



Technical Requirements for Bio-Lab Security

**Preventing Bio Terrorism
1st Interpol Global Conference
Lyon, France
March 1, 2005**

**Natalie Barnett
Sandia National Laboratories**



Security System Considerations

- **Cannot protect every asset against every conceivable threat**
- **Detection of theft extremely difficult**
 - **Microscopic**
 - **No detectable signature**
 - **Constantly changing quantities**
- **User input necessary**
 - **Minimize operational impacts**
 - **Integrate with biosafety systems**
- **Resources are limited and must be allocated effectively**
 - **Risk assessment**





Evaluate Value of the Assets from an Adversary's Perspective

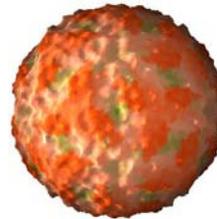
- **Biological agents**

- **Consequences**

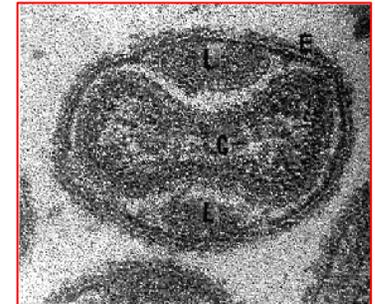
- Lethality
 - Morbidity
 - Infectivity
 - Transmissibility

- **Weaponization potential**

- Environmental hardiness
 - Ease of processing
 - Ease of distribution
 - Ease of growth
 - Availability
 - Ability to camouflage as a natural outbreak



FMD virus



Variola major

- **Information related to the security of dangerous biological materials could assist an adversary in gaining access**
- **Operational systems may be targeted to facilitate gaining access to dangerous biological materials**



