



Components of Laboratory Biosecurity

**International Biological Threat Reduction Department
Sandia National Laboratories
October 15, 2006**

**Overview of the Principles of Laboratory Biosecurity
ABSA pre-conference course**

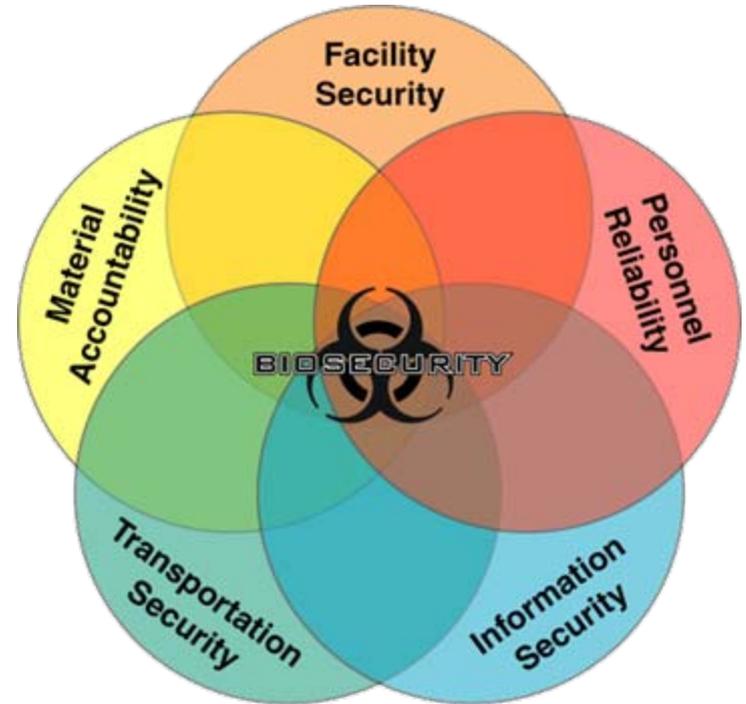
www.biosecurity.sandia.gov

SAND No. 2005-3288 C

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Biosecurity System

- **Biosecurity system components**
 - Physical security
 - Personnel security
 - Material handling and control measures
 - Transport security
 - Information security
 - Program management practices
- **Each component implemented based on results of risk assessment**
- **In general, biosecurity for**
 - Moderate risk focuses on the insider
 - High risk focuses on both the insider and the outsider



Elements of a Physical Security System

- Graded protection
- Access control
- Intrusion detection
- Response force



Physical Security: Concentric Layers of Security

- **Property Protection Areas**

- **Low risk assets**

- Grounds
- Public access offices
- Warehouses

- **Limited Areas**

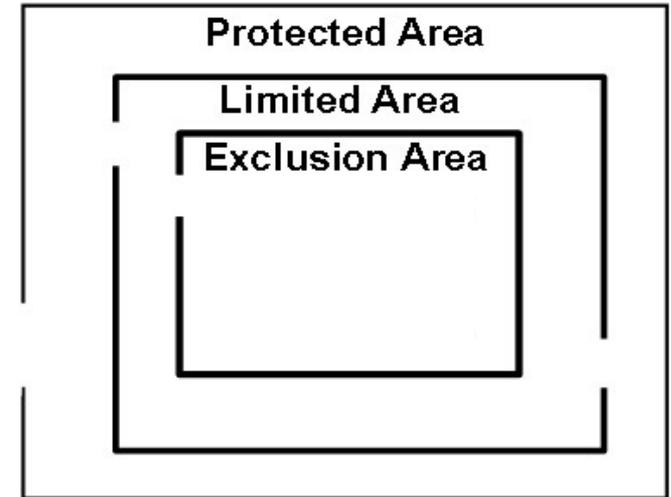
- **Moderate risk assets**

- Laboratories
- Sensitive or administration offices
- Hallways surrounding Exclusion Areas

- **Exclusion Areas**

- **High risk assets**

- High containment laboratories
- Computer network hubs



Physical Security: Property Protection Control

- **Fences**
 - **Mark the boundaries of your property**
 - **Announce your intention to protect the property**
 - **Elicit strong statement of intent from intruder**
 - **Terrain features can also serve this purpose**



Physical Security:

