



# Components of a Biosecurity Program

**International Biological Threat Reduction  
Global Security Center  
Sandia National Laboratories  
April 2009**

**BEP-ANBio Workshop**

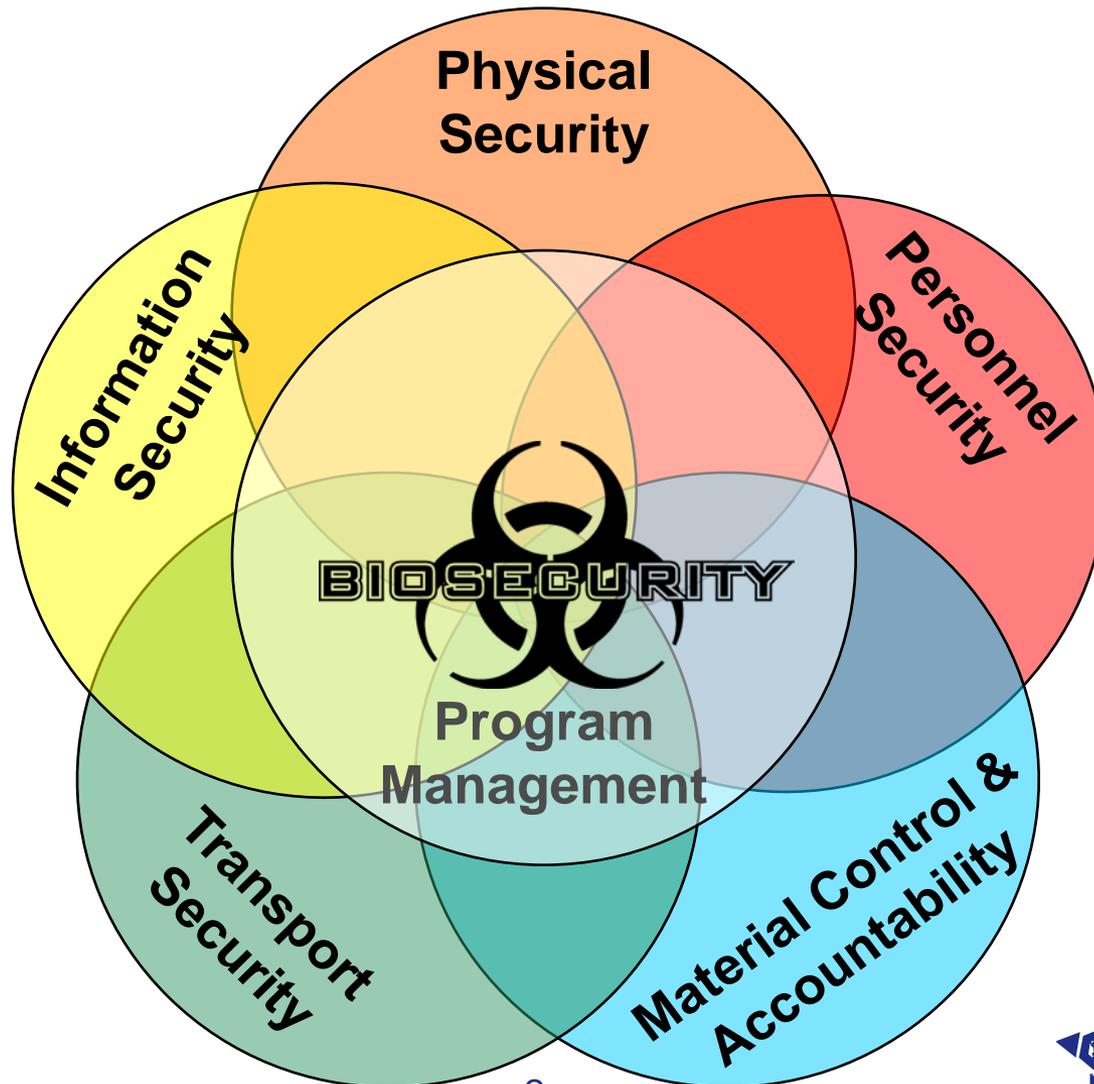


SAND No. 2008-0480P  
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,  
for the United States Department of Energy's National Nuclear Security Administration  
under contract DE-AC04-94AL85000.





