



---

# *Developing and Implementing a Balanced Biosecurity System*

**Reynolds M. Salerno, Ph.D.  
Sandia National Laboratories  
May 13, 2003**

SAND 2003-1562P





# Overview

---

- **Biosafety versus Biosecurity**
- **Security Fundamentals**
- **Challenges to Securing Biological Material**
- **Biosecurity Cost-Benefit Considerations**
- **Sandia Biosecurity Methodology**
- **Achieving Biosecurity**

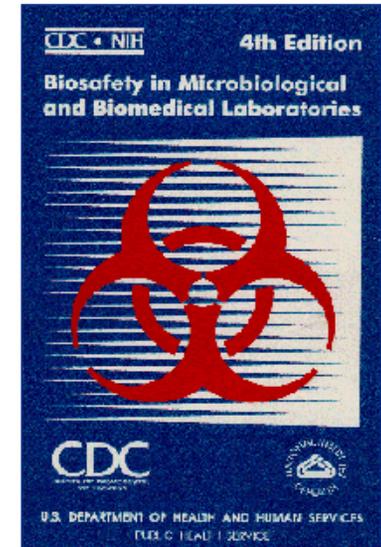
# Biosafety vs. Biosecurity

- **Biosafety**

- **Objective:** to reduce or eliminate exposure of laboratory workers or other persons and the outside environment to potentially hazardous agents involved in microbiological or biomedical facility research
- **Strategy:** implement various degrees of laboratory “containment” or safe methods of managing infectious materials in a laboratory setting

- **Biosecurity**

- **Objective:** to protect against diversion of certain high consequence pathogens and toxins, which could be used in bioterrorism or biological weapons proliferation
- **Strategy**
  - ◆ Biological risk and threat assessment
  - ◆ Site vulnerability assessment
  - ◆ System design, planning, implementation, and review
  - ◆ Biosecurity ethos





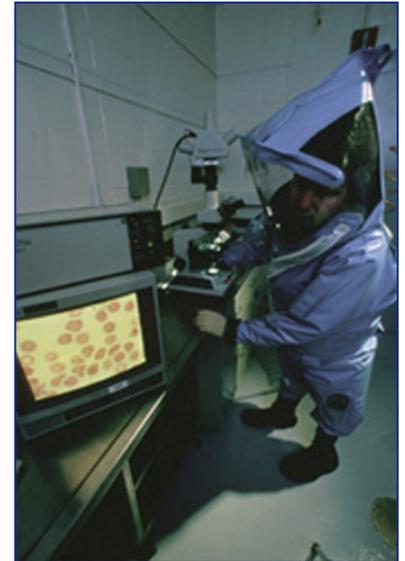
# Security Fundamentals

---

- **A security system cannot protect every asset against every conceivable threat**
- **Security resources are not infinite**
- **Security systems should be based on the asset or material that requires protection**
  - **In biological world, this requires understanding of biological agents and research, as well as probabilities and consequences of biological weapons use**
- **Security systems should be designed to address unique situations**
  - **How will security at a bioscience laboratory interact with other existing critical operating systems (e.g. biosafety)?**
- **Ideally, security should be based largely on policies and procedures, be transparent to the users, use resources efficiently, and not unnecessarily hinder normal operations**

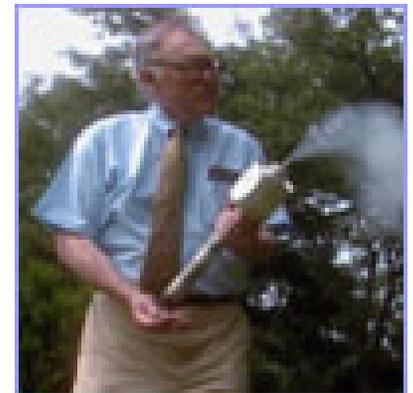
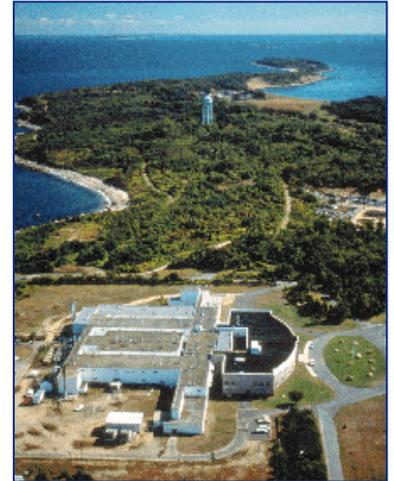
# Challenges to Securing Biological Material

