



# Defining Biosecurity in Theory and Practice

**Reynolds M. Salerno, Ph.D.**  
**Sandia National Laboratories**

**Biosecurity in a Regional Context: South and East Asia**  
**April 14, 2004**



SAND No. 2004-0323P  
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.





# The Problem: Bioscience Research and International Security

- Increase in awareness of biological weapons and bioterrorist threat
- Recent realization that bioscience research facilities are potential sources of viable and virulent biological agents and toxins
- Yet the bioscience research community has not been accustomed to operating in a security conscious environment
- Research community needs specific tools to achieve a balance between
  - Adequately protecting certain biological agents and toxins
  - Not jeopardizing research on those agents and toxins





# Biosafety vs. Biosecurity

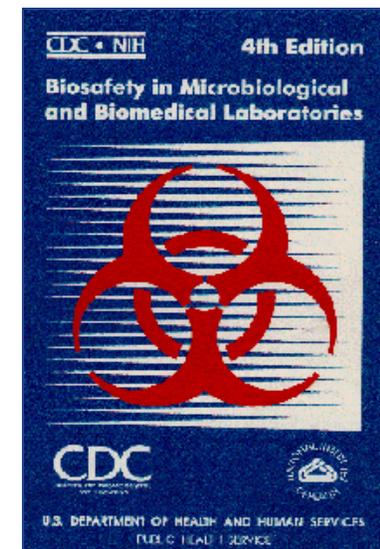
- **Biosafety**

- **Objective:** reduce or eliminate accidental exposure to or release of potentially hazardous agents
- **Strategy:** implement various degrees of laboratory “containment” or safe methods of managing infectious materials in a laboratory setting



- **Biosecurity**

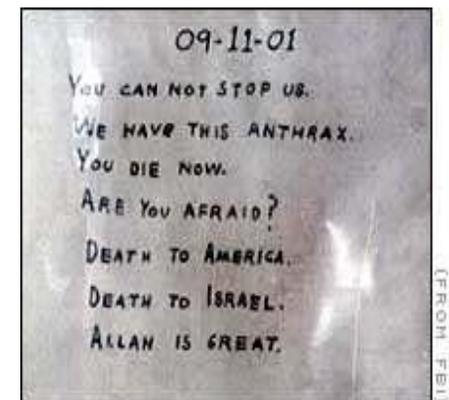
- **Objective:** protect certain biological agents and toxins against theft and sabotage
- **Strategies**
  - Practice risk management
  - Apply a graded protection approach
  - Integrate security technologies and procedures
  - Impact operations only to the level required





# Need to Secure Certain Biological Agents

- Aim of biosecurity is to mitigate biological weapons (BW) threat at the source
  - Prevent terrorists or proliferant states from acquiring biological agents from government, commercial, or academic facilities
- Biosecurity only addresses a small part of the BW threat
  - Biosecurity cannot prevent BW terrorism or proliferation, or even diversion
- Biosecurity is an important element of comprehensive BW nonproliferation program
  - Biosecurity must be augmented by other mechanisms





# General Truisms About Security

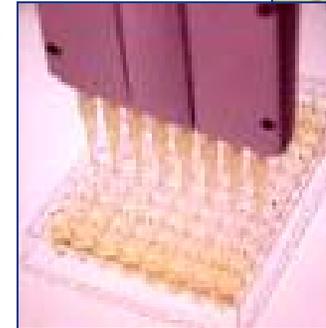
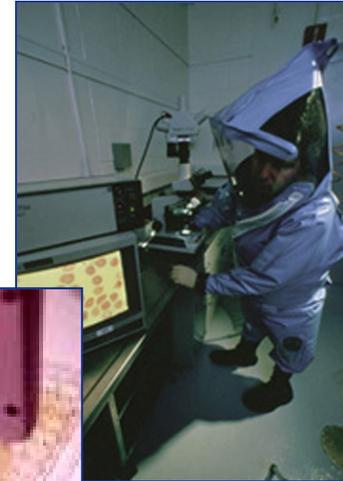
---

- **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**
- **Security systems should be designed to address unique operations**