Limited and Exclusion Area Access Control

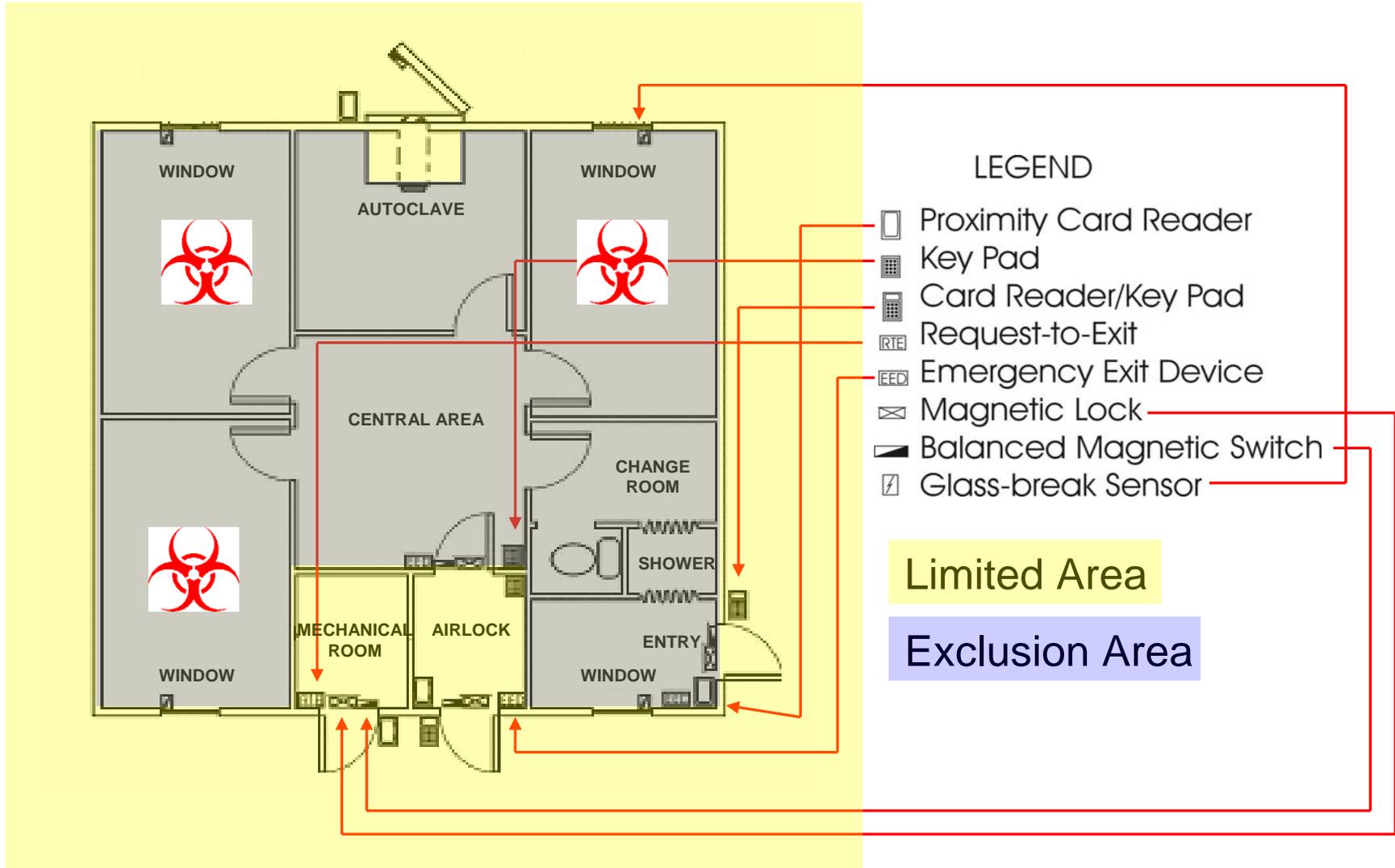
- Access control ensures that only authorized individuals are allowed into certain areas
 - Increasingly strict controls as you move toward higher risk assets
- Limited Areas
 - Unique item
 - Controlled possession
 - Electronic or physical key
- Exclusion Areas
 - Unique item
 - Unique knowledge
 - Controlled possession
 - Electronic key card and keypad or biometric deviceor
 - Controlled key and second individual to verify identity



Physical Security: Intrusion Detection and Response

- **Intrusion Detection**
 - Guards
 - Electronic sensors
- **Alarm Assessment**
 - Validation of violation before response
 - Can be direct (guards) or remote (video)
- **Response**
 - **On-Site Guard Force**
 - Supports electronic systems
 - Patrols or guards perimeter and buildings
 - Summons and directs local law enforcement
 - **Local law enforcement (police) support**
 - Reinforces or substitutes for on-site guard force
 - Memorandum of understanding

Physical Security: Example Laboratory Building



Physical Security: Procedures

- **Impose consequences for security violations**
- **Log personnel (including visitor) access to restricted areas**
- **Establish controls on animal and supply handling**
- **Enforce escort policies**
 - **Visitors**
 - **Maintenance and cleaning personnel**
 - **Delivery personnel**
- **Train personnel on what to do about:**
 - **Unrecognized persons**
 - **Unusual or suspicious activity**

Physical Security:

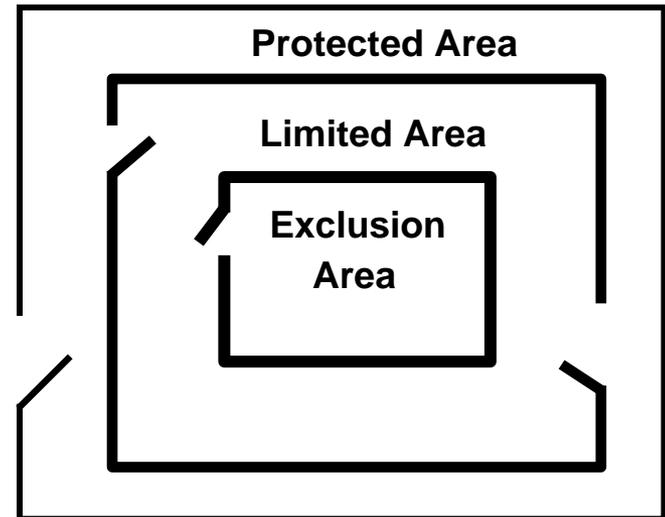
Performance Testing and Maintenance

- **Create security performance test plan and procedures**
- **Schedule periodic testing of hardware and policy implementation**
- **Schedule periodic testing of response force procedures**
- **Document test results**
- **Take corrective action**
 - **Schedule maintenance and repair of hardware**
 - **Corrective training and policy adjustments as appropriate for policy implementation failures**
 - **Corrective training and exercises for guard force**

