

# Laboratory Biosecurity

[www.biosecurity.sandia.gov](http://www.biosecurity.sandia.gov)

SAND No. 2005-3288 C

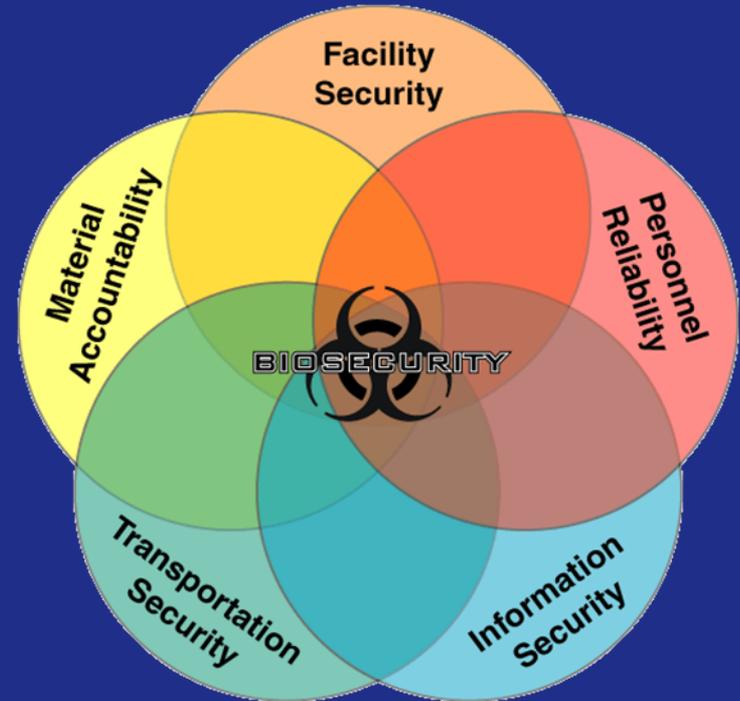
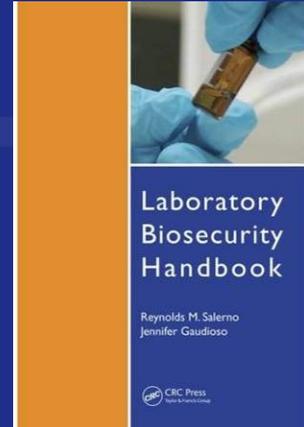
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,  
for the United States Department of Energy's National Nuclear Security Administration  
under contract DE-AC04-94AL85000.



