



Biosecurity Methodology

Reynolds M. Salerno

International Security Programs

February 4, 2004



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

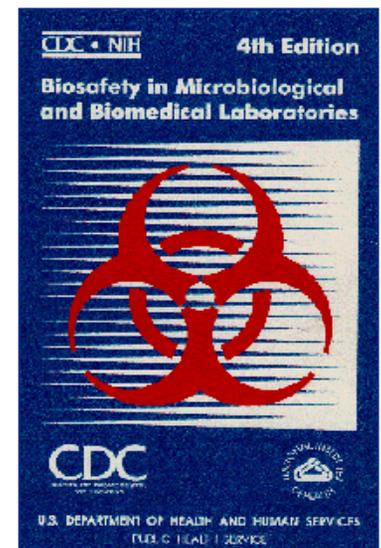
- **Biosafety**

- **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**

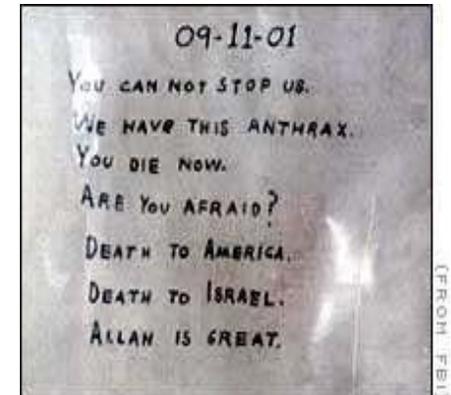
- **Objective:** protect biological agents against theft and sabotage
- **Strategies**
 - **Prioritize assets based on consequences of loss**
 - **Define unacceptable and acceptable risks by evaluating probabilities and consequences**
 - **Apply a graded protection approach**
 - **Integrate security technologies and procedures across all affected systems**
 - **Impact operations only to the level required**





Need to Secure 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





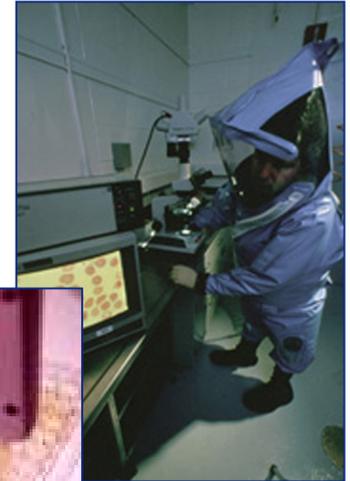
General Truisms About Security

- **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**
- **Ideally, security should**
 - **Rely largely on policies and procedures**
 - **Be transparent to the users**
 - **Use resources efficiently**
 - **Not unnecessarily hinder normal operations**



Challenges to Securing Biological Agents

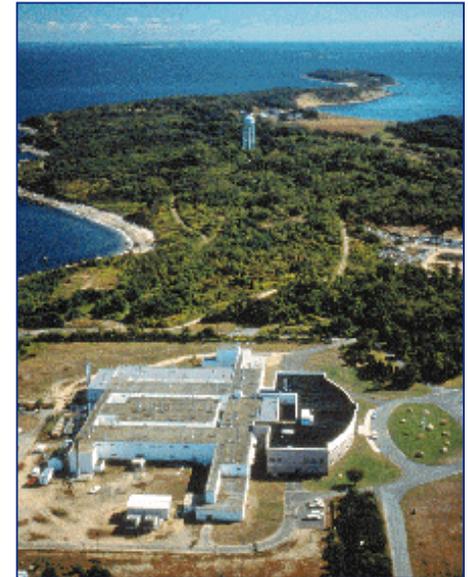
- **Dual-use characteristics**
 - Valuable for many legitimate, defensive, and peaceful commercial, medical, and research applications
- **Nature of the material**
 - Living and self-replicating organisms
 - Used in very small quantities
 - Cannot be reliably quantified
 - Exist in many different process 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**