Physical Security

- **Moderate**
 - Store and use pathogens (and infected animals) within Limited Areas
 - Restrict access using controlled keys and secured windows
 - Control visitors

- **High**
 - Store and use pathogens (and infected animals) within Exclusion Areas
 - Electronic Intrusion Detection System and/or guards
 - Controlled and authenticated key
 - Something you *have* (key) plus something you *know* (PIN)
 - Restrict and control visitors
 - Maintain records of entry/exit



Elements of a Personnel Security Program

- Personnel Screening
- Badges
- Visitor Control
- Training



Personnel Security: Screening

- **Conduct screening for authorized individuals**
 - **Degree of scrutiny commensurate with level of risk associated with the position**
 - **Need for unescorted access to restricted areas**
 - **Types of assets held in the restricted areas**
 - **Level of authority in association with high risk materials**

- **Mechanisms**
 - **Verify credentials**
 - **Check references**
 - **Criminal history**
 - **In-depth background investigation**



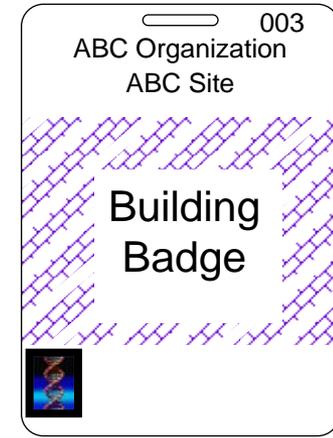
Personnel Security: Visitor Controls

- **Types**
 - **Personal Visitors**
 - Family members
 - **Casual Visitors**
 - Tours, seminars
 - Equipment repair technicians
 - **Working Visitors**
 - Visiting researchers
 - Facility maintenance personnel

- **Controls**
 - All visitors should have a host at the facility
 - Visitors should be escorted in restricted areas

Personnel Security: Badges

- Badges should be issued to those individuals authorized to be in restricted areas



- Badge return
 - Upon employee termination
 - Daily or at the conclusion of a limited term for visitors
- Report lost or stolen badges

Personnel Security: In-Processing and Out-Processing

- **In-Processing**
 - Complete all required forms, safety training, security training and immunizations as applicable for work environment

- **Out-Processing**
 - Access changes or termination
 - Retrieve property
 - Deactivate computer and electronic access accounts



Personnel Security: Employee Assistance Program

- **Provide resources to address problems associated with a variety of personal issues**
 - **Marital issues**
 - **Family issues**
 - **Eldercare/childcare issues**
 - **Job conflict**
 - **Grief**
 - **Financial issues**
 - **Legal issues**
 - **Stress**

Personnel Security: Security Violations

- Security violations should be ranked according to the effects upon the organization

Organization ABC keeps large quantities of HMUR agents in Building 1, Room 123, Freezer A.



Personnel Security

- **Moderate**
 - **Background investigation**
 - Criminal history
 - Verifiable compliance with rules and regulations
 - **Drug test**

- **High**
 - **Moderate plus**
 - Personal and associate interviews
 - Credit history
 - Terrorist/extremist/criminal affiliation
 - Periodically reinvestigate



Material Control & Accountability: Objective

- **Ensure the complete and timely knowledge of:**
 - What materials exist
 - Where the materials are
 - Who is accountable for them

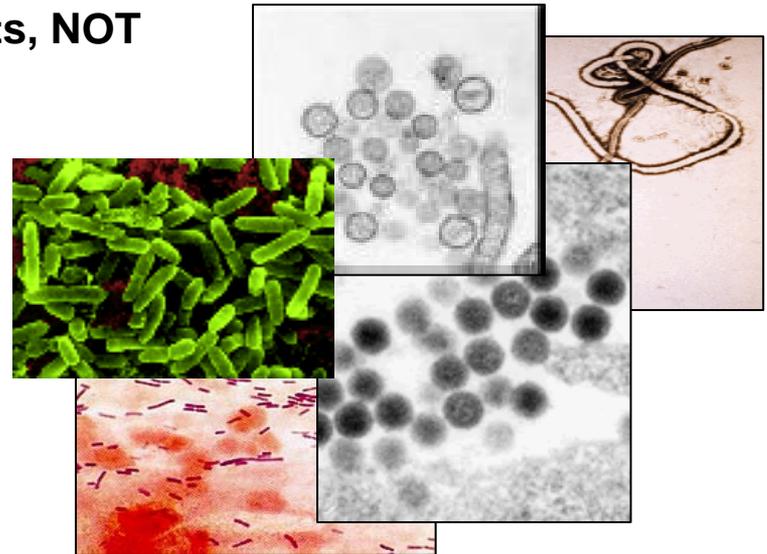
- **NOT: to detect whether something is missing**