# A Systems Approach to Biosecurity

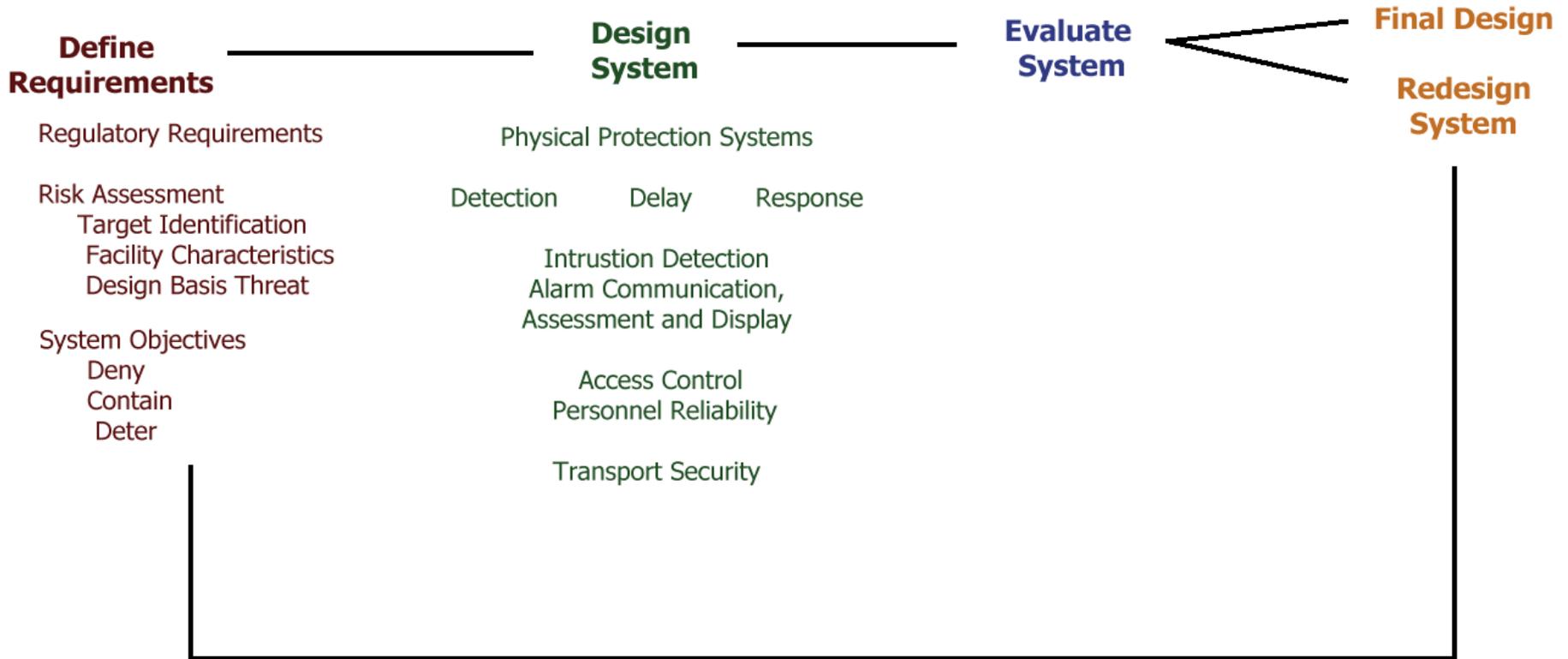


- **Biosecurity system components**
  - Physical security
  - Personnel security
  - Material handling and control measures
  - Transport security
  - Information security
  - Program management practices
- **Each component implemented based on results of risk assessment**
- **Biosecurity mitigates risk for both**
  - The insider
  - The outsider





# Laboratory Biosecurity Systems





# Biosecurity Risk Assessment

## 1. Characterize assets and threats

- a. Identify and evaluate assets (including pathogens and toxins)
- b. Evaluate adversaries who might target those assets

## 2. Evaluate scenarios

- a. Create scenarios consisting of “specific adversaries” attempting to target specific assets
- b. Determine how the various scenarios could be perpetrated (vulnerability assessment)

## 3. Characterize the risk

- a. Evaluate threat potential and consequences of each scenario
- b. Determine acceptable and unacceptable risks; develop risk statement





**“...given the high level of know-how needed to use disease as a weapon to cause mass casualties, the United States should be less concerned that terrorists will become biologists and far more concerned that biologists will become terrorists.”**

**-World At Risk,**

The report of the commission  
on the prevention of  
weapons of mass destruction  
proliferation and terrorism,  
December 2008



# Biological Targets

- **Identification of a ‘target’ is more difficult for biological agents/materials**
  - Microbes cannot be counted
  - The ‘target’ or asset maybe all over a room, inside an animal, in the waste system, etc
  - Microbes cannot necessarily be detected if missing (an entire tube may be detected but not a microbe from within)
- **Material Control and Accountability (MC&A) ensure complete and timely knowledge of:**
  - What materials exist
  - Where the materials are
  - Who is accountable for them
- **NOT: to detect whether something is missing**



