Risk Assessment

International Biological Threat Reduction Department
Sandia National Laboratories
October 15, 2006

Managing a Laboratory Biosecurity Program
ABSA pre-conference course

www.biosecurity.sandia.gov

SAND No. 2005-7039C
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.

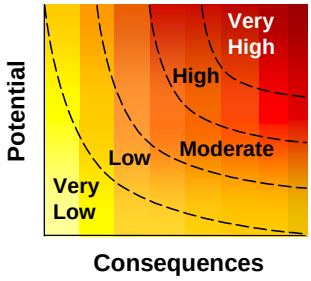
Risk

- **Is a function of the likelihood an adverse event will occur**
- **Laboratory work with pathogens will always involve some level of safety and security risk**
  - **Distinguish between "acceptable" and "unacceptable" risks**
  - **Cannot protect against every conceivable adverse event**
- **Resources for risk mitigation are not infinite**
  - **Existing resources should be used efficiently**

2

Biosecurity and Biosafety Based on Risk Management

- Most biological materials occur in nature and can be isolated from nature
- Critical not to compromise legitimate bioscience operations
  - Systems should be designed to address unique situations
- Management must distinguish between "acceptable" and "unacceptable" risks
  - Ensure that protection and the cost is proportional to the risk

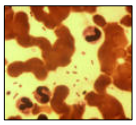


- Protect against unacceptable risk scenarios
- Develop incident response plans for acceptable risk scenarios

3

Challenges to Securing Biological Agents

- Dual-use characteristics
  - Valuable for legitimate, defensive, and peaceful commercial, medical, and research applications
    - Possession does not imply intent
- Nature of the material
  - Living and self-replicating organisms
  - Cannot be reliably quantified
    - Cannot keep an accurate inventory
  - Used in very small quantities
    - Cannot visually discern whether material is missing
  - Exist in many different process streams in facilities
    - Decentralization makes restricting access to authorized individuals more difficult
  - Contained biological samples are virtually undetectable
    - Cannot use sensors to alert unauthorized removal
- Laboratory culture
  - Biological research communities not accustomed to operating in a security conscious environment



Yersinia pestis

4

International
BIOLOGICAL THREAT REDUCTION

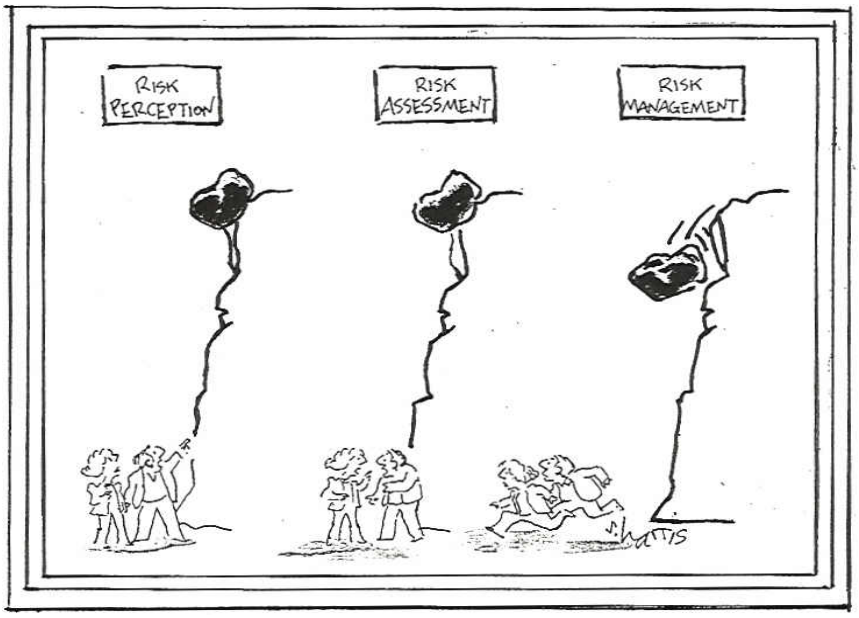
Biosecurity Cost-Benefit Considerations

- Bioscience facilities are not unique repositories
  - Most agents can be isolated from nature
  - Many similar collections of agents exist worldwide
- Relatively few agents can be easily grown, processed, weaponized, and successfully deployed while maintaining virulence/toxicity
  - Very few agents used as a weapon could cause mass human, animal, or plant casualties
- Need a methodology to make informed decisions about how to design an effective and efficient biosecurity system

FMD outbreak, U.K.