# Challenges to Securing Biological Agents

- **Dual-use characteristics**
  - Valuable for many legitimate, defensive, and peaceful commercial, medical, and research applications
- **Nature of the material**
  - Living and self-replicating organisms
  - Used in very small quantities
  - Cannot be reliably quantified
  - Exist in many different process streams in facilities
  - Contained biological samples are virtually undetectable using standoff technologies
- **Laboratory “culture”**
  - Biological research communities not accustomed to operating in a security conscious environment

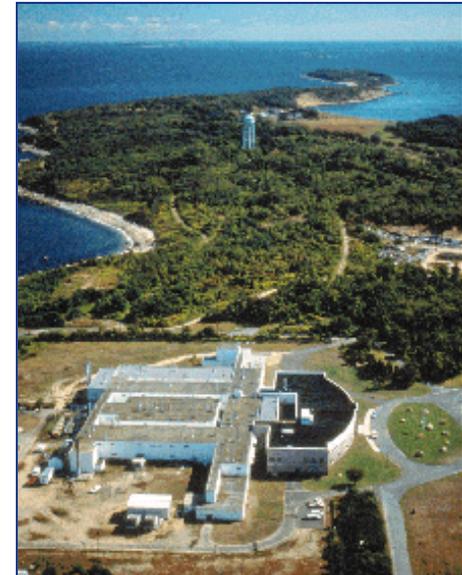




# Biosecurity Cost-Benefit Considerations

---

- **Bioscience facilities are not unique repositories**
- **Relatively few agents can be easily grown, processed, weaponized, and successfully deployed while maintaining virulence/toxicity**
- **Need a methodology to make informed decisions about how to design an effective and efficient biosecurity system**





# Opportunity to Develop Defensible and Achievable Biosecurity Guidelines

---

- **Need to appreciate that risk will always exist**
  - Distinguish between “acceptable” and “unacceptable” risks
- **Conduct an asset-based security risk assessment**
  - Ensure that the amount of protection provided to a specific asset, and the cost for that protection, is proportional to the risk of the theft or sabotage of that asset





# Biosecurity Risk Assessment

---

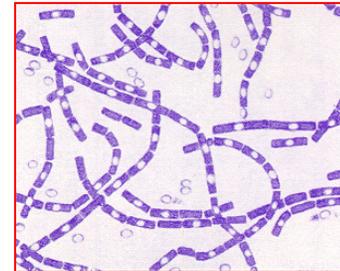
---

- 1. Define the assets of a facility or group of facilities**
- 2. Evaluate the consequences of the loss of those assets**
- 3. Prioritize the assets based on their consequences of loss**
- 4. Identify the adversaries who would attempt to steal or sabotage those assets**
- 5. Assess the motives and the methods of the adversaries**
- 6. Evaluate the risk (probability and consequences) of those potential undesirable events**

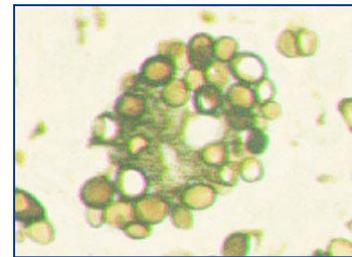


# Biological Agent Security Risk Assessment

- All pathogens and toxins do not need the same level of protection
- Agents should be placed in a Biosecurity Level based upon their risk of theft and use as a biological weapon
  - Risk is a function of both weaponization potential and consequences of use
- Weaponization potential is the ease or difficulty that an agent may be deployed as a weapon
- Consequences of use are associated with infectious disease characteristics of the agent