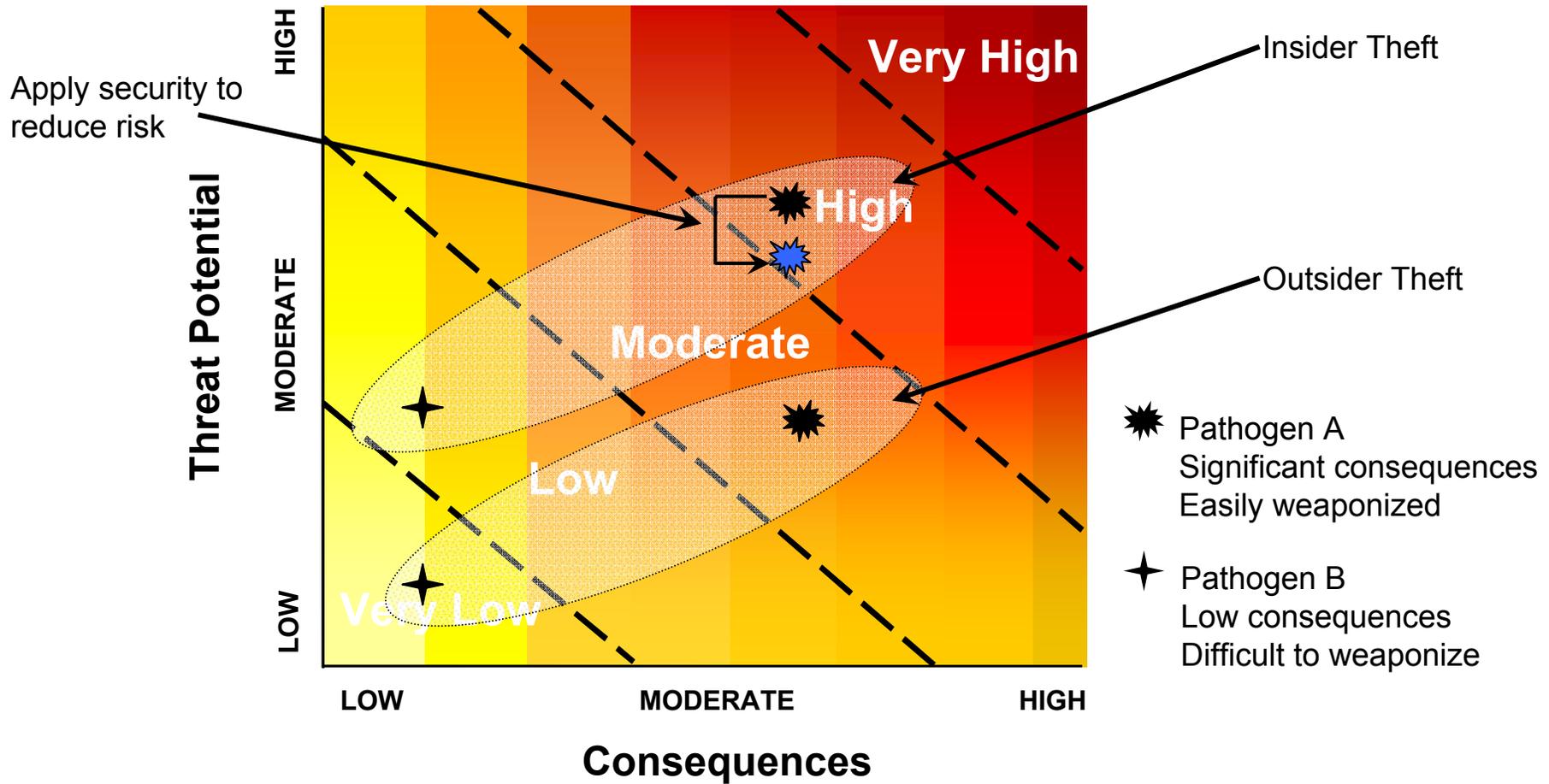
Elements of Risk

- Evaluate adversaries
 - Insiders
 - Outsiders
- Evaluate threat potential
 - Capabilities
 - Tools
 - Motivation
 - Weaponization potential
 - Possibility of being caught
- Evaluate consequences
 - Death and illness
 - Economic
 - Symbolic
 - Social