# Components of Biosecurity





# Physical Security



# Purpose of Controlling Access

- **Allow entry of**
  - Authorized persons
- **Prevent entry of**
  - Unauthorized persons
- **Allow exit of**
  - Authorized persons





# 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





# Access Control Examples: Manual

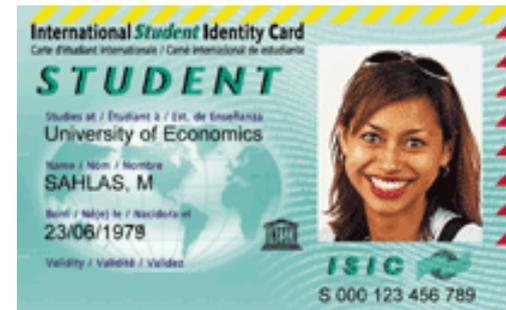
- **Mechanical Keys**

- Controlled keys
- Pros
  - Familiar to user
  - Inexpensive
- Cons
  - Can be copied
  - May be lost or stolen
  - Relatively easy to defeat
  - Must be recovered when authorization is terminated



- **Guard verification of identity**

- May use photo badges or id cards
- Pros
  - Easy to implement
  - Recognize personnel
- Cons
  - Labor intensive
  - Easy to tamper with badge





# Access Control Examples: Coded Badges

## Positive Features

- Control access by area and time
- Record each access
- Have low false rejection rate
- Perform consistently
- Easy to Change Authorization

## Negative Features

- | Identify badge, not person
- | Require maintenance
- | May be defeated by counterfeit badge





# Access Control Examples: Biometric

- **Identification is based on a unique feature, such as:**

- Fingerprint
- Face
- Hand geometry
- Retinal pattern
- Iris pattern

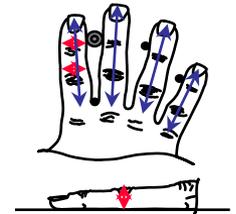


- **Most biometric systems verify identity**

- You claim to be someone by presenting a card or PIN
- System compares recorded template for the claimed identity with the live biometric (one-to-one)

- **Some biometric systems recognize you**

- No claim of identity is required
- System searches through database to find a match (one-to-many)





# 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: 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





# Personnel Security



# Granting Access to the Laboratory

- **Personnel screening**
  - Are they qualified to do the job?
  - Are they trustworthy?
  - Degree of scrutiny proportional to the risks
- **Training**
  - Biosafety and biosecurity
  - Task-specific training
- **Medical evaluation**
  - Immunizations?
  - Potential allergies, compromised immune system?
- **PPE**
  - Training
  - Fit-testing



- **Individuals granted authorized access should be trustworthy individuals who understand the hazards and mitigation measures in place at the facility**



# Personnel Security Programs

- **Personnel security programs address the insider threat**
  - Help an institution determine who they can trust
- **Additional benefits of personnel security programs\***
  - Liability if employee's actions hurt someone
    - **Negligent hiring lawsuits increasing**
  - False information on application for employment
    - **30-40% of all job applications and resumes contain false or inflated information by some estimates**
  - Can help reduce risk of workplace violence
    - **Acts of extreme violence in the workplace are often preceded by some sign of extreme emotional pain, stress, mental disturbance or some previous incident of violent behavior**
  - Others?