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**



Define the Assets

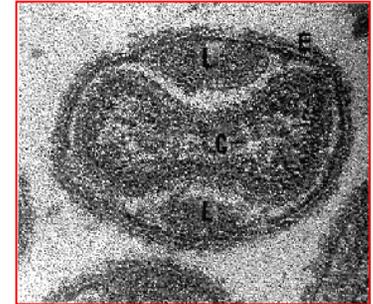
- Buildings
- Building automation equipment
- Power
- Lab equipment
- Personnel
- Biological agents and toxins
- Information





Evaluate Consequences of Loss

- **High consequences**
 - Loss of asset could directly lead to a national or international security event (e.g., high numbers of casualties, extensive economic damage)
- **Moderate consequences**
 - Loss of asset could lead to an event with consequences that do not threaten national or international security
 - Loss of asset could assist an adversary in perpetrating a high consequence event or help an adversary gain access to a high consequence asset
- **Low consequences**
 - Loss of asset could affect the local operations of an individual facility



Variola major

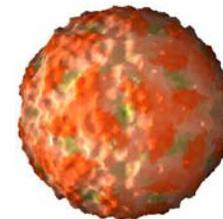


Patient's leg covered in smallpox



Prioritize Biological Agents

- All biological agents do not need same level of protection
- Prioritize agents based on the consequences of their diversion and their attractiveness to adversaries
 - Infectious disease risk
 - Likelihood agent would be used as a weapon



FMD virus

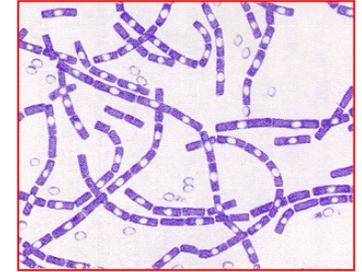


Yersinia pestis



Classify Assets from a Biosecurity Perspective

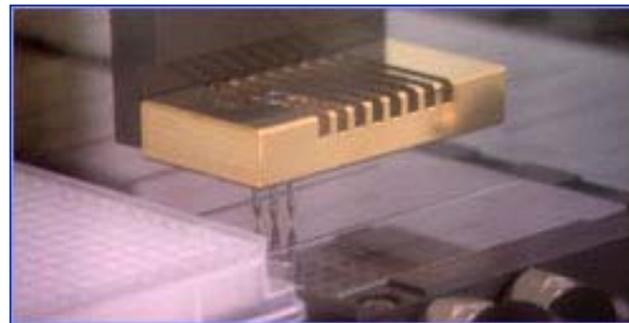
- **High**
 - High Consequence Pathogens and Toxins (HCPTs)
- **Moderate**
 - Moderate Consequence Pathogens and Toxins (MCPTs)
 - Certain information assets
- **Low**
 - Low Consequence Pathogens and Toxins (LCPTs)
 - Certain facilities, equipment, etc.



Bacillus anthracis



Castor beans





Identify Potential Adversaries

- **Insider with authorized access**
 - Principal investigator
- **Invited outsider(s)**
 - Visiting scientist
- **Outsider(s) with limited access and system knowledge**
 - Delivery personnel
- **Outsider(s) with no access but has general knowledge**
 - Political activist
- **Outsider(s) with no access and no general knowledge**
 - Psychotic
- **Collusion between an insider and an outsider**





Evaluate Motives and Methods

- **What will the adversaries aim to do?**
 - Steal, destroy, or disperse agents
 - Steal or destroy information
 - Steal or destroy equipment
 - Destroy operational systems
 - Destroy or deface facility
 - Injure or kill people
- **How will the adversaries perpetrate the event?**
 - Alone or in a group?
 - Armed or unarmed?
 - Covert or overt?