Risk



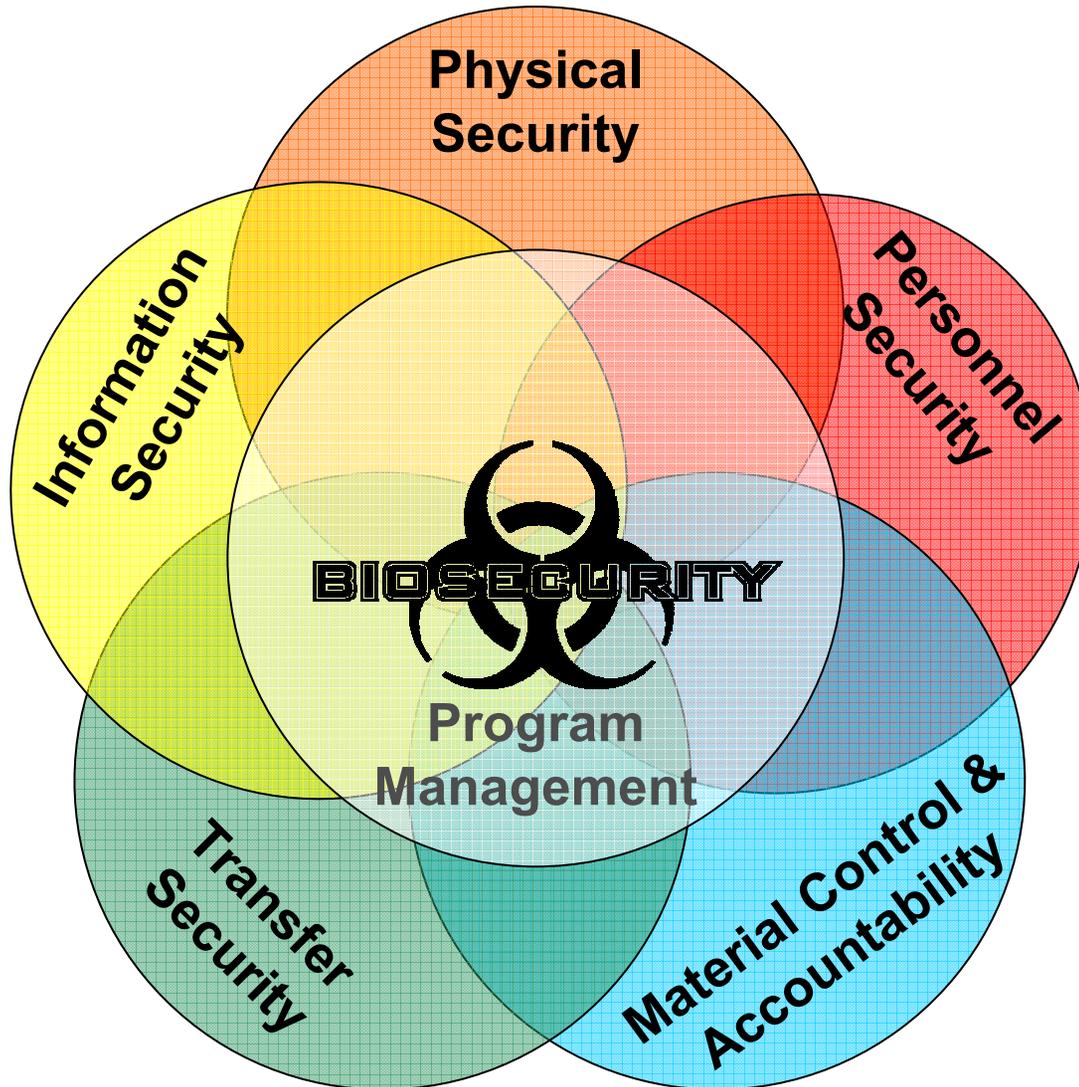


Management Responsibilities

- **Identify which possible but unlikely scenarios the security system should not be required to protect against**
- **Establish a protection strategy**
- **Determine the physical security system design**
- **Develop security policies and procedures**
- **Allocate resources**



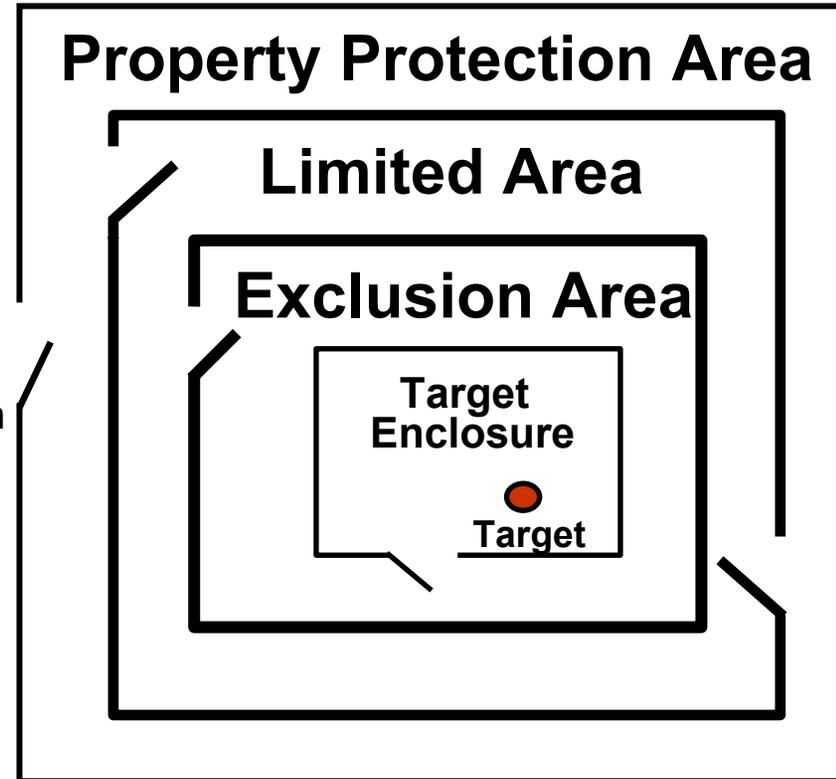
Components of Biosecurity





Graded Protection

- **Property Protection Areas**
 - Grounds
 - Public offices
 - Low Risk Pathogens or Toxins
- **Limited Areas**
 - Moderate Risk Pathogens or Toxins
 - Offices containing sensitive information
 - Healthy animal care facilities
 - Hallways surrounding Exclusion Areas
- **Exclusion Areas**
 - High or Extreme Risk Pathogens or Toxins and contaminated animals
 - Computer network hubs
 - Electronic security system hubs