5

International
BIOLOGICAL THREAT REDUCTION



6

International BIOLOGICAL THREAT REDUCTION

Risk Perception in Laboratories

Biosafety risks: laboratory-acquired infections

- History of lab-acquired infections
  - Often attributed to carelessness or poor technique
  - Relatively few cases can be attributed to direct accident (mouth pipetting and sharps injuries)
  - Exposure to airborne pathogens generally presumed to be most plausible cause
  - Brucellosis is most common
- Sporadic infections in community as a result
  - 1973 and 1978—England had 3 secondary cases of smallpox
  - 1950—2 cases of Q fever in household of scientist
  - 1990—1 documented case of Monkey B virus from animal handler to wife
  - SARS—including 3 generations (9 cases)

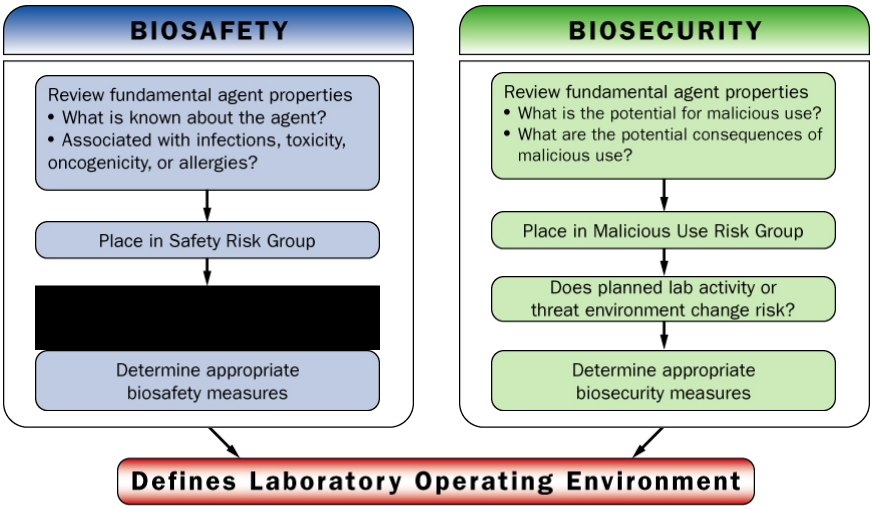
Biosecurity risks: laboratories as sources of material for malicious use

- Bioterrorism has emerged as a threat to international security
  - 1984 Rajneeshee religious cult attacks
  - 1990s Aum Shinrikyo attempts
  - 2001 Anthrax attacks in the US
- Examples of illicit acquisition
  - 1990s—Aum Shinrikyo ordered *Clostridium botulinum* from a pharmaceutical company
  - 1995—Larry Wayne Harris, a white-supremacist, ordered 3 vials of *Yersinia pestis* from the ATCC
  - 1995—Laboratory technician Diane Thompson removed *Shigella dysenteriae* Type 2 from hospital's collection and infected co-workers

7

International BIOLOGICAL THREAT REDUCTION

Risk Assessment: Integrated Biosafety and Biosecurity



8

International BIOLOGICAL THREAT REDUCTION

Risk Assessment

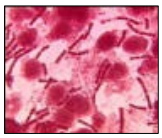
- Enables the professional (e.g. biosafety officer, responsible official) to:
  - Become familiar with the proposed work activities (procedures, equipment, personnel)
  - Be a knowledgeable and credible partner with the investigator to develop a safe and secure environment for the work
- Review all activities associated with infectious materials
  - Proposed work activities
  - Personnel
  - Storage
  - Transfer and transport
  - Destruction

9

International BIOLOGICAL THREAT REDUCTION

Biosecurity Risk Assessment

1. Evaluate assets (agent assessment)
2. Evaluate lab activity
3. Evaluate threat environment



10

Biosecurity Risk Assessment: Malicious Use Risk Group Evaluation

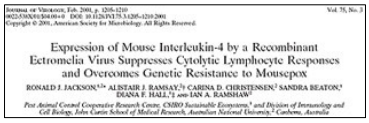
- **Assess value of the agents from an adversary's perspective**
  - **Consequences**
    - **Population**
      - Transmissibility
      - Mortality
      - Morbidity
    - **Economic**
    - **Psychological**
  - **Weaponization potential**
    - **Acquisition**
      - Natural
      - Laboratory
      - Synthetic biology
    - **Production**
      - R&D
      - Covert production
      - Ease of storage
    - **Dissemination**
      - Route of infection (e.g. aerosol, ingestion)
      - Environmental hardiness