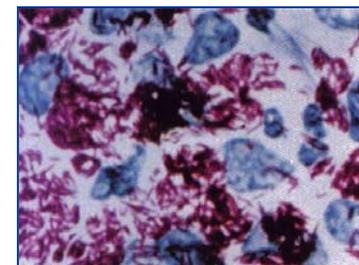
*Bacillus anthracis*



*Coccidioides immitis*



Variola major



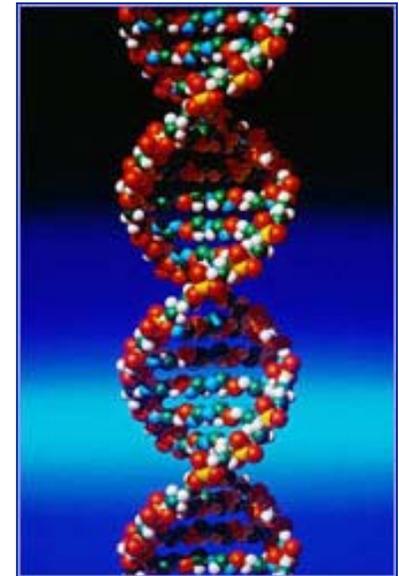
*Mycobacterium leprae*



# Biological Agent Security Risk Levels

---

- **Low Risk Pathogens and Toxins (LRPT)**
  - Relatively difficult to deploy as a weapon, and/or
  - Use as a weapon would have few consequences
- **Moderate Risk Pathogens and Toxins (MRPT)**
  - Relatively difficult to deploy as a weapon, and
  - Use as a weapon would have localized consequences with low to moderate casualties and/or economic damage
- **High Risk Pathogens and Toxins (HRPT)**
  - Not particularly difficult to deploy as a weapon, and
  - Use as a weapon could have national or international consequences, causing moderate to high casualties and/or economic damage
- **Extreme Risk Pathogens and Toxins (ERPT)**
  - Would normally be classified as HRPT, except that they are not found in nature (eradicated)
  - Could include genetically engineered agents, if they were suspected of being a HRPT





