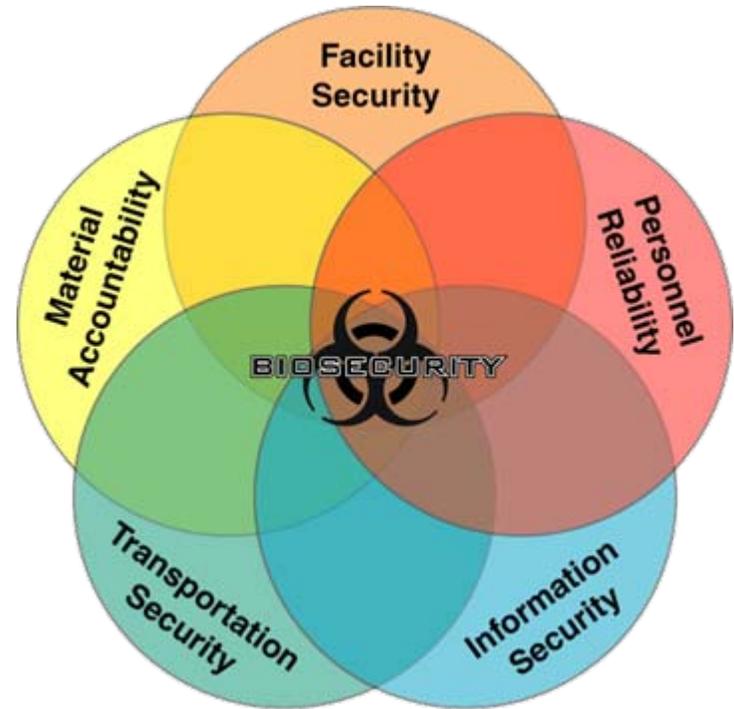

Components of Biosecurity I

Sandia National Laboratories
Laboratory Biosecurity and Biosafety Workshop
Pune, India
3 May 2006

www.biosecurity.sandia.gov

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**

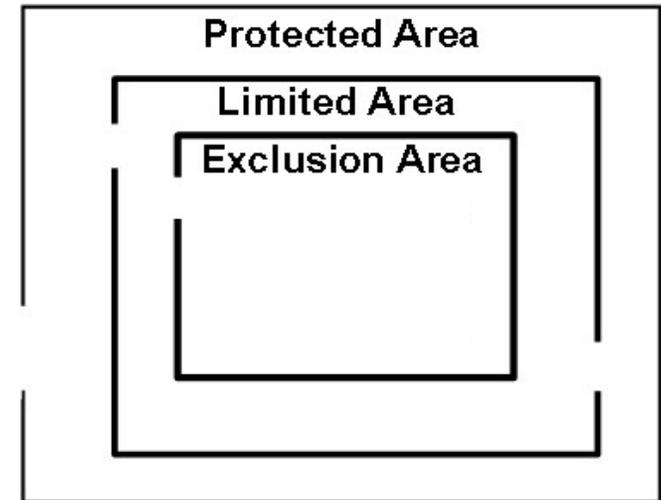
- **Low risk assets**
 - Grounds
 - Public access offices
 - Warehouses