Material Control & Accountability: Key Issues

- **What materials are subject to MC&A measures**
- **The operating procedures associated with the materials**
 - where they can be stored and used
 - how they are identified
 - how inventory is maintained
- **What records need to be kept for those materials and the timeliness requirements for those records**
- **What does accountability means**
- **Documentation and reporting requirements**

Material Control and Accountability

- Defining “material” is complicated
- Agent
 - Name and description
- Quantity
 - Based on containers or other units, NOT number of microbes

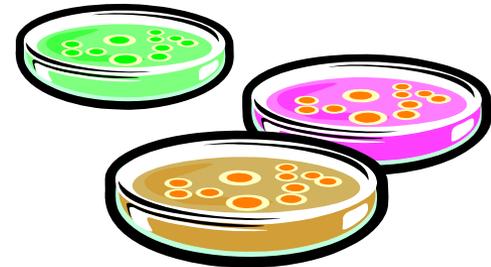


Material Control and Accountability

- **Agent**
 - What agents are high risk?
 - Viable? Whole organism or DNA?
- **Quantity**
 - Any amount can be significant
 - A threshold amount for toxins
- **Form**
 - Repository stocks, working samples, in host, contamination
- **Detail—what level is adequate for MC&A?**
 - Material as *items*
 - Each vial as a separate inventory record?
- **Capture—when does MC&A start & stop?**
 - Naturally occurring; clinical samples; disposition

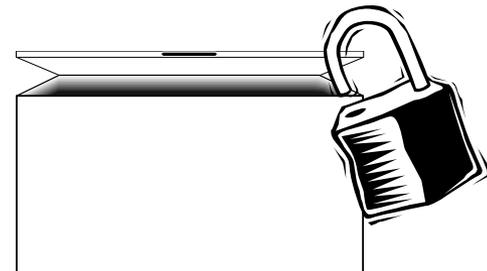
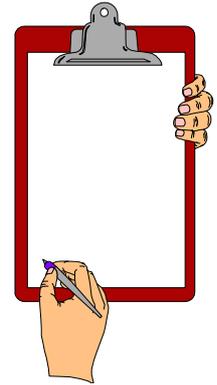
Material Control and Accountability

- **Attributes:** to characterize the material (“what”)
 - Agent / strain
 - Origin
 - Date
- **Description:** to identify a particular *item* of the material (“which”)
 - Container
 - Identification
 - Location



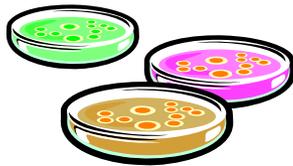
Material Control and Accountability

- **Control is either...**
 - Engineered / Physical
 - Administrative
- **Containment is part of material control**
 - Containment Lab / Freezer / Ampoule
- **Procedures are essential for material control**
 - For both normal and abnormal conditions



Material Control and Accountability

- All material should have an associated “accountable person”
 - The person best in a position to answer questions about the associated material
 - Not someone to blame!
 - Ensure that no material is “orphaned”



Material Control and Accountability

- **Procedures should ensure accountability**
 - **Experimental work: laboratory procedures**
 - **Inventory: know what you have**
 - **Reporting: document routine MC&A practices**
 - **Audit/ assessment: is this working?**
 - Ensures effective *implementation* of MC&A
 - **Training: personnel understand requirements**

Material Control & Accountability

Much of MC&A is likely already done for reasons other than biosecurity...

- **Biosafety**
- **Good research practice**
- **Business interest**

Material Control & Accountability

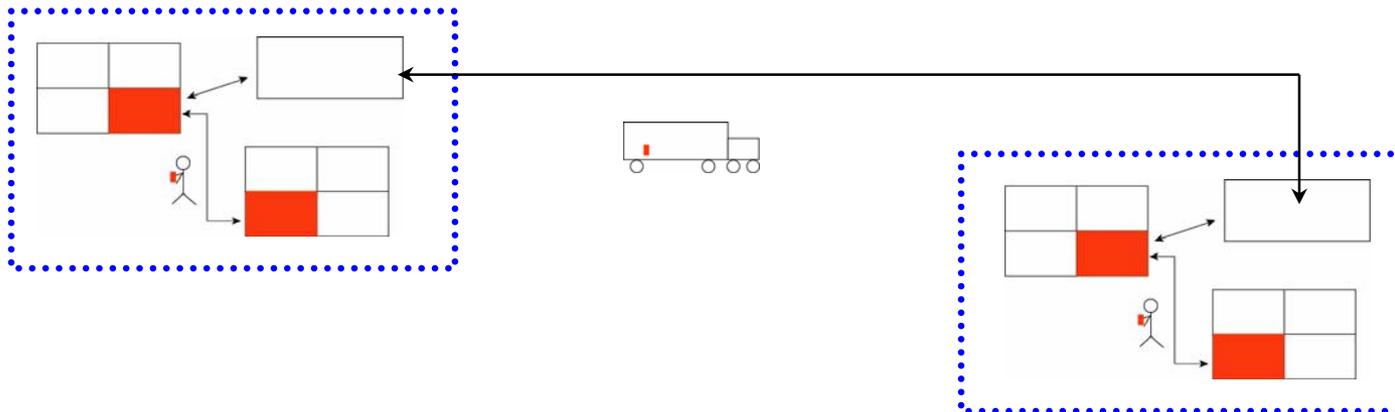
- **Moderate**
 - **Seed stocks cataloged and records stored securely**
 - Transfers in and out
 - Source
 - Strain
 - Form
 - Responsible individual
 - **Working stocks, including infected animal status, tracked through laboratory notebooks**