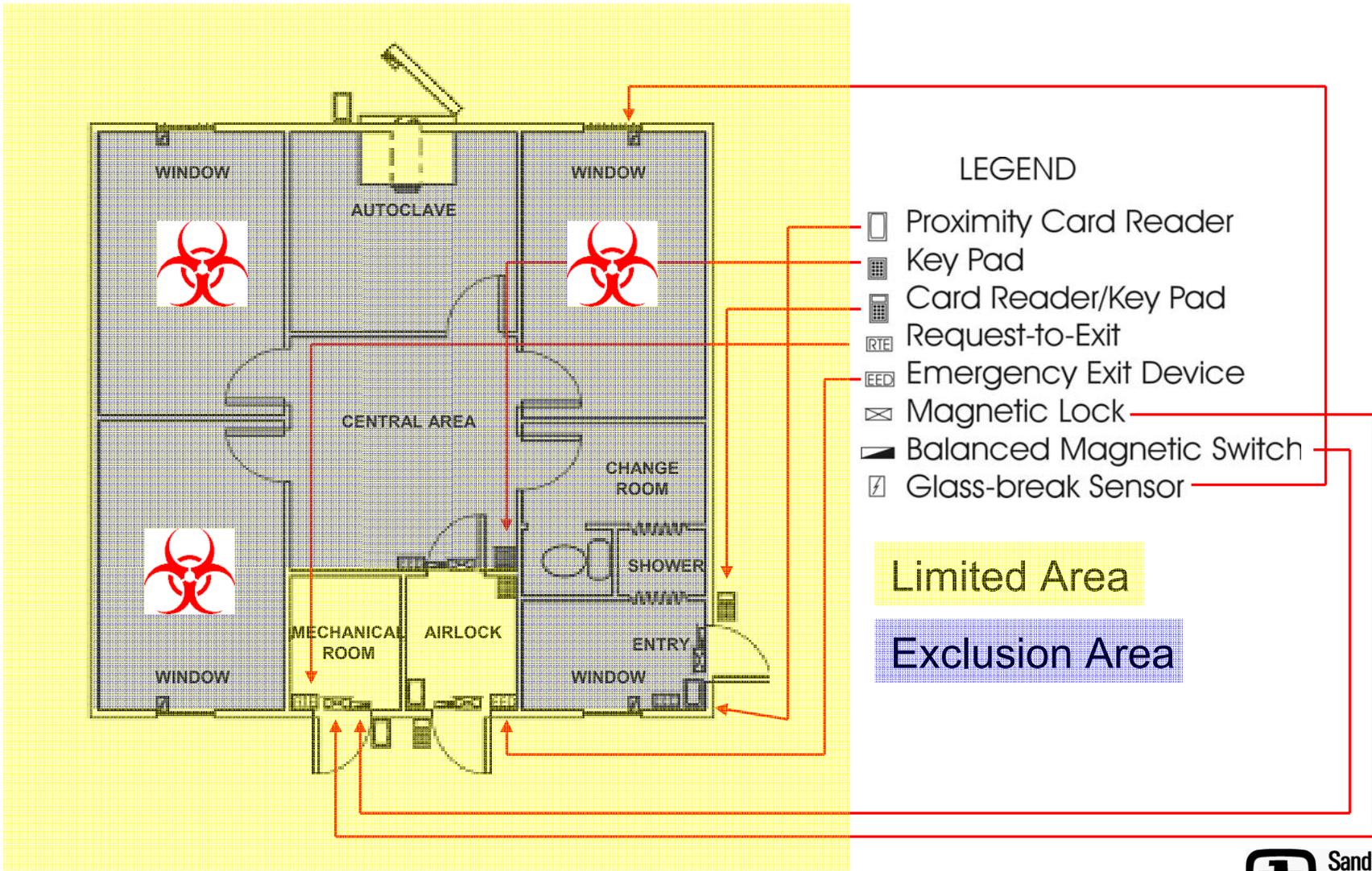
Access Control

- Ensures only authorized individuals are allowed entry
- Increasingly strict controls as you move toward highest risk assets
- Electronic systems record and time-stamp transactions
- Limited Areas
 - Controlled key required for access
- Exclusion Areas
 - Controlled key and unique knowledge required for access





Example Laboratory Building





Personnel Security

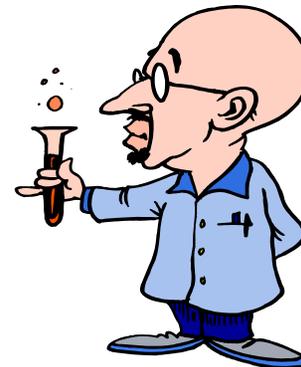
- **Personnel Screening**
 - Review and verify personal information
 - Administer personality questionnaires
 - Conduct comprehensive background investigations
- **Badges**
- **Visitor Control**
- **Training**