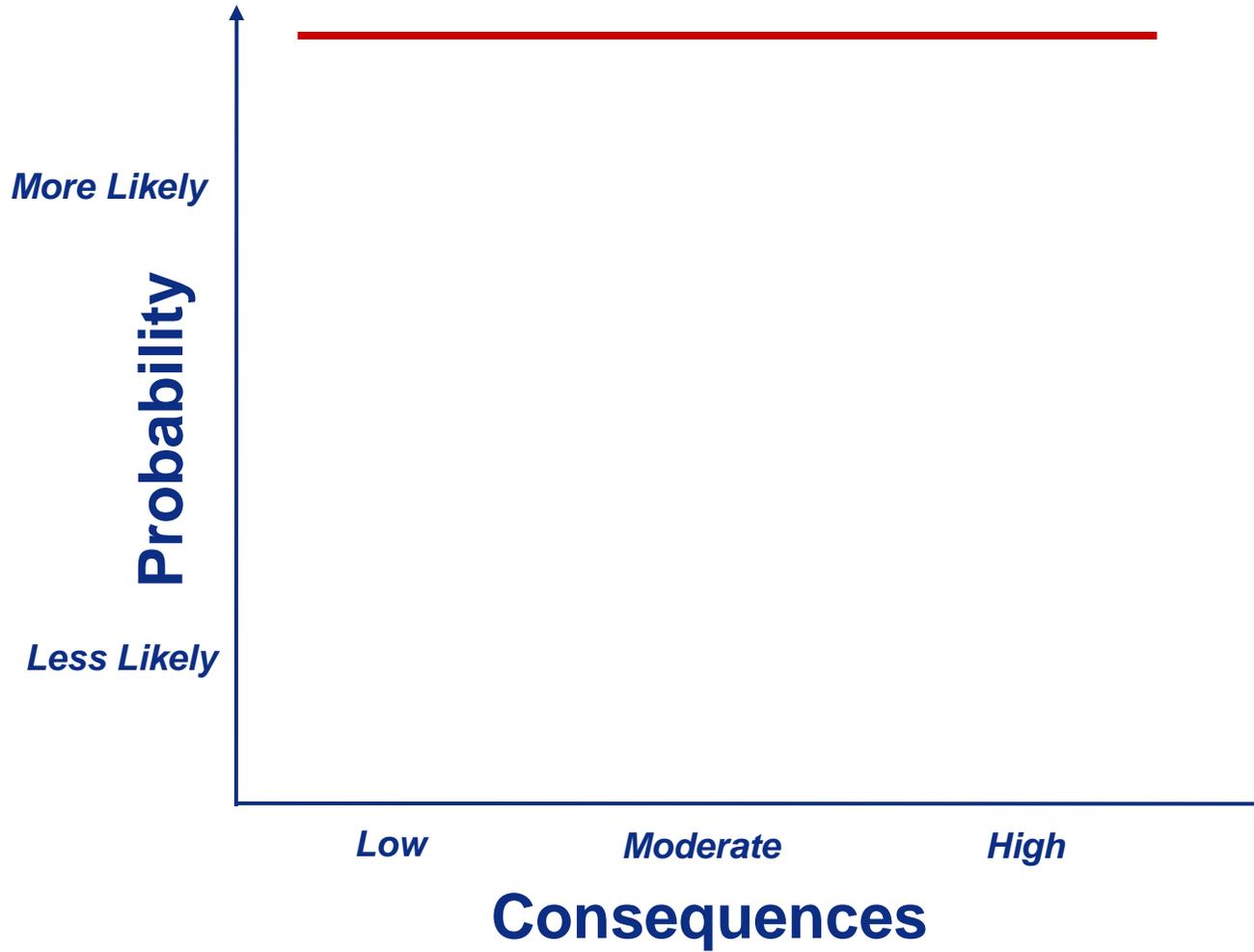
## Result of a Biosecurity-Level System

---

- **Most pathogens and toxins would likely be LRPT**
- **Most current US Select Agents would likely be MRPT**
- **Security associated with LRPT and MRPT would be achievable at reasonable cost for the broad biological research community**
  - **Rely heavily on existing biosafety measures**
- **Very few US Select Agents would be HRPT or ERPT**
- **Security for facilities that work with HRPT or ERPT would be relatively significant, but should still**
  - **Rely largely on policies and procedures**
  - **Be transparent to the users**
  - **Use resources efficiently**
  - **Not unnecessarily hinder normal operations (e.g. research, diagnostics, biosafety)**

