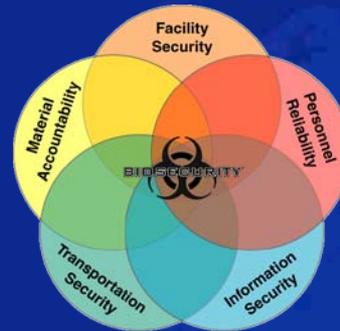




Physical Security



Biosafety and Biosecurity Awareness Training
For Afghan and Pakistani Bioscientists
December 7 to 9, 2009

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.



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

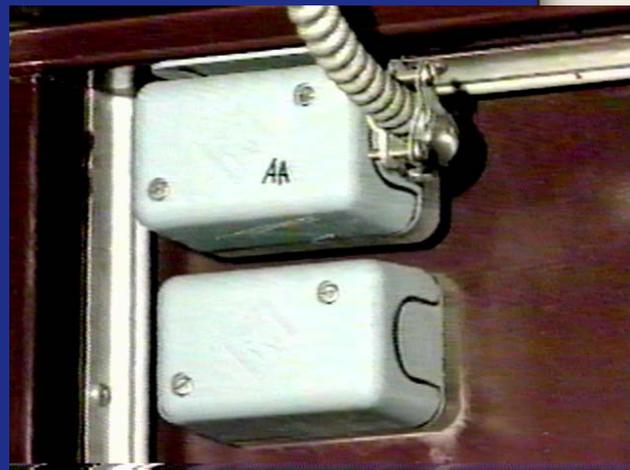
- **Access Control**

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



Intrusion Detection

- Detect unauthorized access
- Many types of intrusion detection
 - Personnel notice unauthorized access
 - Electronic Sensor





Video Assessment vs. Video Surveillance

- **Assessment**

- Alarm information triggered by sensor activation and directed to a human to determine if unauthorized access has occurred
- Cameras can be used to communicate
- Humans can directly observe

- **Surveillance**

- Continuous use of a human as a intrusion detector to monitor several restricted areas
- Systems often have many cameras
- Someone must watch all video screens all the time





Delay

- Slow down an intruder
- Detection should come before delay

- Many types of delay methods
 - Guards
 - Perimeter Fencing
 - Solid doors with locks
 - Bars on windows
 - Magnetic switches on doors





Guards

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





Response

- **The objective of response is tied to the overall system objective**
 - Deny: To prevent an adversary from reaching the target/objective
 - Contain: To 'catch' an adversary before they leave with the target or before they accomplish the objective
 - Deter: To initiate consequence mitigation measures



Response Force

- **On-site guard force**
 - Patrols perimeter and buildings
 - Summons and directs local law enforcement
 - Deters
 - Can be the primary response depending on the motives of the adversary
 - Information gathering for secondary response

- **Local law enforcement**
 - Secondary response
 - Reinforce on-site guard force
 - Respond according to plan when summoned
 - Equipped and authorized to confront adversary





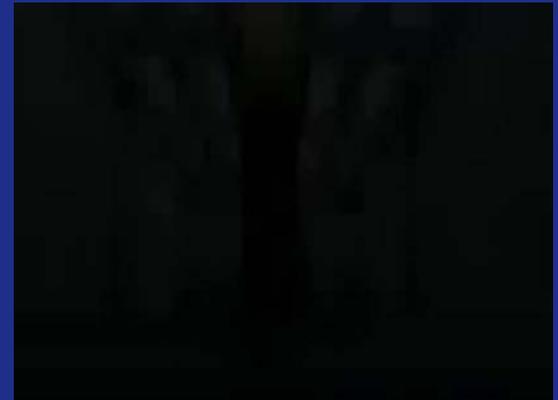
Response Force Requirements

- **Qualification and training**
 - Enforcement responsibilities and skills
 - Equipment familiarity and training
 - Familiarity with facility features and operations
 - Knowledge of restricted area access and biosafety
- **Guard Force Orders**
 - List specific duties and limits of authority
 - Procedures for response to specific alarm conditions
 - Emergency response procedures
 - Notification list
- **Memorandum of understanding with local law enforcement**
 - Specific instructions and agreements
 - On-site training and orientation



