stored securely
  - Paper, tapes, videos, etc., are locked up when not in use
  - Computers and applicable databases or files are protected by passwords or other mechanisms
- Passwords are not shared with unauthorized individuals
- Information and/or data are only shared with authorized individuals

# Information Security (2)

- Procedures for maintaining the integrity of and access to specific kinds of information
- Categorizing the sensitivity level of information
  - Based on outcome of misuse
  - Compromising defense
  - Scientific integrity

# Information Security (3)

- Preventing individuals from obtaining information by
  - Physically stealing it
  - Access to offsite storage
  - Finding discarded material in trash or elsewhere
  - Accidental release
  - Breach of computer/network security
  - Overhearing verbal discussions occurring in inappropriate areas

# Material Control & Accountability

- Current inventory of all hazardous agents is required
- Hazardous agent inventories must be conducted semi-annually and reported to the Safety Officer
- Inventory updated when new chemicals or agents are received or when inventory changes
- New agents acquired only when there is an approved protocol

# Material Control & Accountability (2)

- Hazardous agents not currently in use & for which there are no immediate plans for use must be transferred to another laboratory, destroyed or disposed of according to VHA and local policy
- Hazardous agents are not “shared” with other investigators or laboratories without the appropriate permissions.
- Hazardous agents must be stored in secure areas as required by VHA and local policy

# Vulnerability Assessment

- A systematic evaluation that identifies:
  - Potential threats
  - The impact of an event if it occurs
  - How current security measures would prevent an incident
  - Potential solutions/protections
  - Resources required to implement solutions/protections
- Applies qualitative and quantitative techniques to analyze vulnerabilities & threats and to develop procedures to mitigate these vulnerabilities and risks

# Risk Assessment

- Identifies
  - What must be protected
  - What happens if there is loss or misuse
  - What is the highest priority for protection
  - What will be compromised and why
  - What is the probability that this will occur

# Emergency Preparedness

- Emergency plans must be in place and all employees must be familiar with the plans
- Plans must include means for emergency responders to gain access to the area
- Laboratory emergency plans must be integrated with the facility-wide plan
- The facility-wide plan must be coordinated with emergency responders from the community



## Part III

# Laboratories Requiring Increased Security

# Laboratories Requiring Increased Security

- BSL-3 laboratories
- Laboratories containing hazardous agents
  - As listed in Appendix A of VHA Handbook 1200.6
    - Chemicals
    - Radiation sources
    - Exempt quantities of toxins per the “Select Agent” rules
- Areas containing select agents &/or toxins

# BSL-3 Research Laboratories

- Specific security measures
  - Location is away from public areas
  - Video monitoring of access door
  - Access control that documents entrance and departure of individuals
  - Specific security standards for doors and windows
- Specific approvals required to work in BSL-3
- Specific construction requirements to ensure safety and security
- New BSL-3 laboratories or major renovations of existing BSL-3 laboratories require VA Central Office (CO) approval

# Laboratories Containing Hazardous Agents

- Requires storage areas including containers, cabinets, refrigerators to be secured when not in direct view
- Laboratory must be locked when laboratory workers are not present
- Special procedures for reporting loss, theft or release of agents

# Laboratories Containing Hazardous Agents (2)

- Specific inventory requirements
- Radiation sources
  - Under control of VHA's National Health Physics Program ([www.nhpp.med.va.gov/](http://www.nhpp.med.va.gov/))
- Exempt quantities of toxins
  - Requirements are the same as for other hazardous agents
  - List of exempt quantities found at [www.cdc.gov/od/sap](http://www.cdc.gov/od/sap)

# Select Agents & Toxins

- Regulated by HHS (CDC) and Department of Agriculture (APHIS)
  - CDC: Centers for Disease Control & Prevention
  - APHIS: Animal & Plant Health Inspection Service
- Specific regulations published that address the possession, use and transfer
- Laboratories must be registered with CDC or APHIS prior to obtaining select agents or toxins
- Personnel must undergo a specific Security Risk Assessment conducted by FBI prior to working in laboratory

# Select Agents & Toxins (2)

- Security requirements more stringent
- VHA policies are found in Handbook 1200.6
- Regulations found in:
  - 42 CFR Part 72 and 73
  - 7 CFR Part 331
  - 9 CFR Part 121
- CDC or APHIS websites contain further information including list of select agents and toxins
  - [www.cdc.gov/od/sap](http://www.cdc.gov/od/sap)
  - [www.aphis.usda.gov](http://www.aphis.usda.gov)



# Part IV

## Employee Responsibilities for VHA Biosecurity

# Employee Responsibilities

- Be familiar with
  - Your facility's security plan and emergency response plan
  - Applicable biosecurity regulations and policies (national and local)
- Complete the required initial and annual training
- Follow all security procedures
- Report
  - Any unusual activities or activities not allowed by policy or procedures
  - All breaches of security such as doors propped open, missing chemicals or biologic agents
  - All suspicious packages
- Wear your ID badge at all times

# Employee responsibilities (2)

- Access control:
  - Never allow someone to enter the facility behind you without their using their own security access device (key, card, code, etc.)
  - Never share your keys, keycards or passwords
  - Challenge any person without a photo ID or who does not belong in the laboratory area

# Employee Responsibilities (3)

- Access control continued:
  - Do not disable security systems
  - Keep all storage areas, refrigerators and cabinets for hazardous agents and select agents or toxins secured by locks or other means when not in direct sight
  - Do not allow persons in the laboratory area who have not been approved to access the area

# Employee Responsibilities (4)

- Maintain computer and data security
- Participate in the annual vulnerability assessment when requested
- Conduct inventory of all hazardous agents and select agents as required
- Safeguard your keys, keycards, passwords and other security codes or cards

# Employee Responsibilities (5)

- Forward requests for unpublished data to the FOIA officer
  - If you believe the requested records contain information which, if disclosed, may possibly compromise national/homeland security, communicate this concern to the:
    - FOIA Officer
    - ACOS/R&D who may forward the request to the Chief, Police Service
- Report all breaches of security to your supervisor



A secure workplace is  
everyone's responsibility

# Biosecurity Training

## Certificate of Completion

I, \_\_\_\_\_ have read and understand  
the *VHA Introduction to Biosecurity for VHA Research  
Laboratory Staff Training*.

Date: \_\_\_\_\_

Signature: \_\_\_\_\_