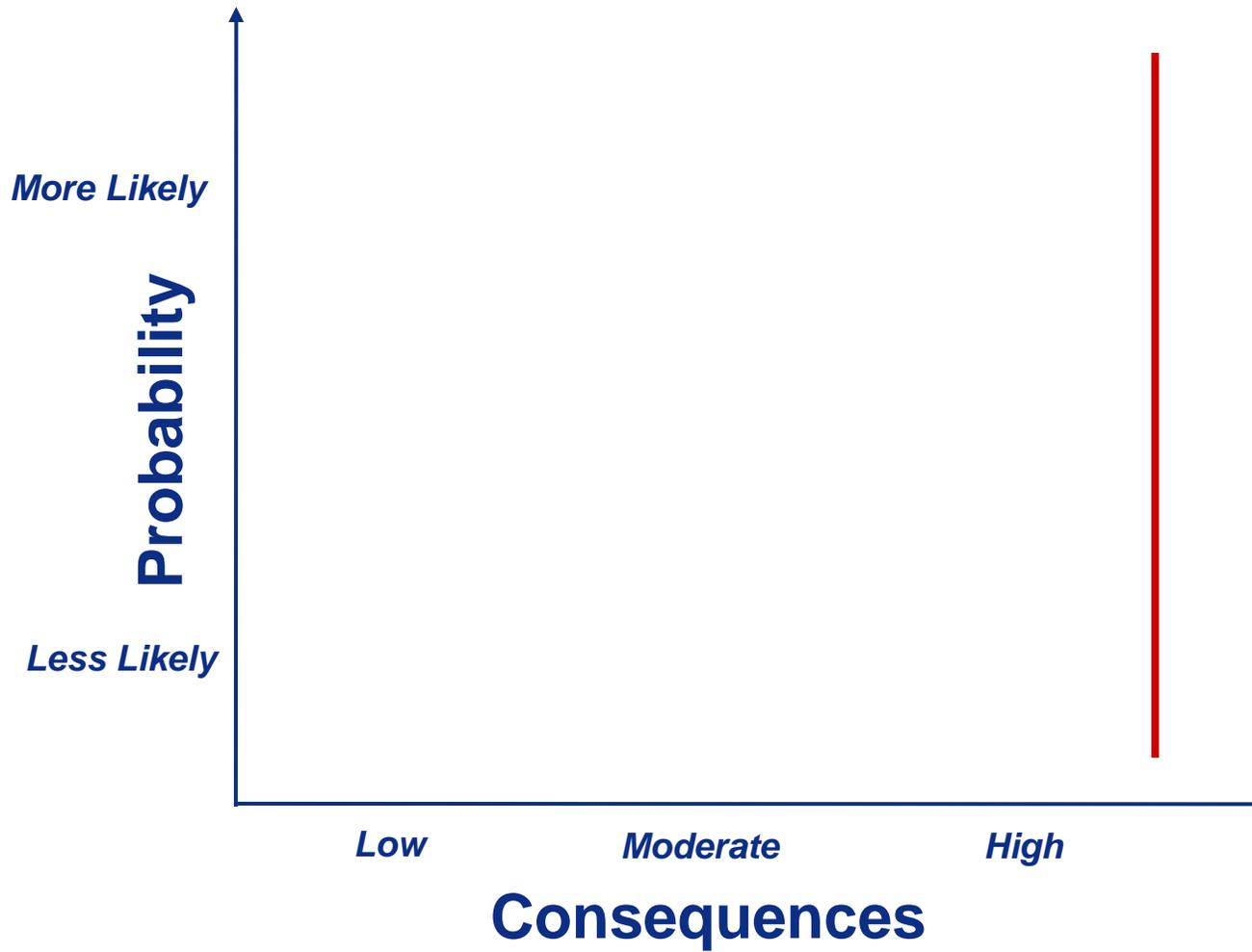


# Risk Graph



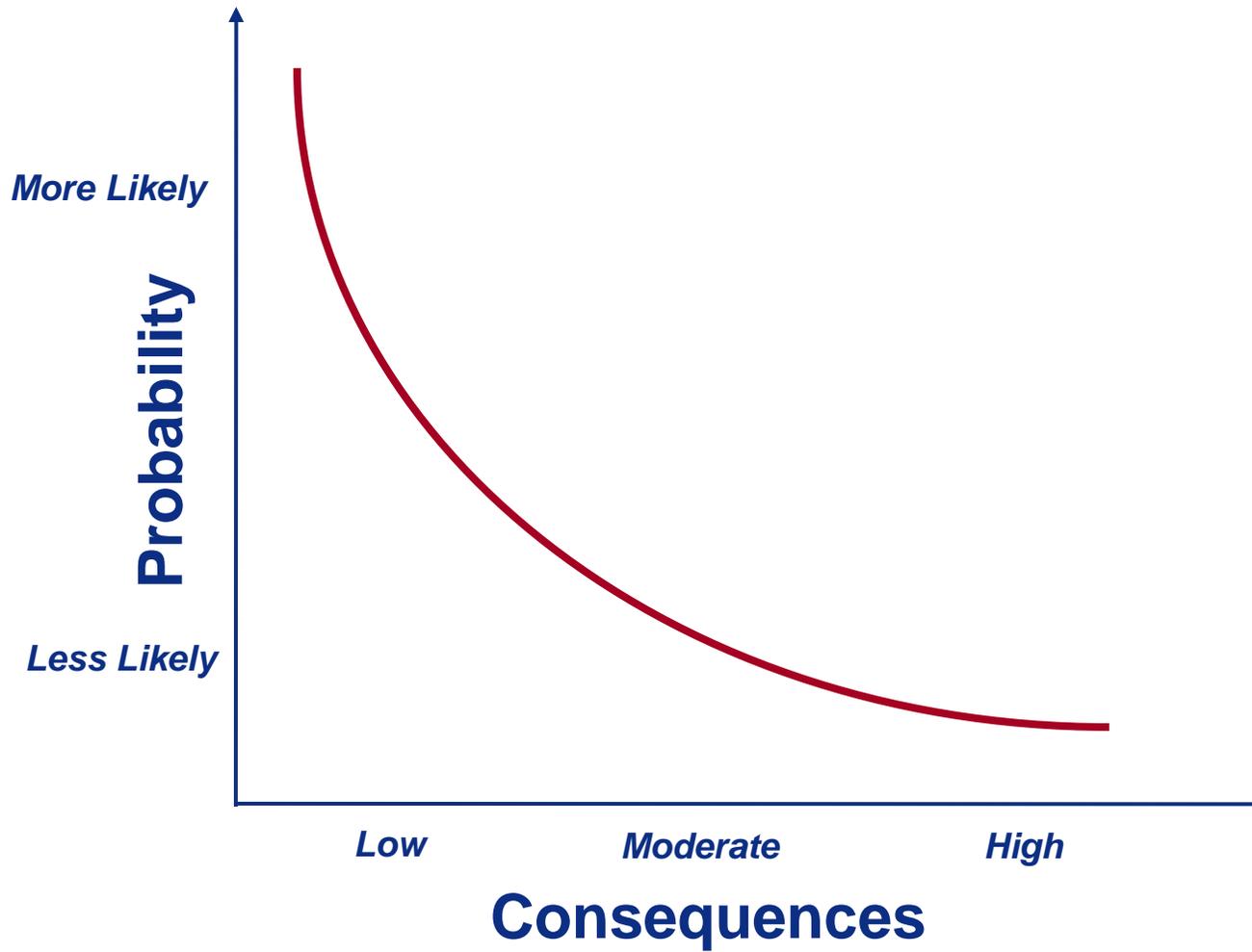


# Risk Graph



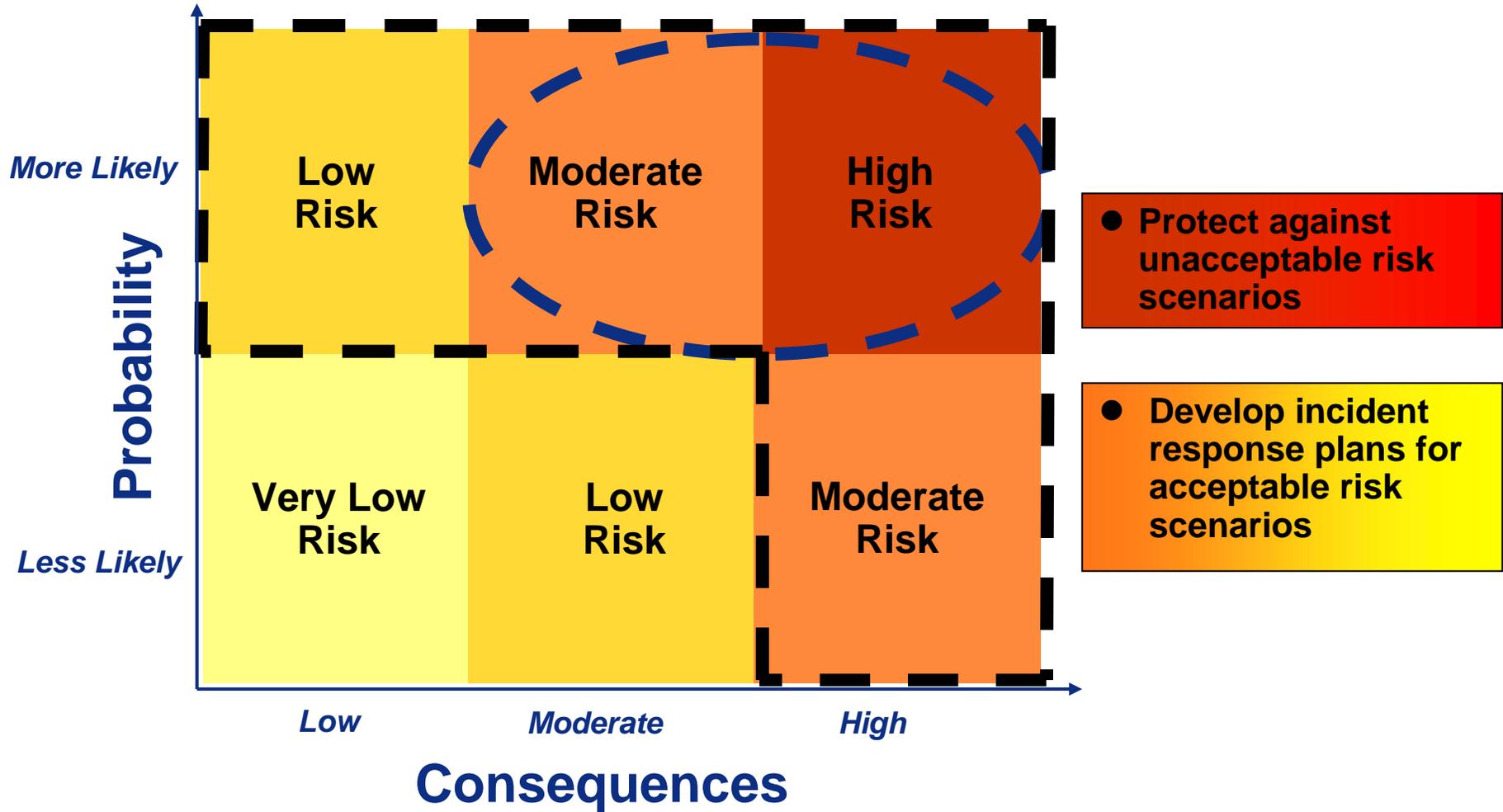


# Risk Graph





# Management Risk