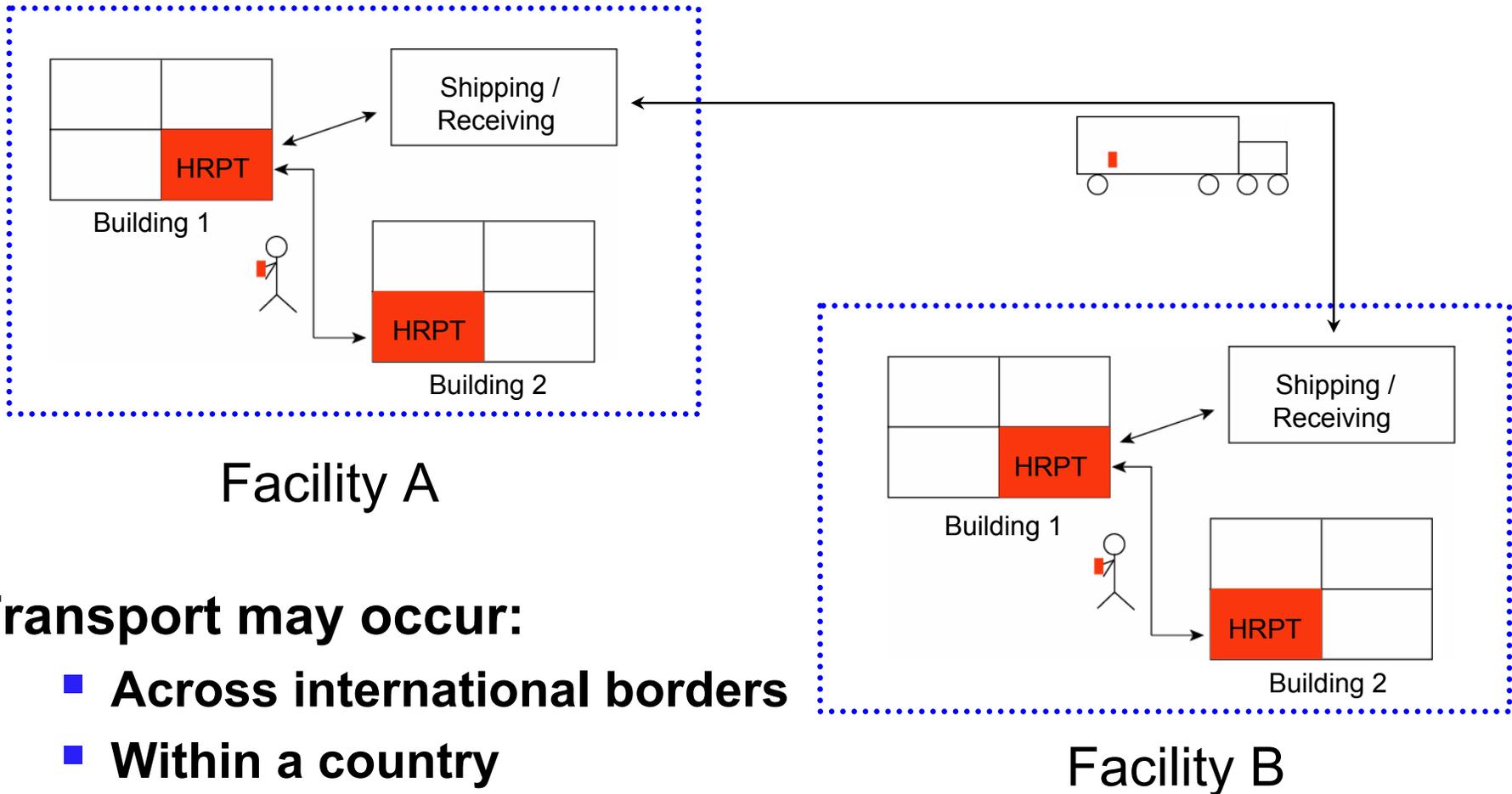
Material Control and Accountability

- **Documentation:**
 - Agent name and description
 - Quantity
 - Based on containers or other “units” NOT the number of microbes
 - Location
- **Control:**
 - Physical, personnel, information, and transfer security
 - Biosafety/Biocontainment
 - Recordkeeping
- **Responsibility:**
 - Accountable individual





Transport Security



Facility A

Facility B

Transport may occur:

- **Across international borders**
- **Within a country**
- **Within a facility or building**



Chain of Custody

- **Keep a running record of each individual who has possession of the biological material en route**
- **Confirm receipt of biological material at destination**
- **Documentation includes:**
 - **Description of material being moved**
 - **Contact information for a responsible person**
 - **Date and time of each change in custody**
 - **Record of any individual who assumes custody on behalf of someone else**



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**
- **Types of sensitive information:**
 - **Security of dangerous pathogens and toxins**
 - **Risk assessments**
 - **Security system design**
 - **Access authorizations**
 - **Personnel records**
 - **Financial records**





Conclusions

- **Necessary to take steps to reduce the likelihood that dangerous pathogens and toxins could be stolen from a legitimate bioscience facility**
- **Collaboration between security system designers and scientific experts necessary for effective risk assessment and security system design**
- **User input is required to avoid operational impacts and conflicts with biosafety**
- **Bio-lab security should integrate physical, personnel, information, material and transfer security systems**