Access Control

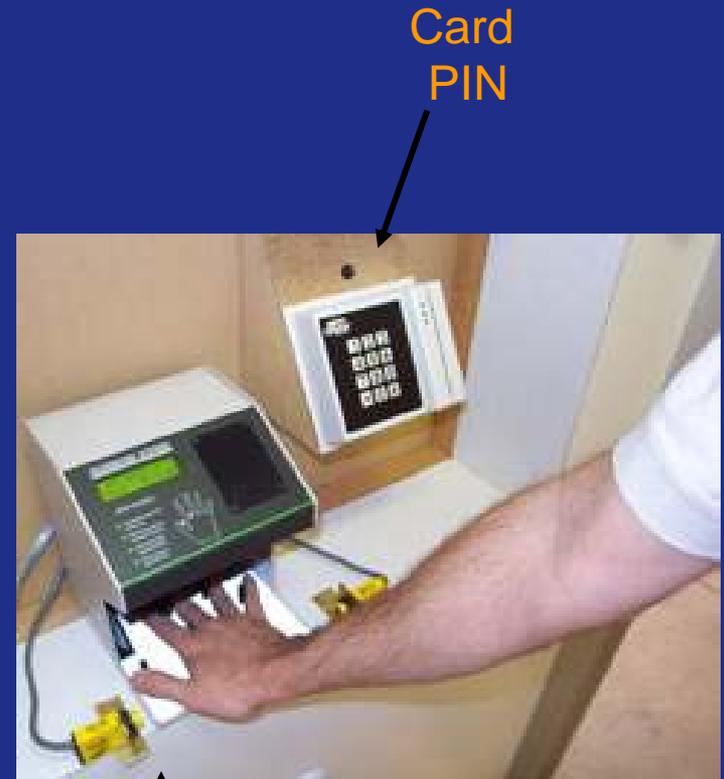
- **Mechanism to 'by-pass' security system**
- **Allow entry of**
 - Authorized persons
- **Prevent entry of**
 - Unauthorized persons
- **Allow exit of**
 - Authorized persons





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, face)
- **Combining factors greatly increases security**