Decision





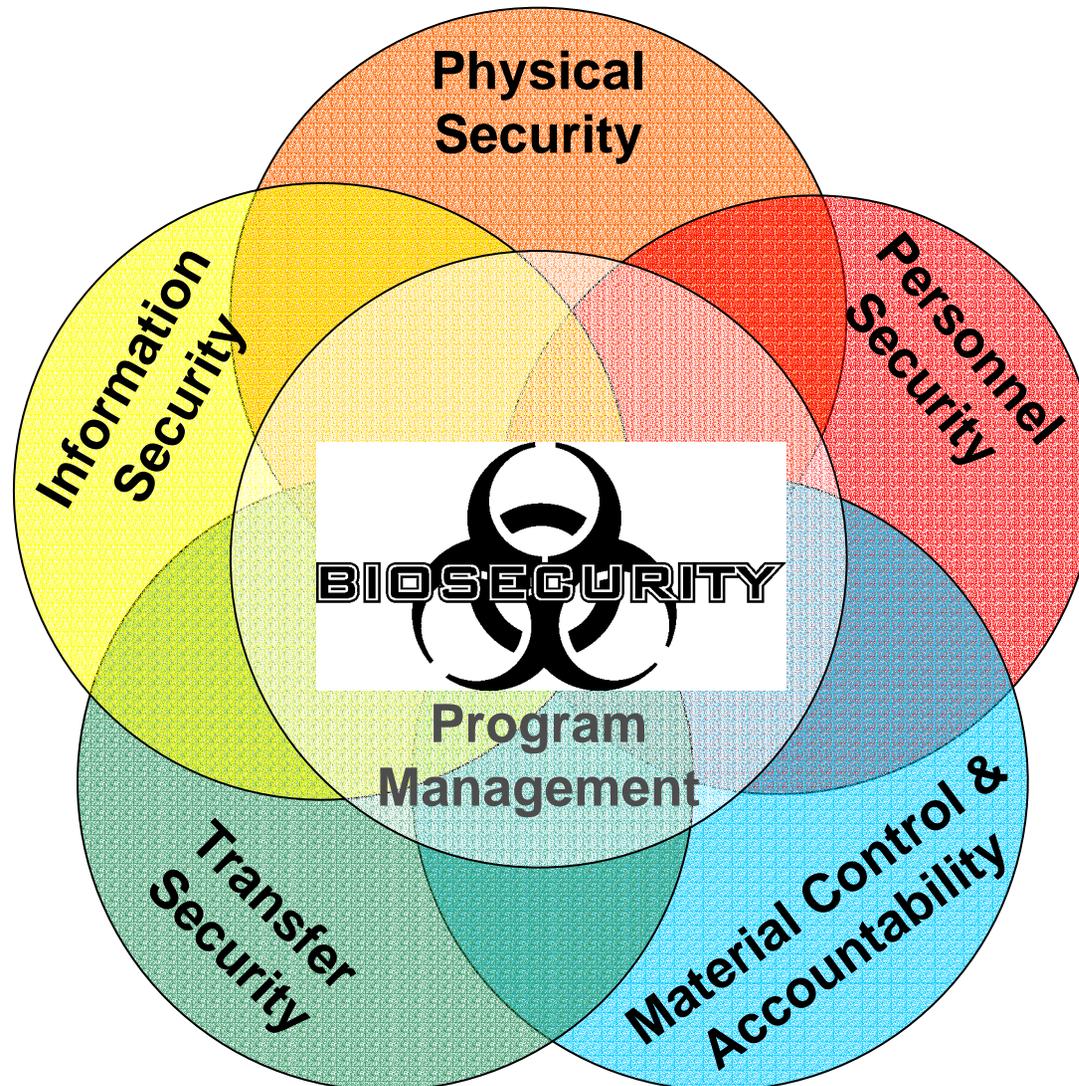
# Generic Risk Assessment Results

- **High risk scenarios**
  - Insider, visitor, or outsider with limited access attempting to steal HRPTs covertly
- **Moderate risk scenarios**
  - Insider, visitor, or outsider with limited access attempting to steal HRPT-related information covertly
- **Low 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