# Design Basis Threat

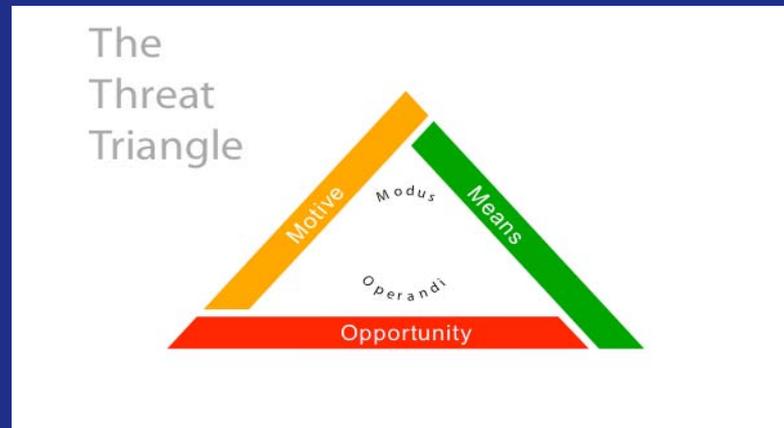
- **Threat assessment is challenging**
  - Little information about targeting of bioscience facilities
  - Little historical data
- **Threats become a policy decision**
  - Design basis threat is a policy statement that articulates the threats and the security system objectives
- **Design Basis Threat statement**
  - Should be developed by all stakeholders
    - Scientific and operational personnel at institution
    - Signed by Head of institution or other responsible decision maker





# Assessing Threats

- **Motive**
  - The reason for the crime. Motivations include ideological, personal, economic, and psychotic. Motivations give rise to a particular intent or objectives. They also impact behavior (e.g., passive or active, violent or nonviolent).
- **Means**
  - The tools used to commit the crime. Tools include: knowledge (general and specific); equipment (e.g., tools, weapons, explosives, transportation); and people (willing, coerced or unknowing). For an outsider – an insider can be a tool.
- **Opportunity**
  - The occasion that presents itself to allow a crime (e.g., theft or sabotage) to take place.





# Define System Objectives

- **Management responsible for meeting all international, national, and local regulatory requirements**
  - Biological Weapons Convention
  - UN Security Council Resolution 1540
  - National regulations
- **Risk assessment allows management to decide which scenarios to actively protect against – establish a design basis threat**
- **Management determines security system strategy:**
  - Deny: prevent adversary from gaining access to particular pathogen or toxin
  - Contain: prevent adversary from leaving facility while in possession of stolen pathogen or toxin
  - Deter: discourage adversary from stealing a particular pathogen or toxin by making theft of that agent appear very difficult



# Physical Protection System Principles

- **Detection**

- Intrusion Detection is the process to determine that an unauthorized action has occurred or is occurring
- Detection includes sensing the action, communicating the alarm, and assessing the alarm

- **Delay**

- Slowing down an adversary's progress

- **Response**

- The act of alerting, transporting, and staging a security force to interrupt and neutralize the adversary
- Mitigation and recovery interface with the response function