- **Dual use**
  - Valuable for many legitimate, defensive, and peaceful commercial, medical, and research applications
  - Exist in many different process streams in legitimate laboratories
- **Nature of the material**
  - Living and self-replicating organisms
  - Used in very small quantities
  - Cannot be reliably quantified
  - Contained biological samples are virtually undetectable
- **Traditional bioscience ethos**
  - Biological research communities have not been accustomed to operating in a security conscious environment



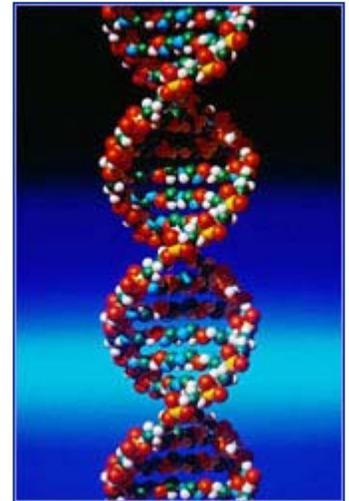
# Biosecurity Cost-Benefit Considerations

- **Bioscience research laboratories are not unique repositories**
  - Most biological agents can be isolated from nature
  - Thousands of similar collections of pathogens and toxins worldwide
- **Consequences of terrorist/state use of biological material**
  - 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 casualties
- **Need a methodology to make informed decisions about how to design an effective and efficient biosecurity system**



# Sandia Biosecurity Methodology

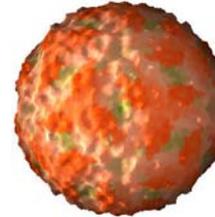
- **Qualitative risk and threat assessment is the essential first step**
  - Essential that this process include scientists, technicians, managers, security professionals, and law enforcement (counter-terrorism) experts
- **Asset identification and prioritization**
  - Consequences of diversion
  - Attractiveness to an adversary
- **Threat scenario identification and prioritization**
  - How would an adversary likely attempt to steal the target assets?
  - What would be the characteristics, motivations, and required capabilities of the adversaries who are likely to attempt to steal the target assets?
- **Risk and threat assessment establishes**
  - Security design parameters
  - Protection principles



# Asset Identification and Prioritization

- **Primary consequence**

- Loss could lead to national security event (bioterrorism)
- Certain biological agents



*FMD virus*



*Yersinia pestis*

- **Secondary consequence**

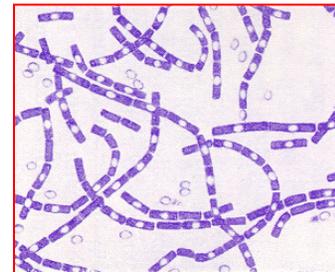
- Loss could assist in achieving a primary consequence or gaining access to a primary asset
- Certain information related to biological material



*Variola major*

- **Tertiary consequence**

- Loss could affect operations
- Certain facilities, equipment, etc.



*Bacillus anthracis*



*Fermentation vessel*

# Agent-Based Risk Assessment

- All biological agents do not need the same level of protection

- Some agents are more likely to be diverted than others

- Agent evaluation and prioritization

- Infectious disease risk

- ◆ Infectivity
- ◆ Pathogenicity
- ◆ Lethality
- ◆ Transmissibility

- Likelihood agent would be used as a weapon

- ◆ Availability
- ◆ Ease of amplification
- ◆ Ease of processing
- ◆ Environmental hardiness
- ◆ Availability of countermeasures/immunity



- Result of this assessment: High Consequence Pathogens and Toxins (HCPTs)

- Those microorganisms and their by-products that are capable, *through their use as a weapon*, of severely affecting national or international public health, safety, economy, and security

# Threat Scenario Identification

- **Adversary categories**

- Insider with authorized access
- Invited outsider(s) – visitor
- Outsider(s) with limited access and system knowledge
- Outsider(s) with no access and general knowledge
- Collusion between an insider and an outsider