- **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

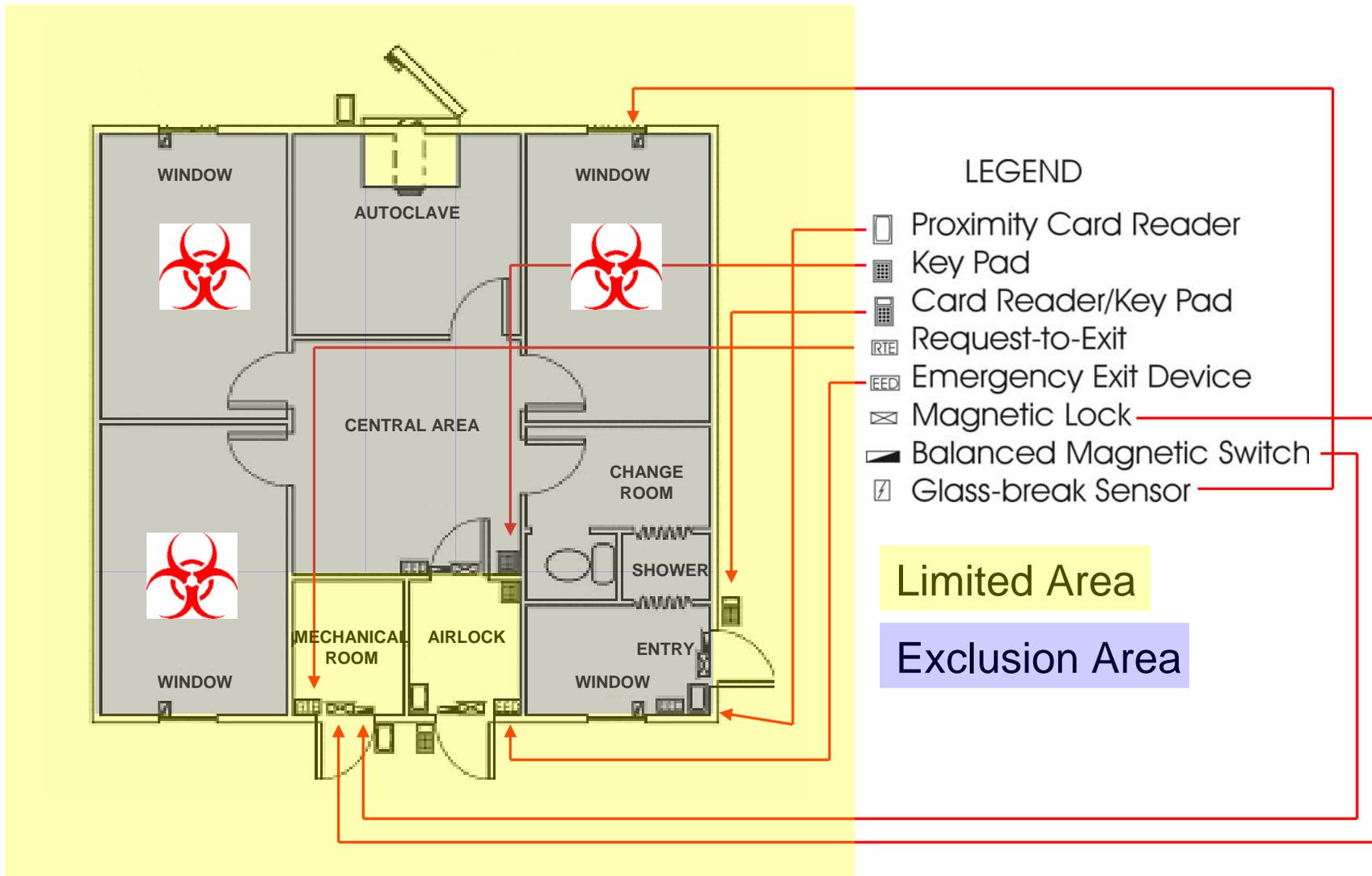
- **Access control ensures that only authorized individuals are allowed into certain areas**
 - Increasingly strict controls as you move toward higher risk assets
- **Limited Areas**
 - Unique item
 - Controlled possession
 - Electronic or physical key
- **Exclusion Areas**
 - Unique item
 - Unique knowledge
 - 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**