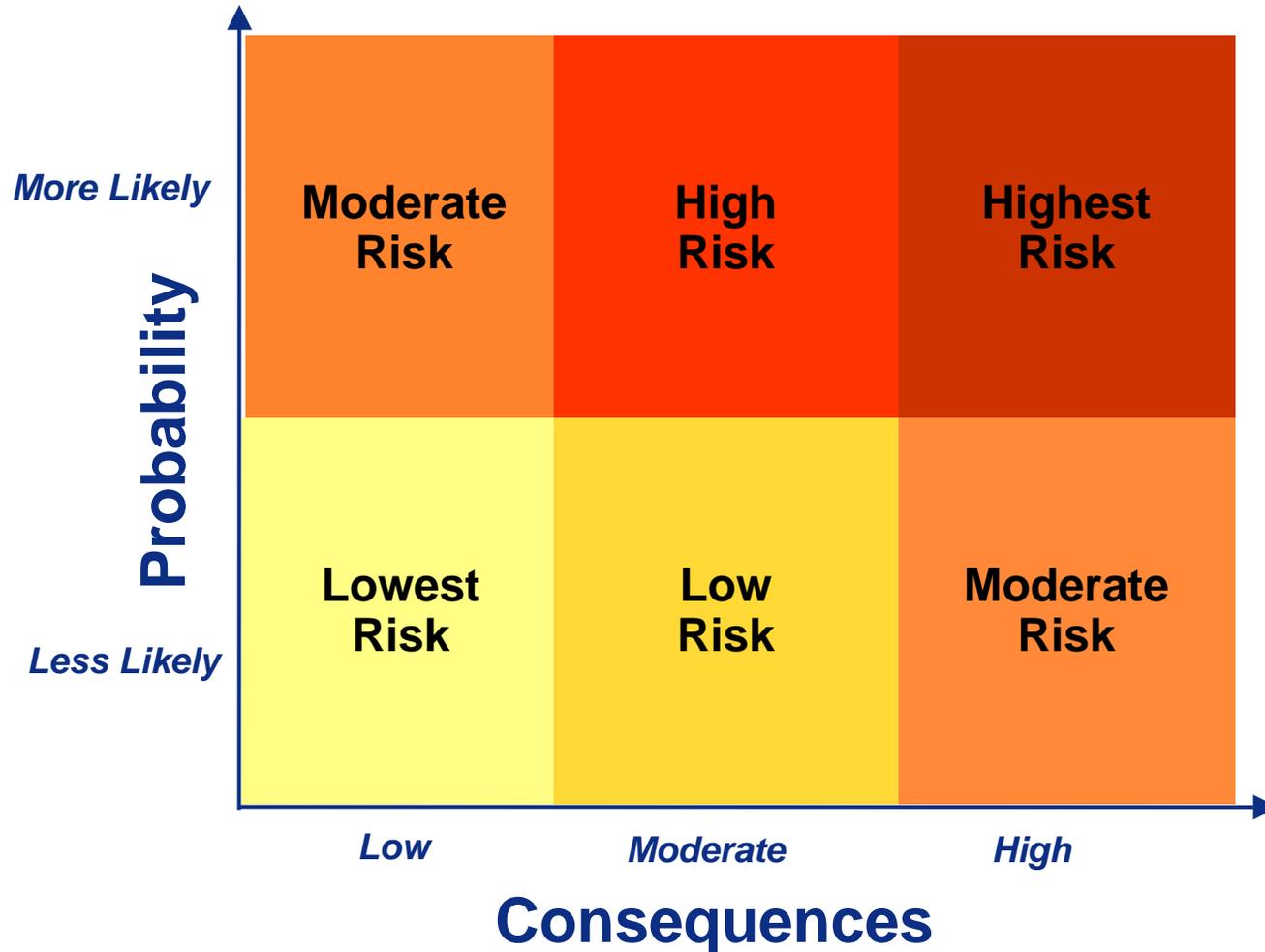


Francisella tularensis





Assess Risk of Threat Scenarios





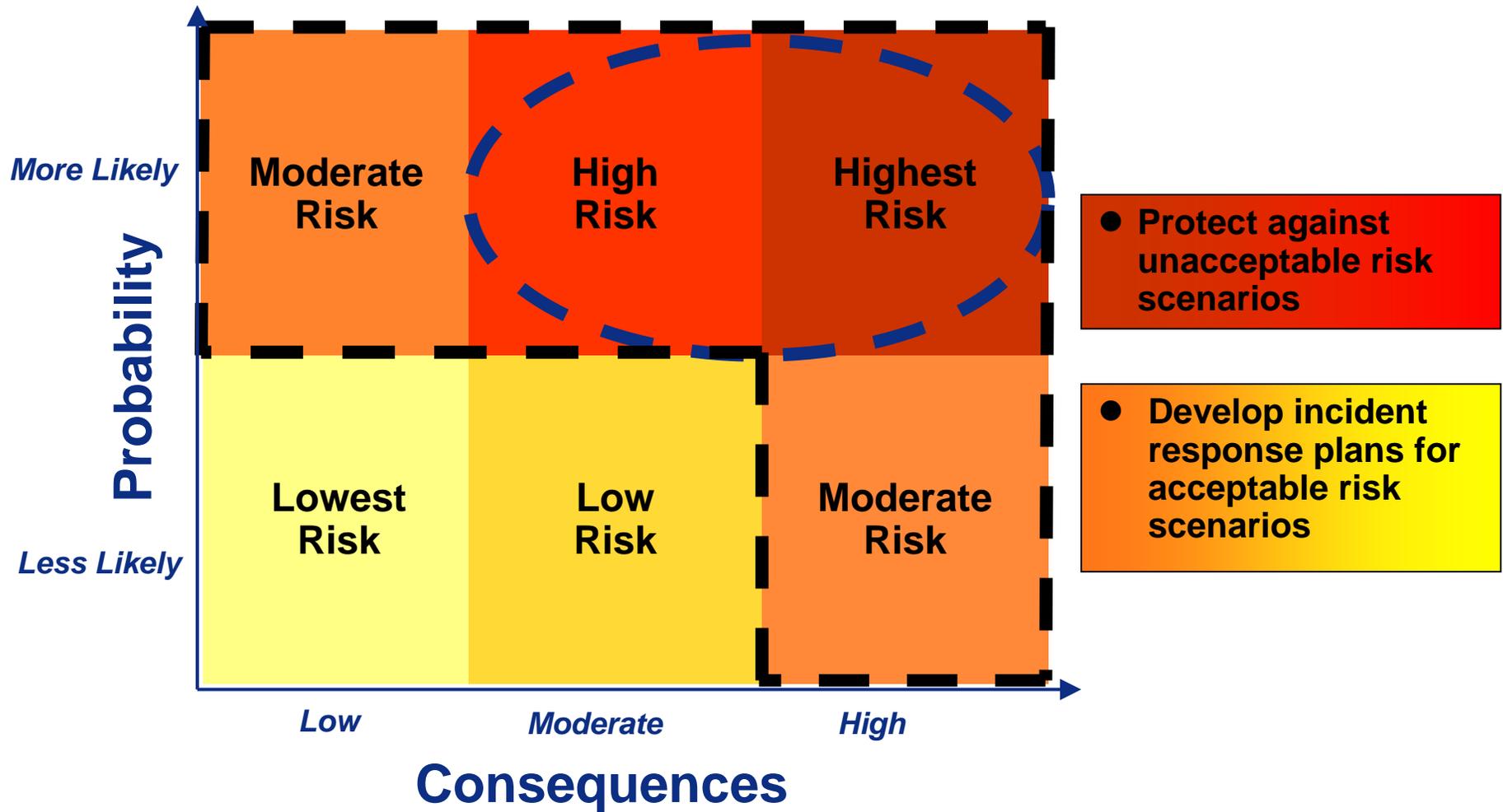
Generic Risk Assessment Results

- **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 HCPT-related information covertly
- **Moderate 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