REPORTS

Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template

Jeronimo Cello, Aniko V. Paul, Eckard Wimmer*

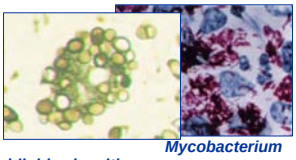
9 AUGUST 2002 VOL 297 SCIENCE www.sciencemag.org


Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox

Biosecurity Risk Assessment: Malicious Use Risk Groups

- **Nonpathogenic**
  - Malicious use would have insignificant or no consequences
- **Low**
  - Difficult to deploy, and/or
  - Malicious use would have few consequences
- **Moderate**
  - Relatively difficult to deploy, and
  - Malicious use would have localized consequences with low to moderate casualties and/or economic damage, and potentially cause pervasive anxiety
- **High**
  - Not particularly difficult to deploy, and
  - Malicious use could have national or international consequences, causing moderate to high casualties and/or economic damage, and the potential to cause mass panic and significant social disruption
- **Extreme**
  - Would normally be classified as highly attractive, except that they are not found in nature (eradicated)
  - Could include genetically engineered agents, if they would otherwise be classified as highly attractive

Malicious Use Risk Group Examples



Coccidioides immitis

Mycobacterium leprae

- **Nonpathogenic**
  - ***Bacillus cereus, Lactobacillus acidophilus*, Saccharomyces cerevisiae**
- **Low Malicious Use Risk (LMUR)**
  - ***Mycobacterium leprae***
    - **Consequences: Not highly virulent, not highly contagious, completely curable**
    - **Weaponization potential: Production is a significant challenge, not environmentally hardy**
- **Moderate Malicious Use Risk (MMUR)**
  - ***Coccidioides immitis***
    - **Consequences: Not contagious, 5-10 out of every 1000 infected develop life-threatening infection**
    - **Weaponization potential: Requires technical skills to handle safely, easy to procure virulent strain, easy to grow**

13

Malicious Use Risk Group Examples

- **High Malicious Use Risk (HMUR)**
  - ***Bacillus anthracis***
    - **Consequences: High fatality rate, not contagious, early diagnosis is difficult**
    - **Weaponization potential: History of malicious use, wide endemic area (but many less virulent strains), very stable, easy to grow and produce spores**
- **Extreme Malicious Use Risk (EMUR)**
  - **Variola major virus**
    - **Consequences: High fatality rate, contagious, few vaccinated**
    - **Weaponization potential: History of weaponization, very stable, difficult to obtain**

Variola major

Bacillus anthracis

14

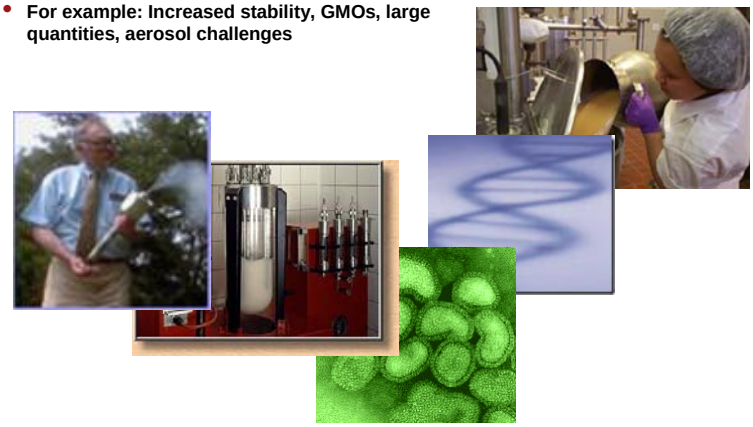
Biosecurity Risk Assessment: Other Assets at Biological Facilities

- Security Information or Systems
  - May be targeted to facilitate gaining access to dangerous biological materials
- Other Facility Assets
  - May be targeted by political extremists, disgruntled employees, etc.
  - May include:
    - High containment laboratories
    - Animals

15

Biosecurity Risk Assessment: Elements That May Modify Risk

- Consider lab experiment
  - Does planned experiment produce an agent with higher weaponization potential or higher potential consequences?
    - For example: Increased stability, GMOs, large quantities, aerosol challenges



16

Biosecurity Risk Assessment: Elements That May Modify Risk

- Adversary Classes
  - Terrorist
  - Extremist
  - Criminal
- Insiders
  - Authorized access to the facility, dangerous pathogens, and/or restricted information
  - Distinguish Insiders by level of authorized access
    - Site
    - Building
    - Asset
  - Facility management, site security, and local law enforcement interviews
- Outsiders
  - No authorized access
  - Local law enforcement, site security, and intelligence community interviews