# Components of Biosecurity





# Summary

---

- **Necessary to take steps to reduce the likelihood that certain pathogens and toxins could be stolen from bioscience facilities**
- **Biosecurity should be applied in a graded manner, ensuring that the amount of protection provided to a specific agent is proportional to the risk of the theft or sabotage of that agent**
- **Critical that biosecurity systems are designed specifically for biological materials and research so that the resulting system will balance science and security concerns**
- **Biosecurity measures should reinforce and complement existing biosafety measures**
- **Need to involve scientific community in development of agent-based security risk assessments and biosecurity standards to build essential understanding and acceptance**



## Contact Information

---

---

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

**[www.biosecurity.sandia.gov](http://www.biosecurity.sandia.gov)**



# Personnel Reliability

- **Allow access only to those individuals who have**
  - Legitimate need to handle HRPTs
  - Appropriate training in biosafety, containment, and security procedures
  - Been registered with CDC/APHIS
- **Conduct background investigations on individuals who handle, use, or transfer select agents**
- **Establish visitor interaction procedures**
  - Screening, badging, and escorting
- **Report suspicious activity**





# Physical Security

- Implement systems to deter, detect, and respond to unauthorized attempts to gain access to HRPTs
- Establish graded protection areas with
  - Intrusion detection
  - Access controls and transaction recording
  - Alarm assessment capabilities
  - Physical barriers and delay systems
  - Law enforcement response capabilities



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



# Material Control and Accountability

---

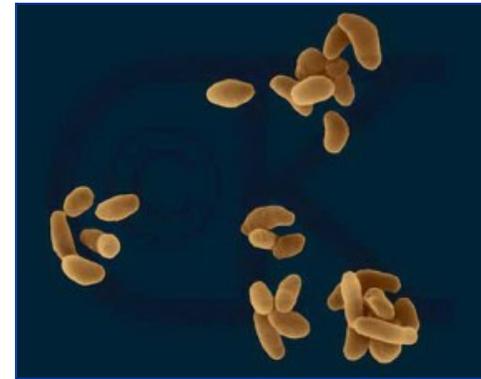
- **Develop systems to document**
  - What materials exist in a certain facility
  - Where they are located
  - Who is responsible for them
  - Who has access to them
- **Avoid trying to apply quantitative material-balance inventory accounting principles**





# Material Transfer Security

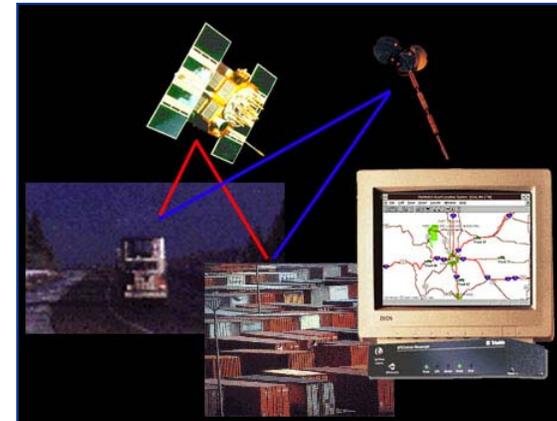
- Document, account for, and control select agents when they are moving between protected areas within a facility
- Receive authorization and monitor external transfers between registered facilities before, during, and after transport





# Information Technology Security

- **Control access to sensitive information related to HRPTs**
- **Establish policies and implement technologies for handling, using, and storing paper-based, telephonic, photographic, and electronic media**





# Program Management

---

- **Provide policy oversight and implementation of the biosecurity program**
- **Maintain documentation of**
  - Security plan
  - Incident response plan
  - Security training program
  - Self-assessment and auditing program