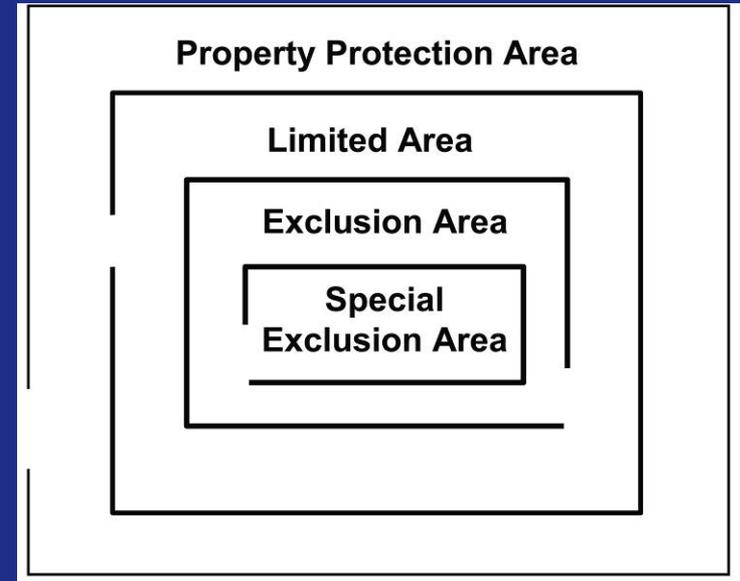
- **Access Control**

- The mechanism to 'by pass' the physical security system



# Graded Protection

- **Property Protection Areas**
  - Low and Very Low Risk Assets
    - Grounds
    - Public access areas
    - Warehouses
- **Limited Areas**
  - Moderate Risk Assets
    - Most bioscience laboratories
    - Administrative offices
    - Hallways adjoining Exclusion Areas
- **Exclusion Areas**
  - High Risk Assets
    - Some high containment laboratories
    - Computer network hubs
- **Special Exclusion Areas**
  - Very High Risk Assets
    - Extremely valuable intellectual property
    - Dangerous biological agents not found in nature





# Purpose of Controlling Access

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





# Basis of Access Controls

- **Something you have**
  - Key
  - Card
- **Something you know**
  - Personal Identification Number (PIN)
  - Password
- **Something you are**
  - Biometric feature (i.e., fingerprints)
- **Combining factors greatly increases security**

Badge swipe  
and PIN



Hand-geometry  
Biometrics



# Considerations for Access Control

- **Access control systems**
  - Can be low or high tech
  - Give varying levels of assurance of person's identity
    - **Risk assessment!**
  - Have error rates and enrollment issues
    - **1-3% of the population is incompatible with any biometric device**
    - **Must have secondary method for those who cannot pass automated inspection**
  - Needs to accommodate peak loads / throughput
  - Should be designed for both entry and exit