- **High**
 - **Moderate plus**
 - Increased control over working stocks



Infectious Substance Transport

- **Transport – movement of biological material outside of a restricted area**
 - **Research labs**
 - Sample transfers are necessary for study and to further research
 - **Public health labs and diagnostic labs**
 - Sample transfers are necessary for diagnosis and analysis
- **Transport can occur**
 - **Across international borders**
 - **Within a country**
 - **Within a facility**



Internal Transport

- **Movement of materials to and from restricted areas within a facility**
- **May involve personnel from**
 - Labs
 - Shipping areas
 - Receiving areas
 - Disposal areas (e.g. autoclave and incinerator rooms)
- **Move materials safely and securely**
 - SOPs
 - Leak-proof containers
 - Pre-approval?
 - Chain of custody?



External Transport

- **Movement of materials from one facility to another facility**
- **May involve commercial carriers**
- **Occur within a wide array of international and state regulations and standards**
- **Must be able to move frozen materials efficiently**
- **Need to be cost-effective**



Development of Regulations for Transport of Infectious Substances

UN Committee of Experts
on Transport of Dangerous Goods



Model Regulations on the Transport of Dangerous Goods



ADR
(road)

RID
(rail)

IMO
(sea)

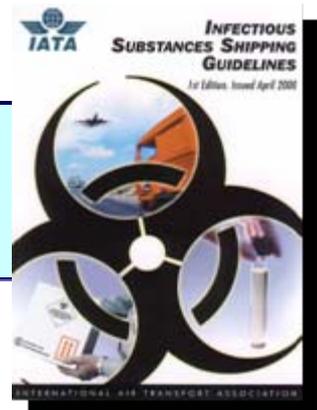
ICAO
(air)



IATA
(air)

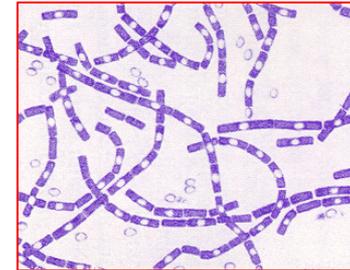


National Regulations

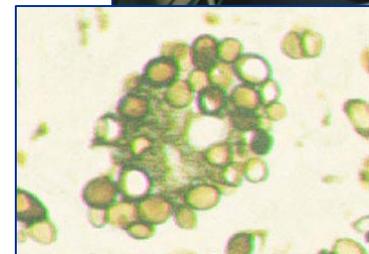
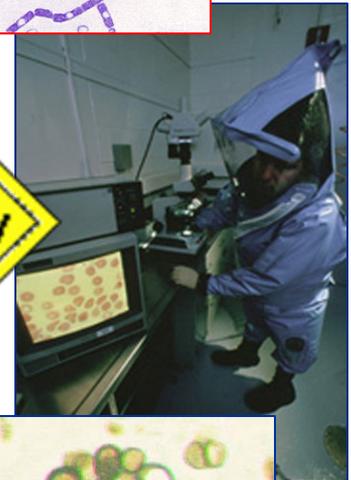


Hazardous Material Transportation Security

- Infectious substances (Class 6.2) and toxins (Class 6.1) are defined as Hazardous Material
- 49 Code of Federal Regulations (CFR) 172 (2003) – HM 232 – mandates security measures for the transport of some Hazardous Material
 - Select Agents regulated under 42 CFR 73 require Hazardous Material transport security measures
- Hazardous Material regulated security requirements include:
 - Training
 - Security awareness training
 - Specific training as appropriate
 - Written security plan
 - Based on assessment of transportation security risks
 - Address personnel security, unauthorized access, en route security



Bacillus anthracis



Coccidioides immitis

Transport Security: Chain of Custody (CoC)

- **Aims to protect sample by documenting**
 - All individuals who have control of sample
 - Secure receipt of material at appropriate location
- **Chain of custody documentation includes**
 - Description of material being moved
 - Contact information for a responsible person
 - Time/date signatures of every person who assumes control



Transport Security: Process

- **Responsible authority pre-approves all transport**
- **Transport should be documented in lab records**
- **Transport is controlled and documented in delivery records**
- **Timely shipping methods are used**
- **Chain of Custody is maintained**
- **Notification of successful receipt**

Transport Security: Facility Responsibilities

- **Personnel security**
 - For people who have access to dangerous pathogens and toxins or information during transfers

- **Establish chain of custody (CoC)**
 - Record all individuals who have contact with the dangerous pathogens and toxins

- **Provide physical security**
 - For packages that need temporary storage

- **Protect transport documentation**

- **Determine who is able to authorize, transport, and receive dangerous pathogens and toxins**

Carrier Security

- **Carriers should provide security by**
 - **Ensuring reliable and trustworthy people handle the package**
 - **Controlling access to transport facilities, docks, and vehicles**
 - **Tracking shipping progress**
 - **Providing ongoing security training for employees**