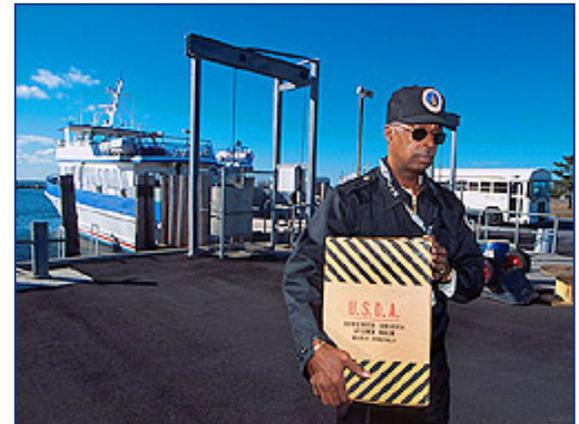


- **What will the adversaries aim to do?**

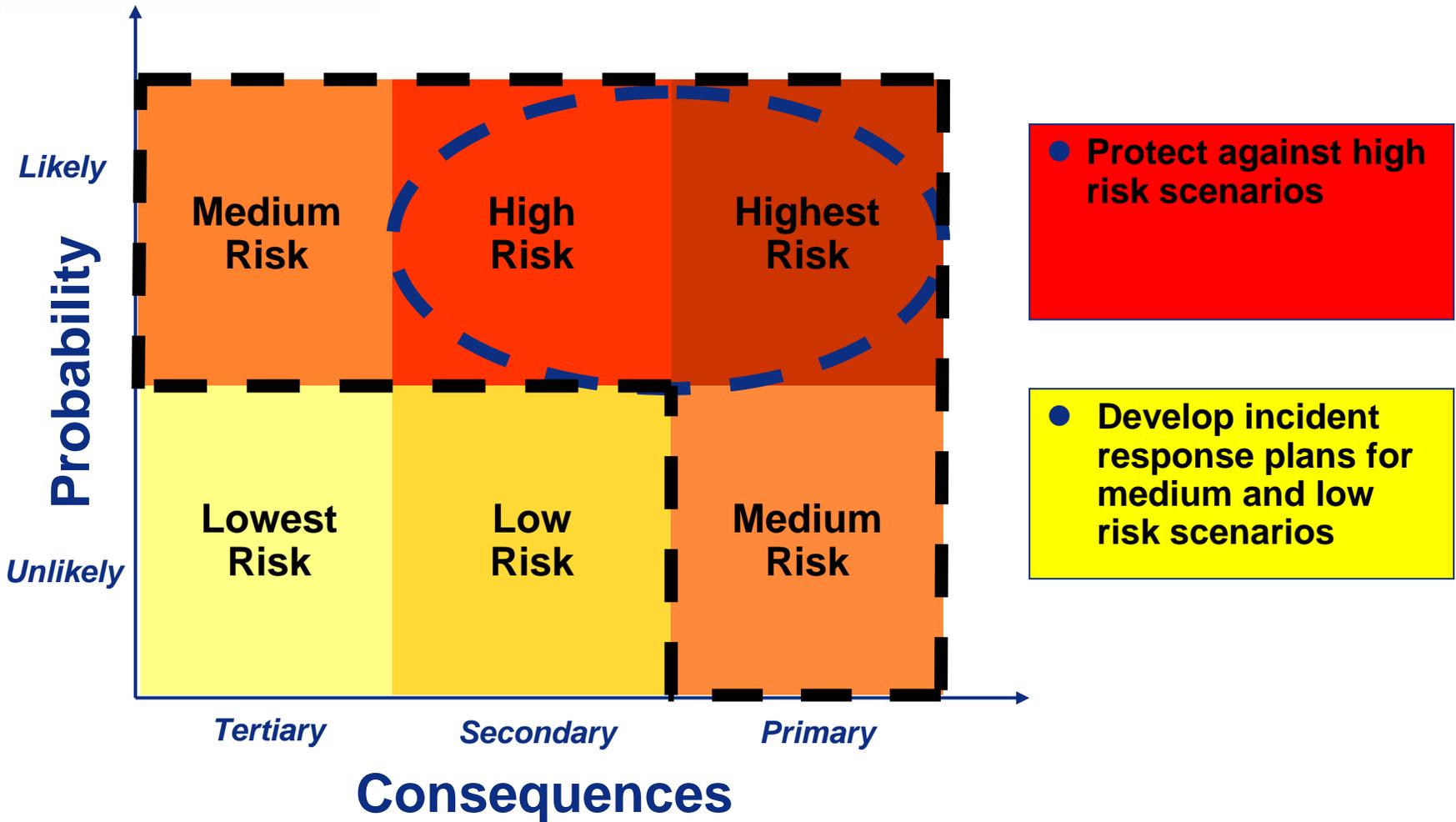
- Steal agents, steal information, disperse agents, destroy/deface facility, steal equipment, etc.