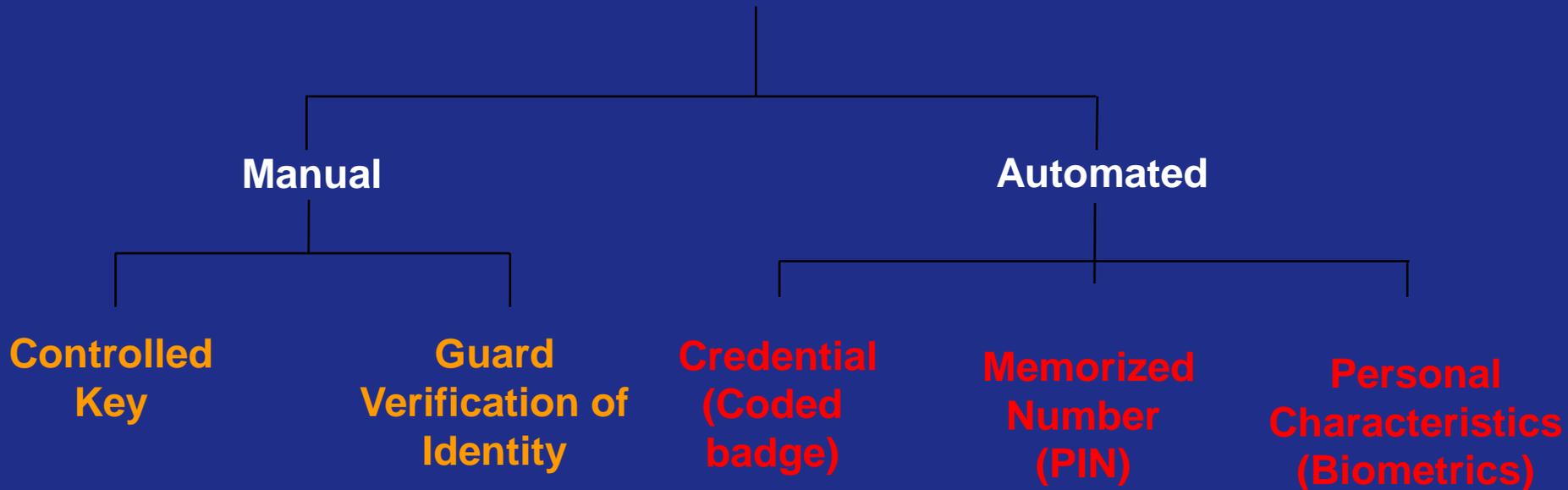


Biometrics



Access Control Techniques

Personnel Entry Control





Examples of Electronic Access Controls

Coded Badges

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

Biometrics

- Fingerprint Scanner
- Hand Geometry Scanner
- Iris Scanner



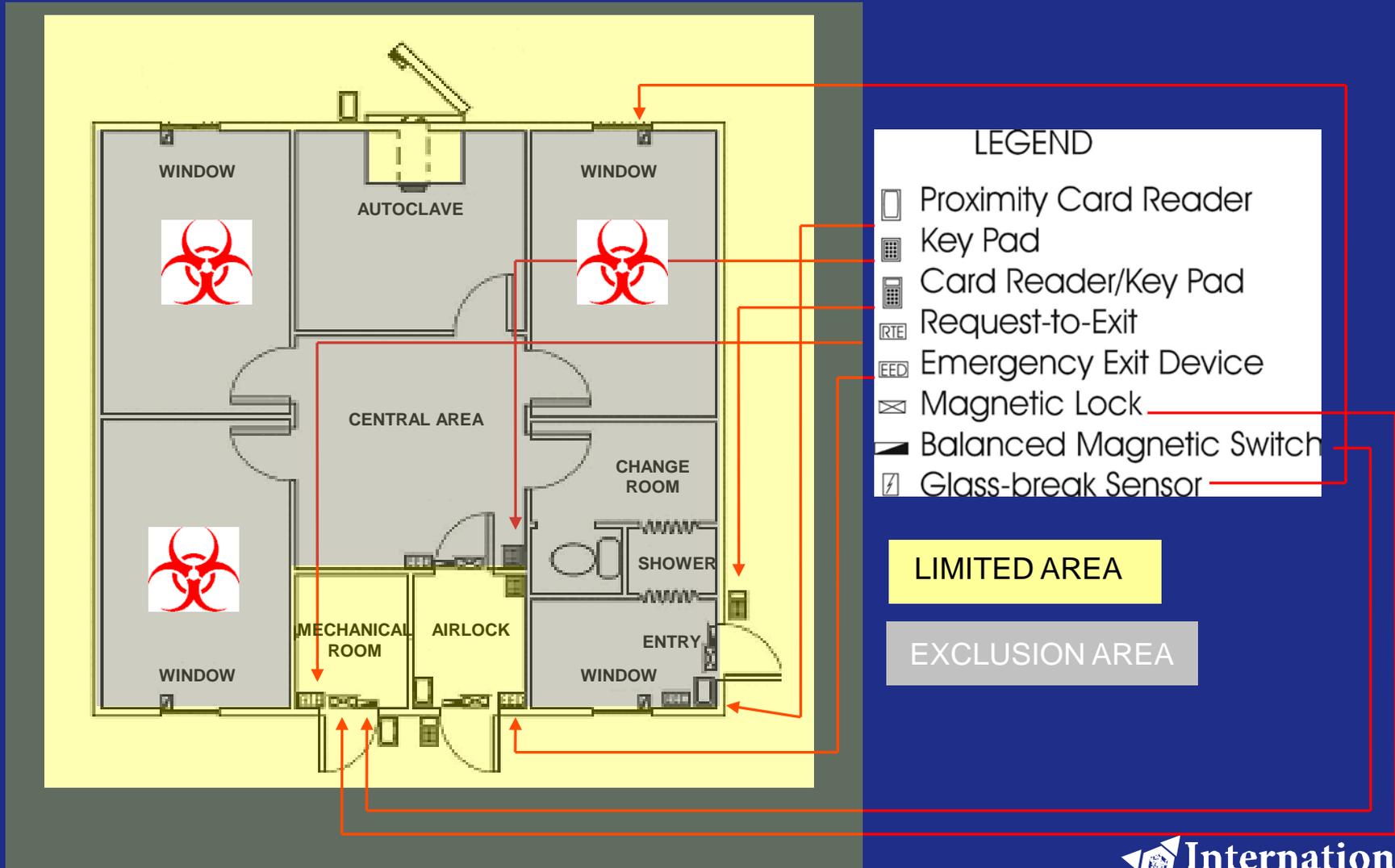


Key Considerations in Selecting Access Controls

- **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
 - Should be designed for both entry and exit



Physical Security: Example Laboratory Building





Questions to think About

- **What types of detection devices would be appropriate in a bioscience facility and why?**
 - Are there types of detection devices that can not be used and why?
- **What are appropriate delay mechanisms for a bioscience facility?**
- **How should a bioscience facility respond to an alarm?**
- **What types of access controls can be used?**
 - Where?
 - Are there types that can not be used in a bioscience facility and why?