Transport Security

- **Moderate**
 - Internal transport personnel screened
 - Recipient screened for legitimacy
 - Safe receipt notification

- **High**
 - **Moderate plus**
 - Chain of custody
 - Physical controls on storage containers

Information Security

- **Protect information that is too sensitive for public distribution**
 - Label information as restricted
 - Limit distribution
 - Restrict methods of communication
 - Implement network and desktop security

- **Biosecurity-related sensitive information**
 - Security of dangerous pathogens and toxins
 - Risk assessments
 - Security system design
 - Access authorizations



Information Security: Identification, Control, and Marking

- **Identification**
 - **Designated sensitivity level**
 - **A review and approval process aids in the identification of sensitivities**
 - Critical prior to public release of information
- **Control**
 - **Individual responsible for control of sensitive information**
 - Physical security
 - Communication security
 - **In the US, in order to refuse public access upon request, information must be exempt from the Freedom of Information Act**
- **Marking**
 - **Sensitivity level designation**
 - Top and bottom of each page / cover sheet
 - **Marking and control methods should be well understood by those working with information**

Moderate

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

December 1, 1995

MEMORANDUM FOR: David Smith, Chief
Division 5

From: Susan Goode, Director

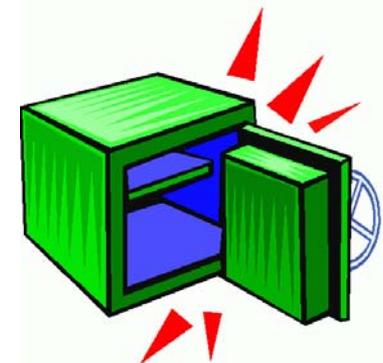
Subject: (U) Recommendations for
Resolving Funding Problems

1. (S) This is paragraph 1 and contains "Secret" information taken from paragraph 2 of the source document. Therefore, this portion will be marked with the designation "S" in parentheses.
2. (U) This is paragraph 2 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.
3. (U) This is paragraph 3 and also contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

Derived from: Memorandum dated 11/1/95
Subj: Funding Problems
Department of Good Works
Office of Administration
December 31, 2000

Declassify on:

Moderate

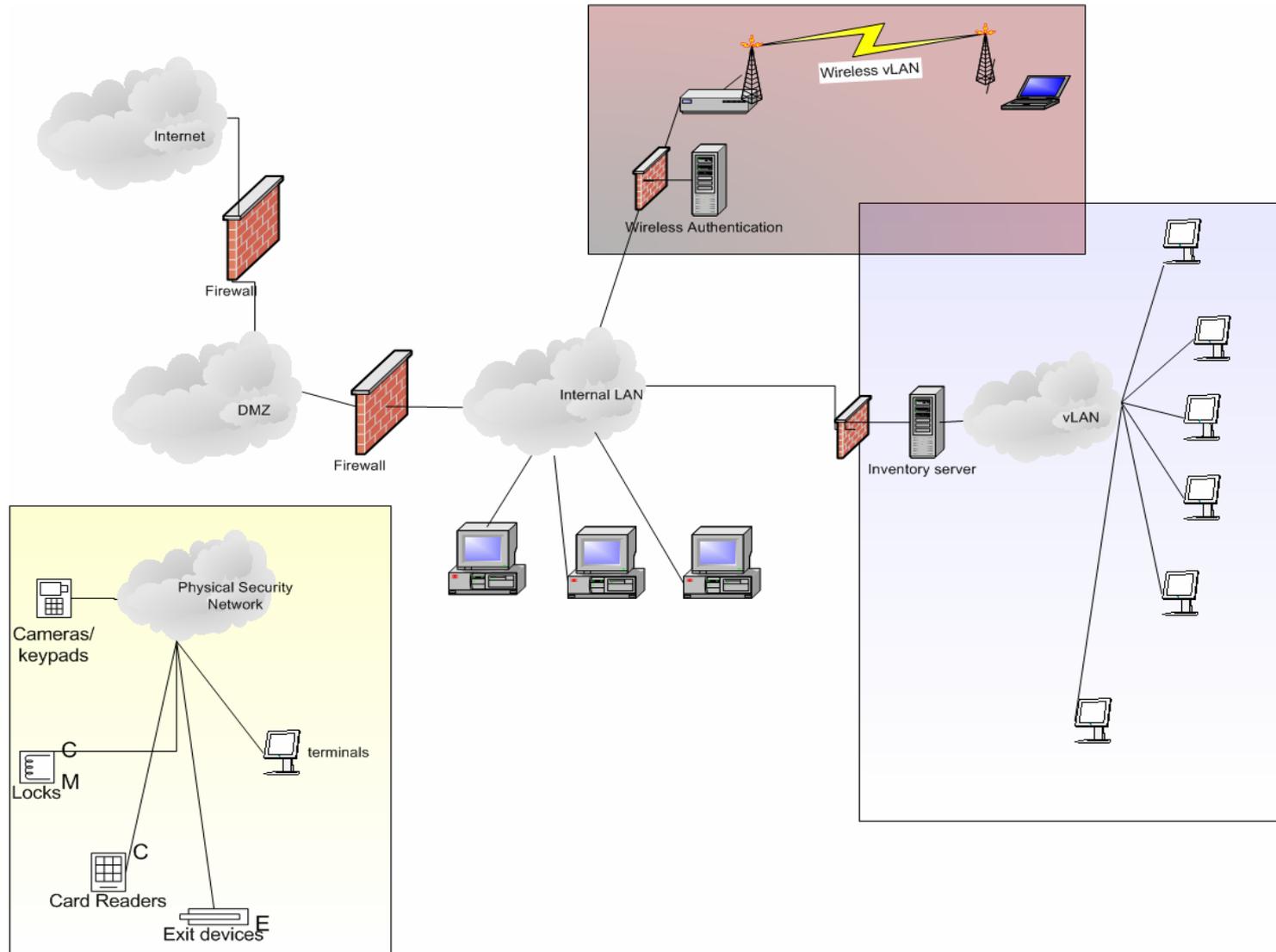


Information Security:

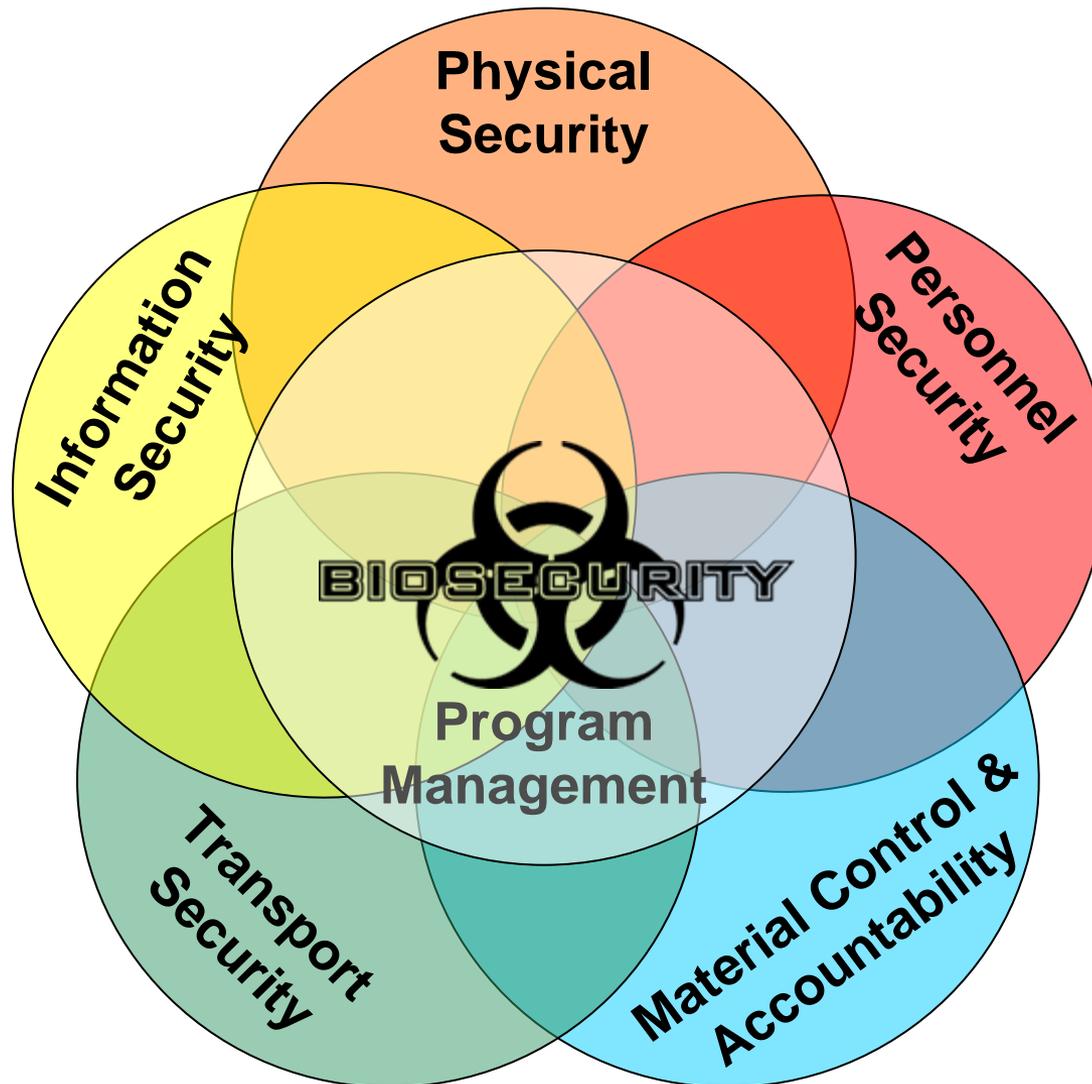
Communication and Network Security

- **Communication Security**
 - Mail, email, or fax security is required
 - Limited discussions in open areas
 - Information should only be reproduced when needed and each copy must be controlled as the original
- **Network Security**
 - Firewalls
 - User authentication
 - Virus protection
 - Layered network access
 - Desktop security
 - Remote and wireless access controls
 - Encryption
 - Authentication