- **How will the adversaries perpetrate the event?**

- Alone or in a group?
- Armed or unarmed?
- With specific assault tools?
- Covert or overt?



# Threat Scenario Prioritization



# Results of Generic Risk & Threat Assessment

- **Highest risk scenarios**
  - Insider, visitor, or outsider with limited access attempting to steal HCPTs covertly
- **High risk scenarios**
  - Insider, visitor, or outsider with limited access attempting to steal certain HCPT-related information covertly
- **Medium risk scenarios**
  - Small outsider groups that would aim to destroy or deface the facility
- **Terrorist commando assault unlikely**
  - Agents available elsewhere
  - Overt attack using force would signal authorities to take medical countermeasures



***Selection of risk determines biosecurity design parameters***

# Achieving Biosecurity

- **Biosecurity design parameters: System objectives**
  - Describe the risk scenarios that the biosecurity system will protect against
    - ◆ Adversary type and number
    - ◆ Adversary goals: what asset is jeopardized?
  - Describe the risk scenarios that the facility will accept
    - ◆ Develop incident response plans
- **Conduct a vulnerability assessment**
  - Identifies only those vulnerabilities that would allow the defined threats to divert the defined assets
- **Design system to mitigate identified vulnerabilities**
- **Implement security system and procedures**
- **Maintain, review, and exercise security system**