17

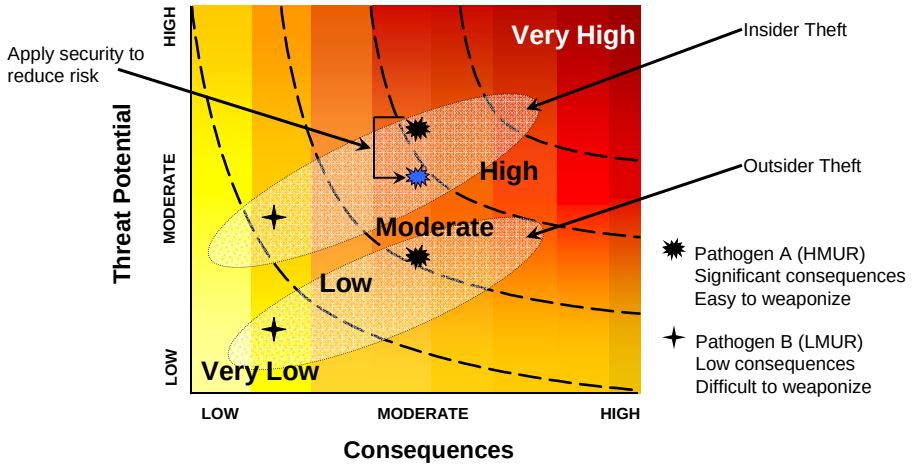
Threat Potential

Evaluate threat potential of possible adversaries:

- Motive
  - Form of potential consequences
  - Level of difficulty associated with achieving the desired result
  - Facility environment
  - Perception of being caught
- Means
  - Technical tools and knowledge
    - Overcome security system
    - Conduct BW
- Opportunity
  - Access
    - Does the adversary have routine access?
    - Are there other authorized individuals that might be present?
    - Would an unauthorized individual be noticed?

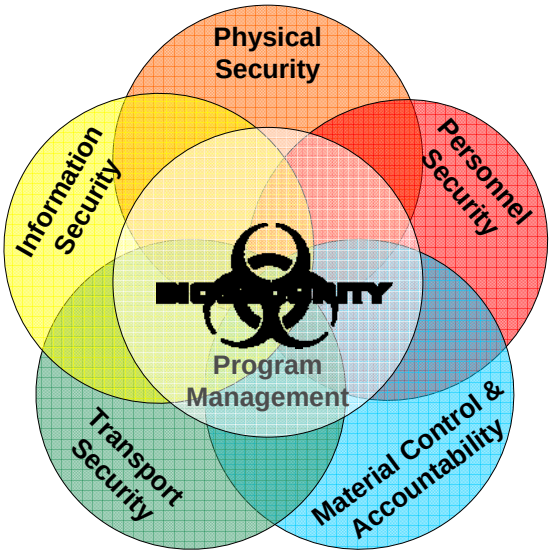
18

Biosecurity Risk: Insider vs. Outsider Threat



19

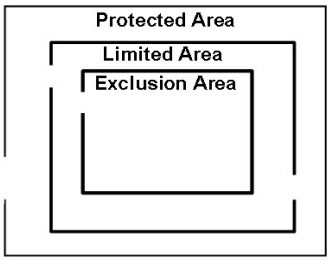
Risk Management: Implementation of Biosecurity



20

Physical Security

- Graded protection
  - Increasingly strict controls from one protection area to another
- Access control
  - Ensures only authorized individuals are allowed entry
- Intrusion detection
  - Detect unauthorized access



21

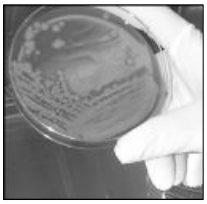
Personnel Security

- Personnel Screening
  - Conduct screening for authorized individuals
  - Increasing level of scrutiny for high risk positions
- Badges
- Visitor Control
- Training

22

Material Control and Accountability

- **Responsibility**
  - **Accountable individual**
- **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**



23

Transport Security

- **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**

24

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

25

Conclusions

- Need to integrate biosafety and biosecurity considerations into decisions about laboratory operations
- Biological facility risk assessment provides an opportunity to concentrate resources on the highest risks
  - Tiered system of protection based on risk assessment and risk management methodologies
- Parallels exist between safety and security risk assessment processes

26