# Which Personnel to Vet?

- **Insiders**
  - Have authorized access to the facility, dangerous pathogens, and/or restricted information
  - Who is an insider depends on a facility's access controls and visitor controls
- **Not all positions present the same risk**
  - Risk depends on based on potential for adverse impact to the organization, e.g. variations based on biological material handled
    - *Bacillus anthracis* vs. *Coccidioides immitis* and SARS vs. Plum pox potyvirus
  - Consider:
    - Personnel with direct access to pathogens and toxins
    - Supervisors of personnel with direct access
    - Computer/network personnel with administrative access
    - Security forces
    - Responsible Official and Alternate Responsible Official
    - Locksmiths
    - Personnel with administrative access to the access control system
    - Safety personnel
    - Security personnel
    - Housekeeping personnel
    - Shipping and receiving personnel who handle infectious substance packages



# Vetting Personnel – General Principles

- **Goal: to determine if a person is ‘trustworthy’**
- **Verify identity and personal information**
- **Verify professional information, such as**
  - Previous employment and education
- **Verify character of individual; may include**
  - Interview with individual
  - Interviews with neighbors, associates
  - Checking provided references
- **Verify level of responsibility of individual; may include**
  - Criminal and financial records



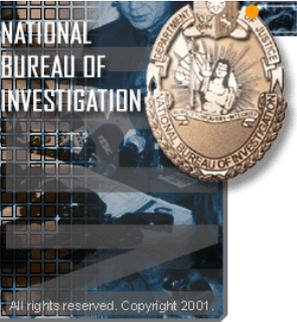
# Approaches for Vetting Individuals

- **Public records**
  - Use governed by national and local regulations
- **Profiling**
- **Polygraphs**
- **Interviews**
- **Drug tests**
- **Medical history**
- **Can be implemented in a graded manner depending on the risk of the position**
  
- **Considerations**
  - Accuracy of information obtained during vetting process
  - Have applicant sign “release of information” statement
  - If periodic reinvestigations will be required, notify applicant during hiring process
  - Legal constraints on use of information for employment decisions





# Background Screening Processes Examples



## The Philippines

- Many positions in the Philippines require a National Bureau of Investigation (NBI) clearance
  - All government positions require an NBI
- Clearance initiated by applicant
- Requires payment and application card
- NBI checks name on card against names in criminal database
  - If a similar name found, NBI will conduct additional research
  - Thumb print required on clearance card and also saved in database

## The UK

- Many positions in the UK require a Criminal Records Bureau (CRB) Disclosure
- Disclosures only available to eligible entities – individual's are not able to access their own disclosure
- Disclosure includes
  - Police records
  - Education and skills records
  - Verification that the individual is not on the protection of children or vulnerable adults lists
  - Any information which the chief officer (police agency completing the disclosure) may believe relevant





# 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





# Visitors: Host Responsibilities and Escorting

- **Prior to visit, host should notify designated institutional representative**
  - Visitor's name and other identifying information
  - Length of stay
- **Escorting**
  - Ensures safety and security
  - Institution needs to set policy on visitor to escort ratios
    - **Can vary between areas at facility based on risk (e.g. animal lab vs. office space)**
  - Are administrative escorting procedures allowed? If so, where?
  - Designated escort must be knowledgeable about areas to be visited



# 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**





# In-Processing

- **In-Processing**
  - How is a new person authorized and
  - Program should document the steps necessary prior to grantee an individual authorized access, e.g.
    - **Background investigation**
    - **Safety and security training**
    - **Job –specific briefing**
    - **Immunizations**
  - Where do new hires work until vetting process and trainings are complete?
    - **Can take months to years depending on process**



# Out-Processing

- **Out-Processing**
  - Access changes or termination
    - **Do combination locks need to be changed?**
  - Retrieve property, including
    - **Badges, keys**
    - **Laboratory notebooks**
    - **Pathogenic materials**
    - **Laptops, PDAs, cell phones, pagers**
    - **Library materials**
  - Deactivate computer and electronic access accounts
  - Is a signed non-disclosure agreement necessary?
  - If appropriate, notification of Responsible Official to change Select Agent program registration