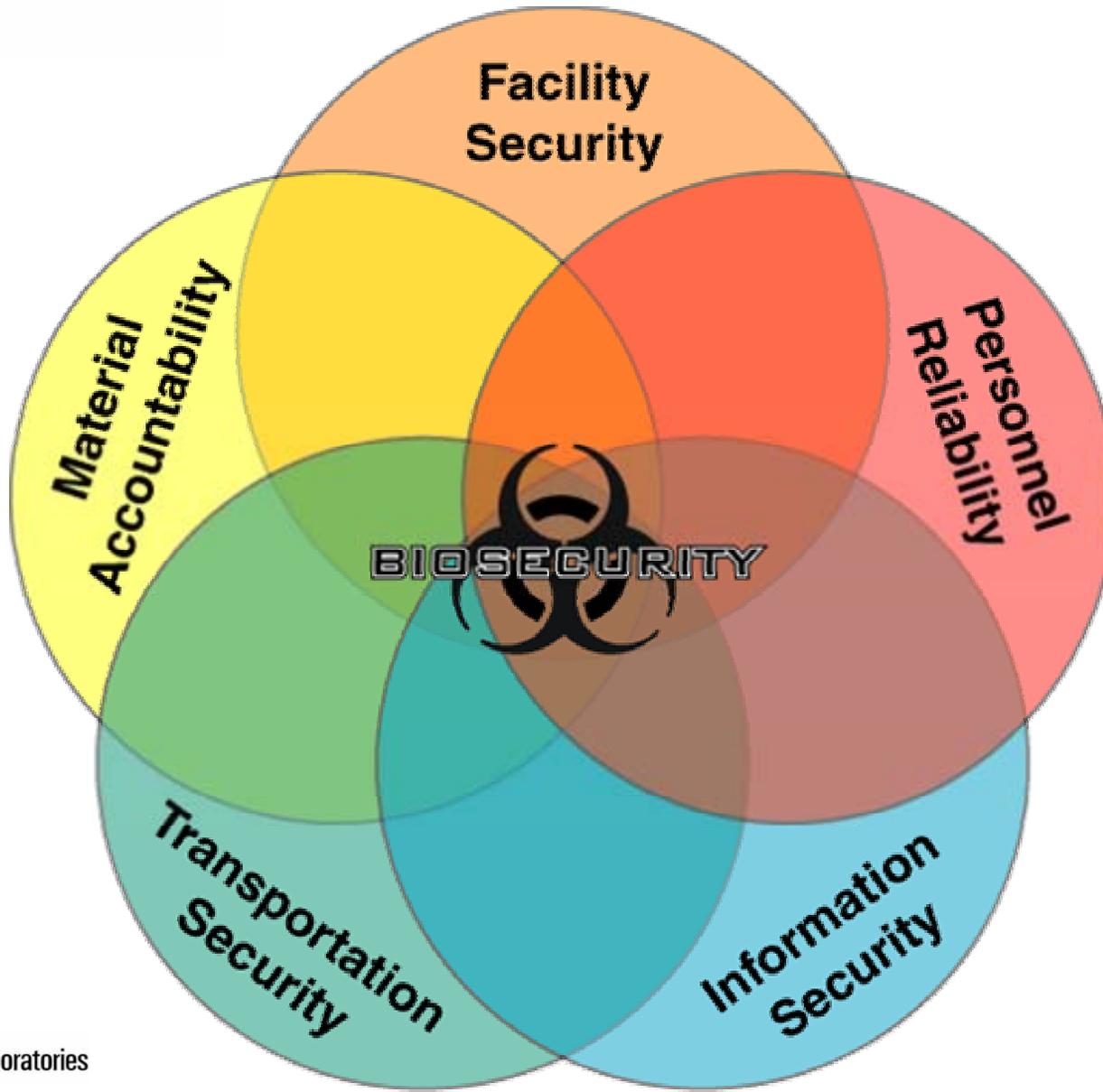
# Generic Biosecurity Protection Principles

- Develop management oversight
- Determine reliability of staff
  - Escort visitors
- Control access and detect intrusion to areas where principal assets are located
  - Physical locations
  - Cyber locations
- Establish response force to assess alarms
- Maintain accountability of materials
  - Chain-of-custody procedures



***Typically excludes substantial perimeter systems and armed guard forces***

# Effective Biosecurity Has Many Components



# Maintain, Review, & Exercise Biosecurity Plan

- Program management
- Personnel reliability
- Physical security
- Information security
- Material accountability
- Material transfer security
- Incident response plan
- Training
- Auditing



***Should describe all elements of the security system***

# Create and Sustain a Biosecurity Ethos

- **Include cross-section of facility's staff in development and implementation of biosecurity system**
  - **Conducting risk and threat assessment**
  - **Setting design parameters**
  - **Establishing protection principles**
  - **Writing a security plan**
  - **Exercising and reviewing the system**
- **Training and education**
  - **Why is security necessary?**
  - **What security are we implementing, and where?**
  - **Demonstrate that system will not unnecessarily hinder normal operations and that resources have been used as wisely as possible**
  - **Show how security systems complement existing systems (e.g. biosafety)**





# Conclusions

---

- **Necessary to take steps to reduce the likelihood that high consequence pathogens and toxins could be stolen from legitimate bioscience research laboratories**
- **Critical that these steps are designed specifically for biological materials and research so that the resulting systems will balance security and research**
- **Need to evaluate biological agents based on weaponization characteristics as well as public and agricultural health criteria**
- **Graded security approach: Agents most likely to be targeted for diversion and with worst consequences if used as a weapon should receive the highest level of protection**
- **Need to develop bioscience-specific risk and threat assessments through collaboration among experts in biological weapons, security systems, microbiology, and public and agricultural health**



## Contact Information

---

**Reynolds M. Salerno, Ph.D.**  
**Principal Member of the Technical Staff**  
**Sandia National Laboratories**  
**PO Box 5800, MS 1373**  
**Albuquerque, NM 87185**  
**USA**  
**Tel. 505-844-8971**  
**email: [rmsaler@sandia.gov](mailto:rmsaler@sandia.gov)**