# Examples of Electronic Access Controls

- **Coded Badges**

- Proximity Cards
- Magnetic Stripe Badges
- Wiegand Cards
- Smart Cards

- **Biometrics**

- Fingerprint Scanner
- Hand Geometry Scanner
- Iris Scanner



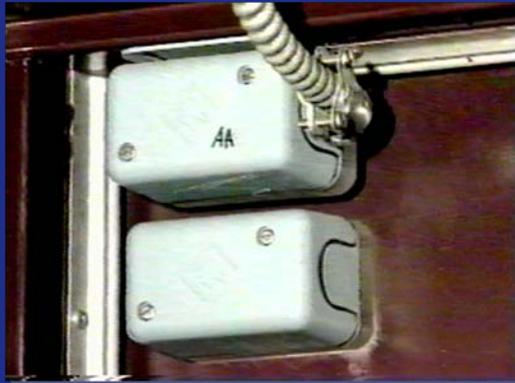


# Intrusion Detection

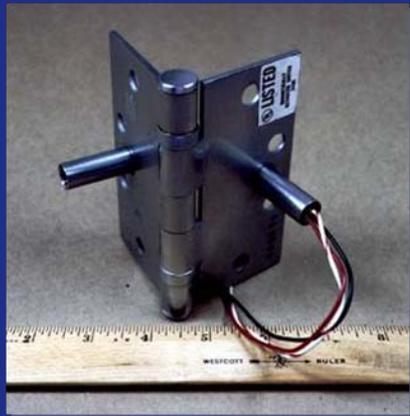
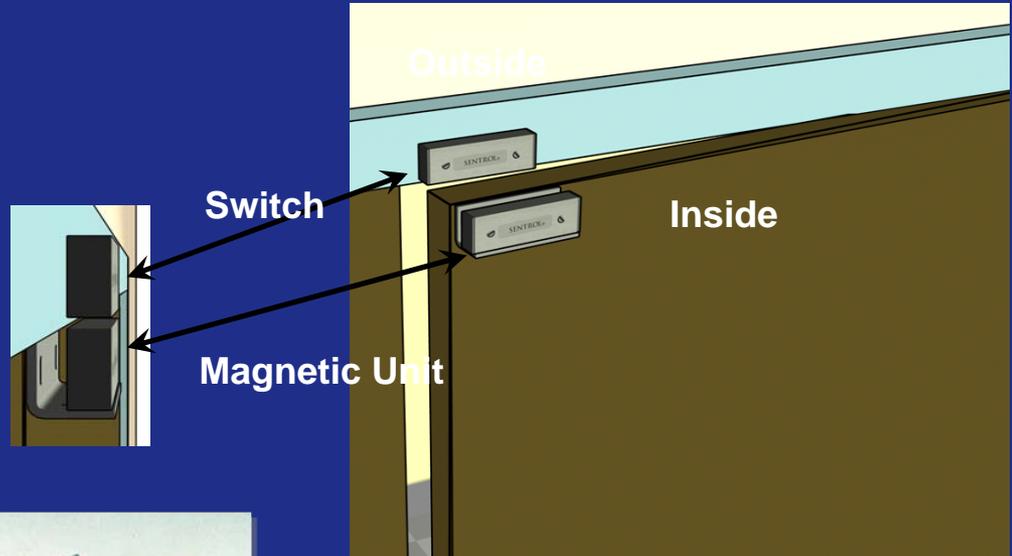
- **Objective: Detect unauthorized access**
- **Many types of intrusion detection**
  - Personnel notice unauthorized access attempt
    - **Training**
  - Boundary sensors most applicable for bioscience facilities
    - **Magnetic switches on doors**
    - **Glass break sensors on windows**
  - Volumetric sensors may be appropriate for low-use areas of high risk (e.g. culture collection storage rooms)
    - **Microwave**
    - **Passive infrared**



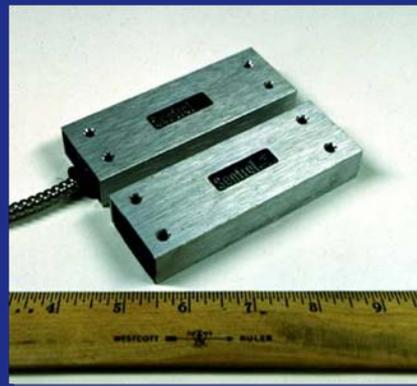
# Magnetic Switches Detection and Delay



Balanced magnetic switch



Covert magnetic switch



Complex balanced magnetic switch



# Alarm Assessment

## Direct observation by guards

- Can be trained employees or other on-site security
- Takes time and can put guard in danger
- Can provide immediate response
- Can only tolerate low rate of nuisance alarms
- Labor intensive



## Remote assessment by video

- Video is immediate and focused
- Video is displayed to an alarm station operator for assessment
- Assessment of an alarm can occur almost immediately
  - Pre-event and post-event recording possible
- Later audit and review
- Efficient use of people
- Requires video infrastructure
- Can have high initial expense
- Maintenance can be expensive





# Video Assessment vs. Video Surveillance

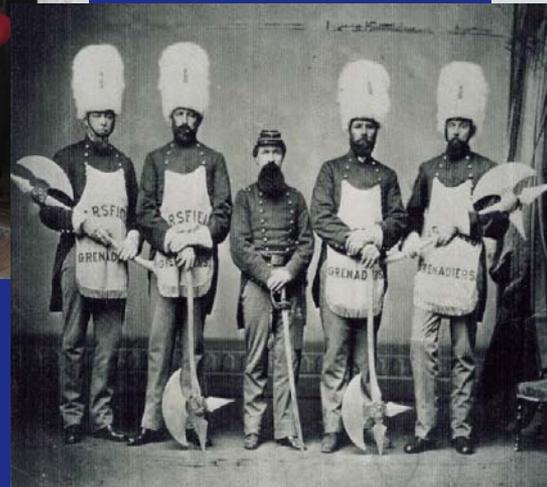
- **Assessment**
  - Alarm information triggered by sensor activation and directed to a human to determine if unauthorized access has occurred in a sensed area
  - Cameras located at sensor locations – e.g. pointed at doors
- **Surveillance**
  - Continuous use of a human as a intrusion detector to monitor several restricted areas that are NOT sensed by intrusion technologies
  - Systems often have many cameras
  - Someone must watch all video screens all the time
    - **Personnel can only watch a few screens for a limited amount of time before fatigue**