Management Risk Decision





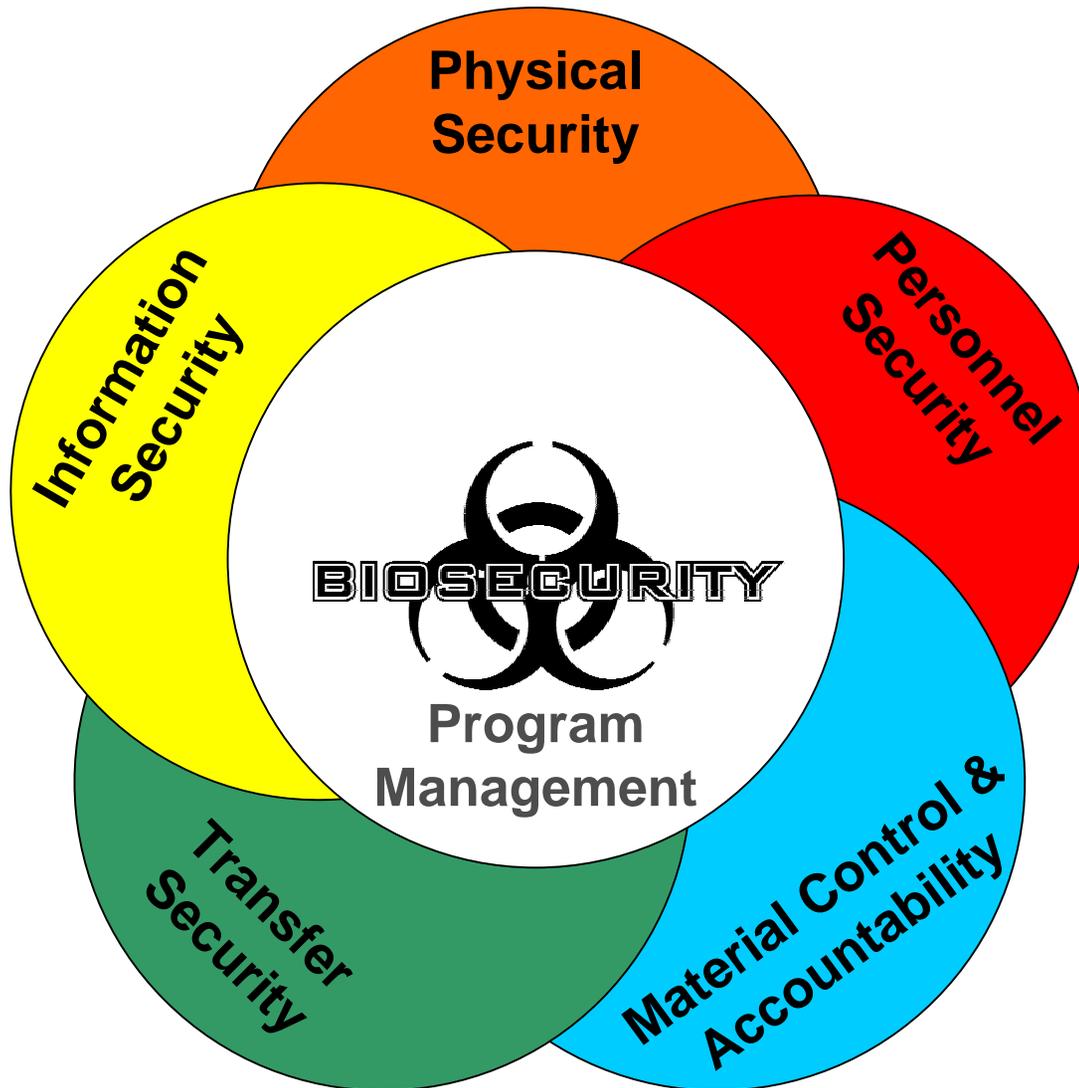
Acceptable and Unacceptable Risks

- **This critical decision reflects management's**
 - **Level of risk tolerance or risk aversion**
 - **Availability of resources**
- **Risk assessment is the essential “resource allocation” step**





Components of Biosecurity





Summary

- **Necessary to take steps to reduce the likelihood that HCPTs could be stolen from bioscience facilities**
- **Critical that these steps are designed specifically for biological materials and research so that the resulting system will balance science and security concerns**