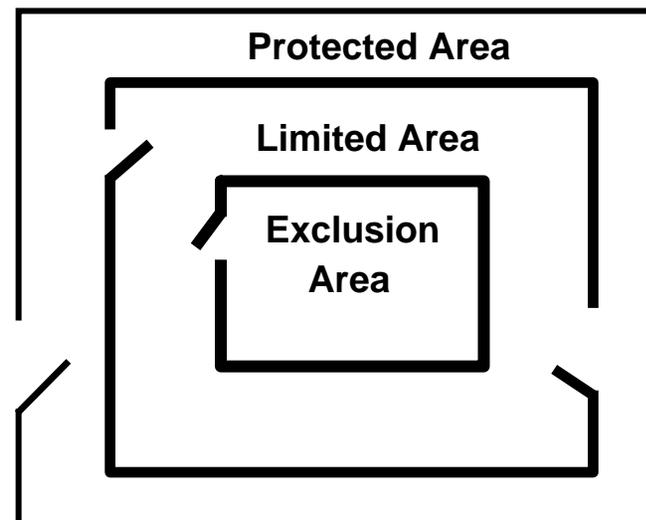
Physical Security

- **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**

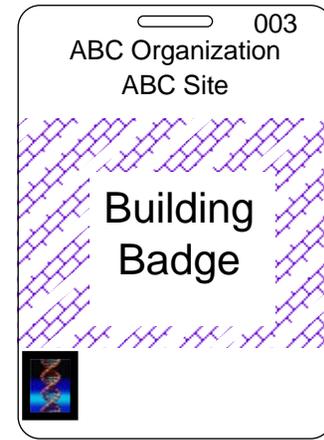
- **Visiting researchers**
- **Facility maintenance personnel**

- **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**



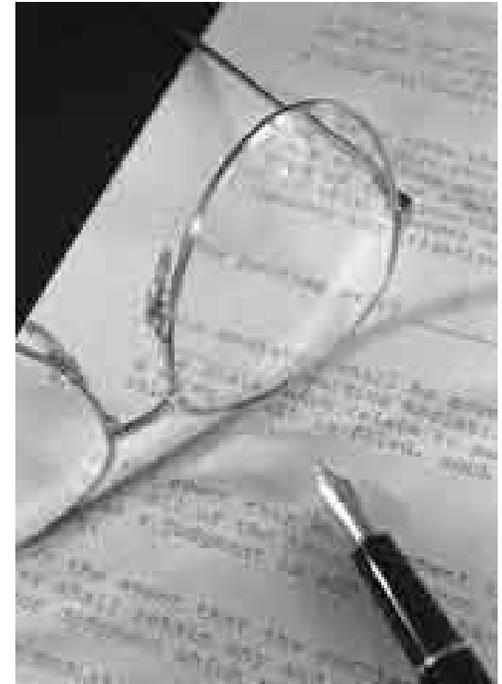
- **High**

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

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

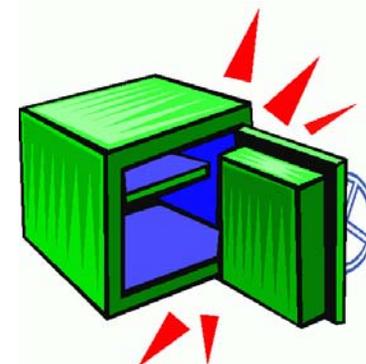
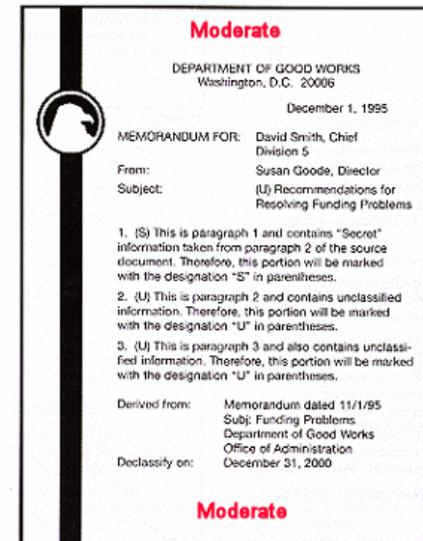
- Designated sensitivity level
- A review and approval process aids in the identification of sensitivities
 - Critical prior to public release of information