# Guards

- Guards delay and detect the intruders and in some cases also provide response





**“Somebody once said that in looking for people to hire, you look for three qualities: integrity, intelligence, and energy. And if they don't have the first, the other two will kill you. You think about it; it's true. If you hire somebody without the first, you really want them to be dumb and lazy.”**

**- Warren Buffett**



# Threats to Bioscience Facilities: Insiders vs. Outsiders

**Scenarios involving Insiders generally pose a higher risk than scenarios involving Outsiders**

## Insiders

- Access to facility and buildings where biological agents are stored and used
  - Can wait for an opportune time
  - Have knowledge of facility operations and security system
  - Some have relevant technical skills and know how to covertly remove the desired biological agent
- **Opportunity – yes**
  - **Means – yes**
  - **Motive – ?**

## Outsiders

- Most biological agents can be readily found elsewhere
    - **Other laboratories and in nature**
  - Do not have authorized access
  - Have limited knowledge about facility operations and security
  - Will not know exactly where the desired biological agent is stored
  - Collusion with an Insider increases risk of detection
- **Opportunity – significantly less**
  - **Means – typically less**
  - **Motive – ?**



# Which Personnel to Vet?

- **Insiders**

- Have authorized access to the facility, dangerous pathogens, and/or restricted information
- The 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 virus 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
- Biorisk Officer

- 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



# Approaches for Vetting Individuals

- **Public records**
  - May also be applicable state and local regulations
- **Personality testing**
- **Skill testing**
- **Interviews**
- **Drug tests**
- **Medical history**
  
- **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



# Reinvestigations

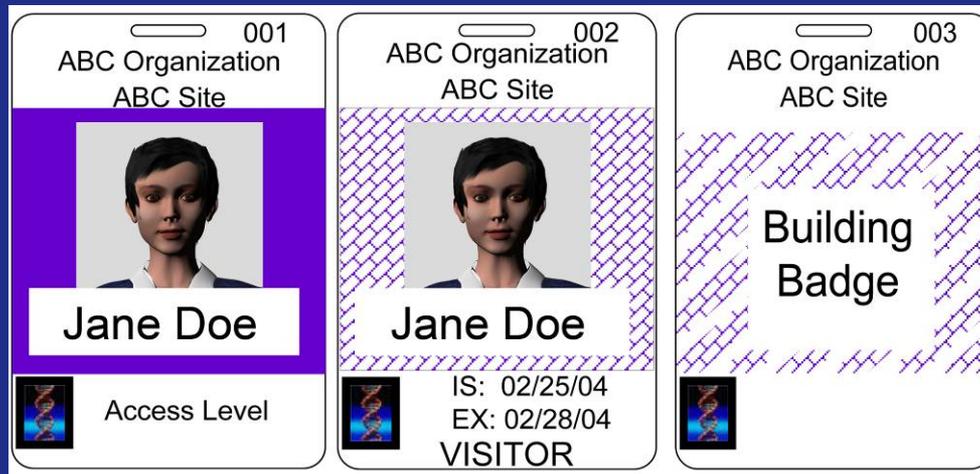
- **A security reinvestigation establishes any security related changes in a person's life**
  - The same checks are typically run as in initial investigation
    - **Differing checks are often the result of a new type of clearance**
    - **The reinvestigation process often doesn't recheck already verified military service records or educational records**
  - Timeline from last investigation to present
  - Identifies changes like
    - **New personal contacts**
    - **New financial situations**
    - **Situations which should have been reported**
    - **Discrepancies from past investigations**