Example Network Design



Components of Biosecurity



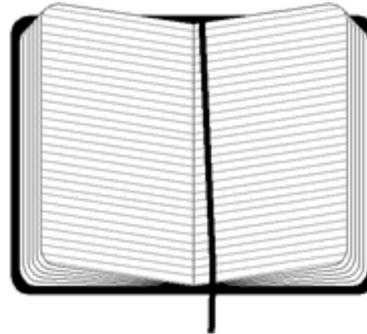
Program Management: Responsibilities

- **Identify the protection objectives of the biosecurity system**
 - Distinguish between “unacceptable” and “acceptable” risks
 - Ensure that the cost to protect an agent is proportional to the risk of malicious use
- **Design the system**
 - Physical security hardware and configuration
 - Biosecurity policies and procedures
- **Write security incident and emergency response plans**
- **Conduct regular training and internal reviews**
- **Allocate resources**



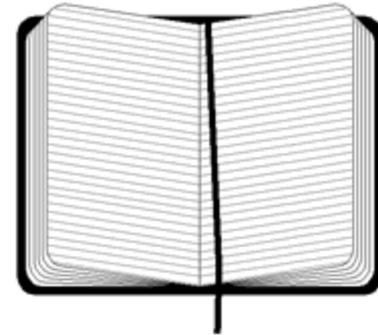
Program Management: Biosecurity Training

- **Annual training tailored to different audiences**
 - **New and current employees**
 - **Managers**
 - **Emergency responders**



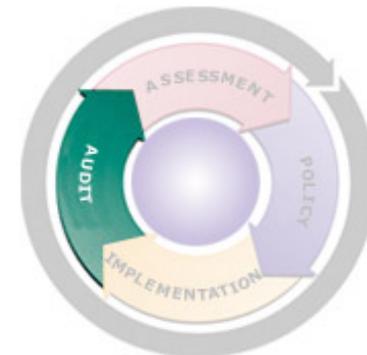
Program Management: Training

- **Annual training tailored to different audiences**
 - New and current employees
 - Managers
 - Emergency responders
 - Guard force
- **Topics**
 - Applicable manuals, SOPs
 - Statutory requirements
 - Operations and procedures
 - Access control procedures
 - Physical security, personnel security, information security
 - Equipment
 - Incident response
 - Incident reporting
 - Disciplinary actions
 - Media and public requests



Program Management: Self Assessments and Management Reviews

- **Internal and third party**
 - **Self assessments ensure compliance with standards and evaluate effectiveness of the biosecurity and biosafety programs**
 - Regular self-inspections by designated employees (daily/weekly)
 - Supervisor inspections to reinforce employee inspections (weekly/monthly)
 - **Management reviews institute corrective and preventive actions, and allocate required resources**
 - Inspections by a site team of employees, supervisors, and site management
 - **Periodic third party reviews provide an independent assessment**



Program Management: Responding to Inspection / Audit Findings

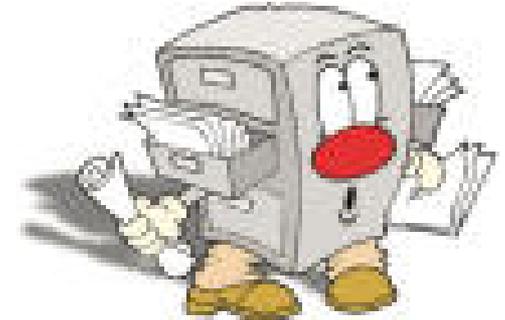
- **Ensure corrective actions are taken to eliminate identified deficiencies**
- **Assign responsibilities**
 - **Ensure that a responsible individual is assigned for the identified deficiency or action item**
- **Implementation schedule**
 - **Create an implementation schedule with set milestones and follow through to completion**
 - **Identify a completion date and provide periodic updates against that completion date**
- **Document completion**
 - **Document all actions and sign-off when corrective actions are completed**

Program Management: Documentation

- **Protocol approvals, registration**
 - Signed by investigator, department director, biosafety officer (biosafety coordinator), responsible official (biosecurity coordinator)
- **Medical & vaccination records**
 - Confidentiality requirements must be addressed
- **Policies, Manuals, SOPs**
- **Training records**
 - Document initial training, supervisor training, refresher training
 - Include dates, trainer qualifications, course syllabus, method of evaluation
- **Auditing records**
 - Include follow up actions

Program Management: Documentation Systems

- **Establish a records management system**
 - **Designate a responsible document control coordinator**
 - **Define appropriate document retention time**
 - **Establish procedures for handling sensitive information**



Program Management: Laboratory Biosecurity Plan

- **Develop laboratory biosecurity plan**
 - Facility mission and description
 - Risk definition
 - Physical security
 - Personnel management
 - Material control and accountability
 - Material transfer security
 - Information security
 - Biosecurity program management
 - Incident response plans and reporting



Program Management: Policies



- **Realistic policies**
 - Policies should be comprehensive
 - Policies should allow for users to work as needed
- **Understanding of policies by all users**
 - Having clear policies is critical to users following them
 - The policies should be easy to locate, understand, and follow

Summary

- **Program management is an overarching component of both biosafety and biosecurity programs**

- **Ensures success of the programs by:**
 - **Planning**
 - **Staffing**
 - **Funding**
 - **Training**

- **Addresses every element of the biosafety and biosecurity program**