---



# Material Control & Accountability



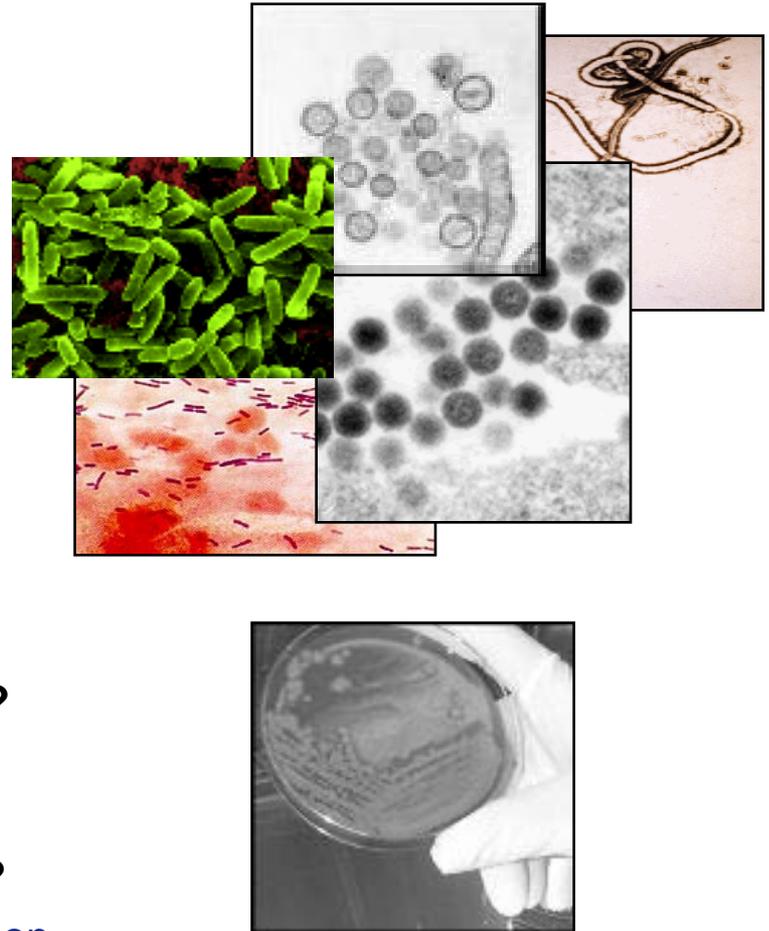
# Material Control & Accountability: Objective

- **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**



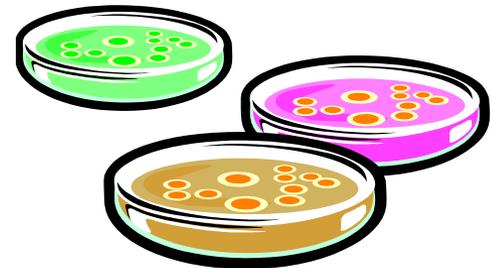
# Material Control and Accountability

- **Defining “material” is complicated**
- **Agent**
  - Name and description
  - What agents are high risk?
  - Viable? Whole organism or DNA?
- **Quantity**
  - Based on containers or other units, NOT number of microbes
  - 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

- **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”
- **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

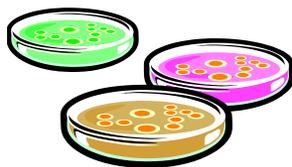




# Material Control & Accountability

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

- Biosafety
- Good research practice
- Business interest





# Transport Security



# Internal Transport Security

- **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 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**



# 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 with reliable carriers are used
- Chain of Custody is maintained
- Notification of successful receipt