● 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

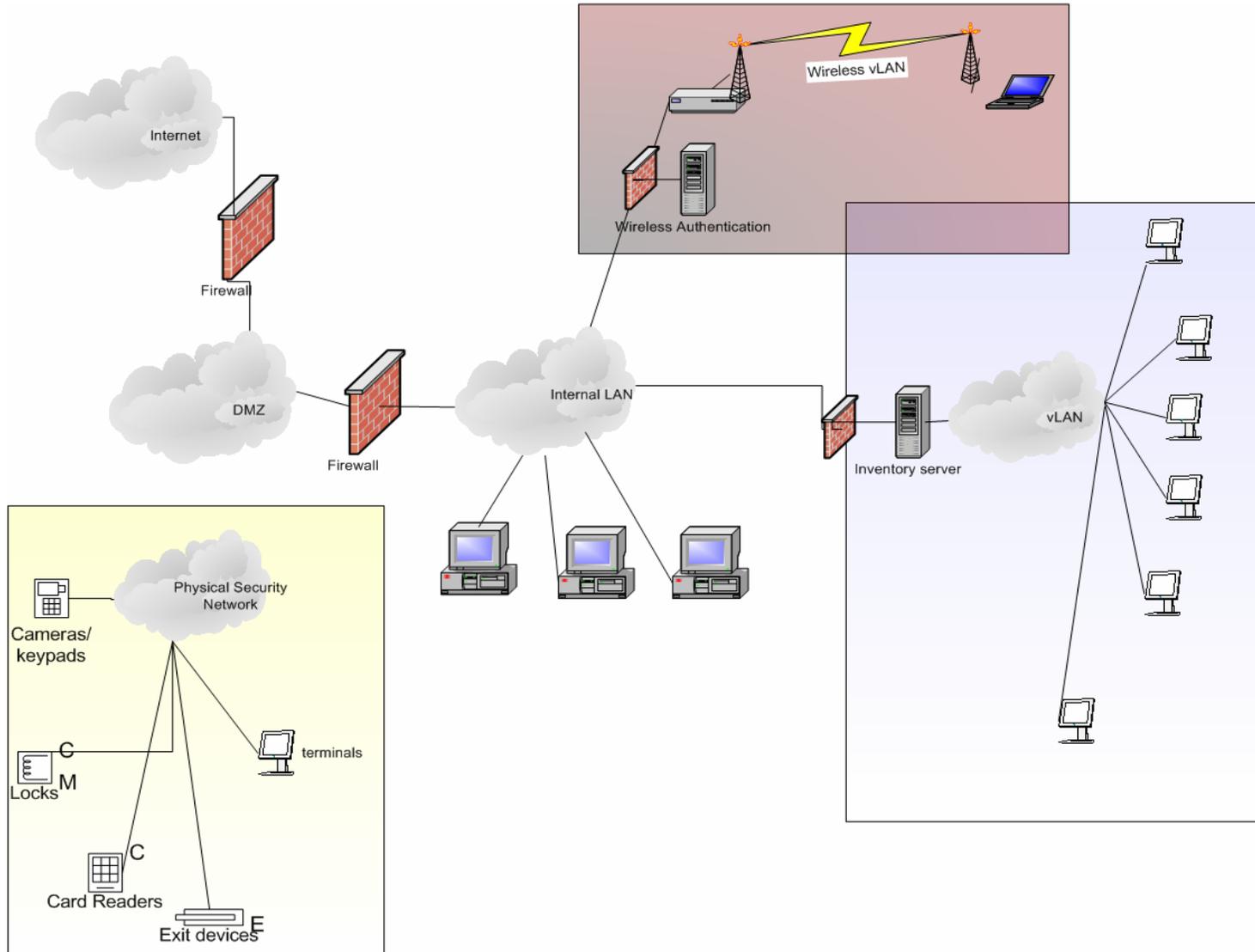
- Sensitivity level designation
 - Top and bottom of each page / cover sheet
- Marking and control methods should be well understood by those working with information



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