# Badges

- **Badges should be issued to those individuals authorized to be in restricted areas**
- **Badge information should include**
  - Individual's name
  - Individual's photograph
  - Expiration date
  - Indication of areas where individual has authorized access
- **Badge return**
  - Upon employee termination
  - Daily or at the conclusion of a limited term for visitors
- **Report lost or stolen badges**





# Visitor Controls

- **Types**

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



- **Controls**

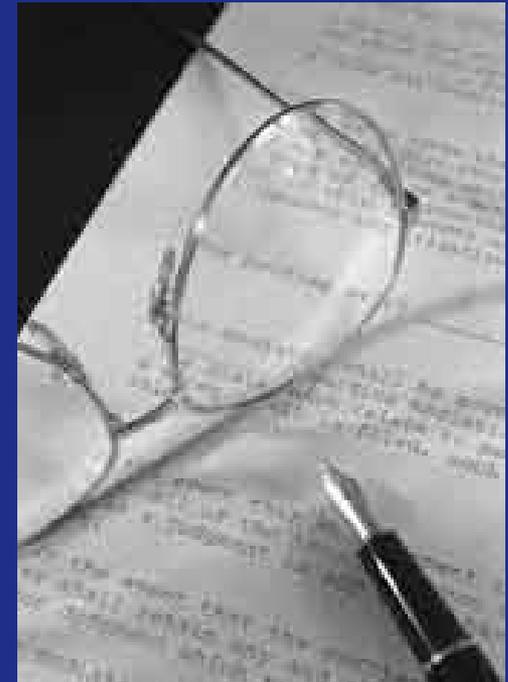
- All visitors should have a host at the facility
- Visitors should be escorted in restricted areas
- Institution needs to establish policy on amount of advance notice required for each type of visitor





# Information Security

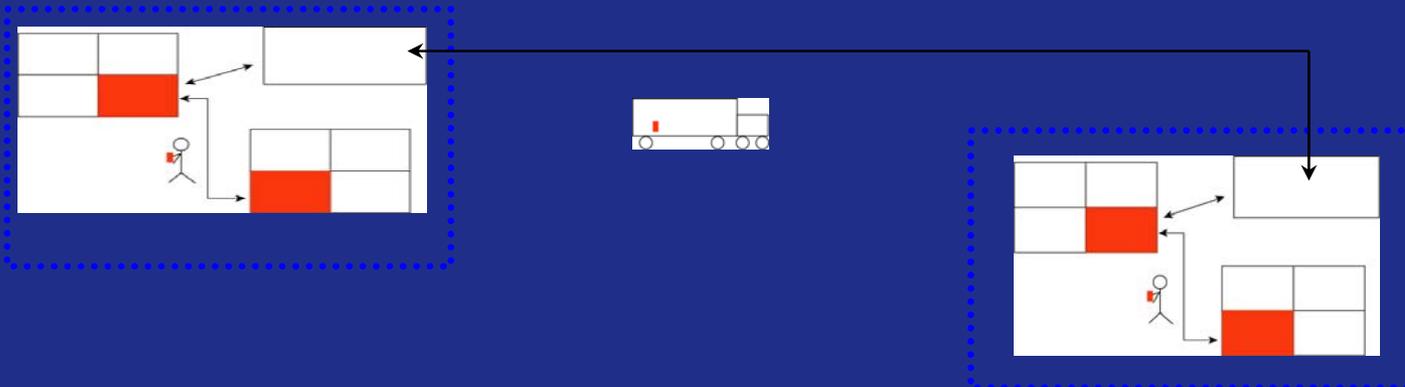
- **Protect information that is too sensitive for public distribution**
- **Risks to information include**
  - Loss of integrity
  - Loss of confidentiality
  - Loss of availability
- **Biosecurity-related sensitive information**
  - Security of dangerous pathogens and toxins
    - Risk assessments
    - Security system design
  - Access authorizations





# 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?
  - Shipper documentation and control?





# 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
- Must follow IATA regulations