# Information Security



# 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





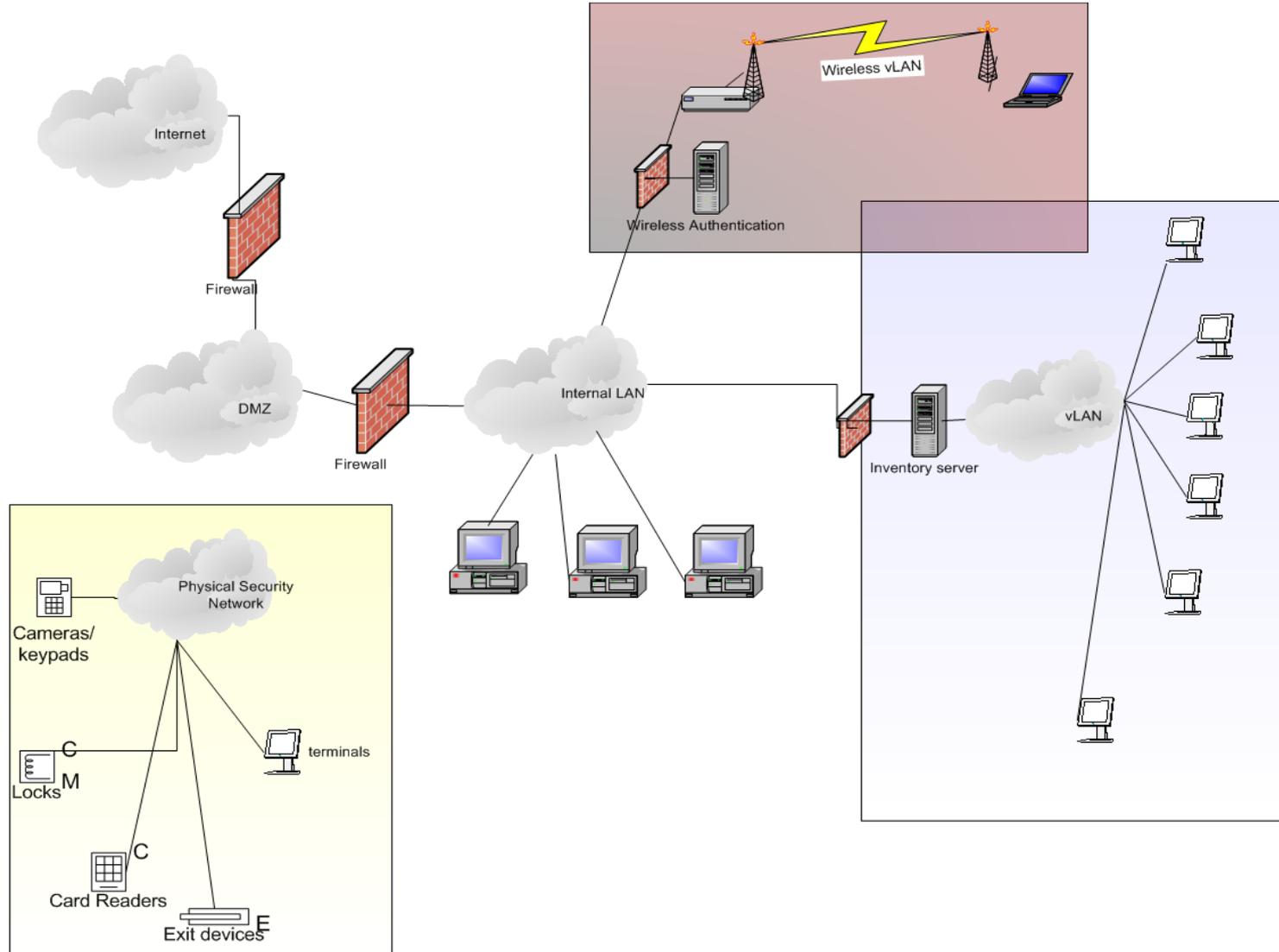
# Information Security: Communication and Network Security

- **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





# Program Management



# Potential Conflicts between Laboratory Biosafety and Physical Security

- **Emergency alarm – electronic locks**
  - Safety – doors fail open
  - Security – doors fail secure
- **Emergency egress**
  - Safety – move people into the safest location as quickly as possible
  - Security – prevent people from moving into or through restricted areas
- **Keys required inside laboratory areas**
  - Safety – contamination concern
  - Security – multiple layers of access
- **Others?**





# Conclusions

- **Need to integrate biosafety and biosecurity considerations into decisions about laboratory operations**
- **Risk assessment is the fundamental resource allocation tool**
  - For making decisions about which risks need to be protected against
  - Graded protection
- **Biosecurity is a key part of laboratory operations**
  - Sustained effort required to build a security culture
- **Program management is an overarching component of both biosafety and biosecurity programs**
  - Should address every element of the biosafety and biosecurity program

**“Security precautions should become a routine part of laboratory work, just as have aseptic techniques and other safe microbiological practices.”**

**(WHO LBM 3rd edition)**

