



A Possible Approach to Biosecurity for the BMBL

**Reynolds M. Salerno, Ph.D.
Sandia National Laboratories
April 12, 2004**



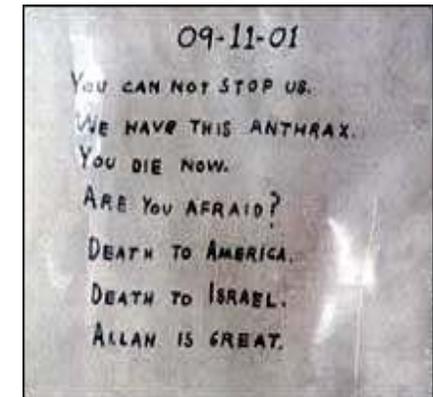
SAND No. 2004-0758P
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.





Need to Secure Certain Pathogens and Toxins

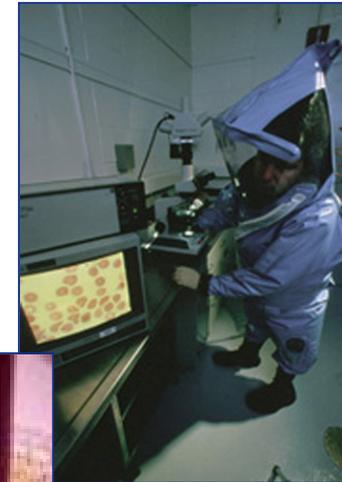
- Aim of biosecurity is to mitigate biological weapons (BW) threat at the source
 - Prevent terrorists or proliferant states from acquiring biological agents from government, commercial, or academic facilities
- Biosecurity only addresses a small part of the BW threat
 - Biosecurity cannot prevent BW terrorism or proliferation, or even diversion
 - Biosecurity should be designed to deter and detect theft or sabotage
- Research community needs specific tools to achieve a balance between
 - Adequately protecting certain pathogens and toxins
 - Not jeopardizing research on those agents and toxins





Opportunity to Develop Defensible and Achievable Biosecurity Guidelines

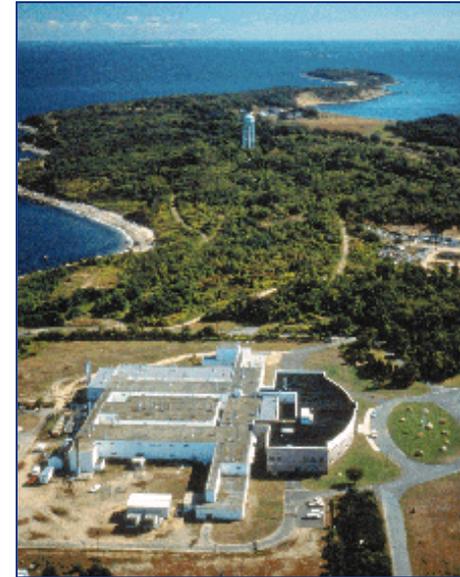
- **Need to appreciate that risk will always exist**
 - Every asset cannot be protected against every conceivable threat
 - Distinguish between “acceptable” and “unacceptable” risks
- **Employ a risk management approach**
 - Conduct an asset-based security risk assessment
 - Ensure that the amount of 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 Cost-Benefit Considerations

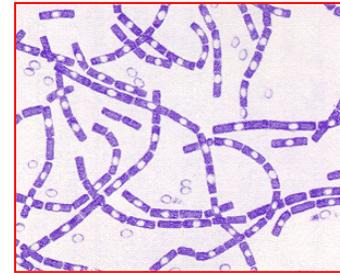
- **Biological agents are naturally occurring organisms**
- **Bioscience facilities are not unique repositories**
- **Relatively few agents can be easily grown, processed, weaponized, and successfully deployed while maintaining virulence/toxicity**
- **An asset-based risk assessment provides a mechanism for making informed decisions about how to design an effective and efficient biosecurity system**



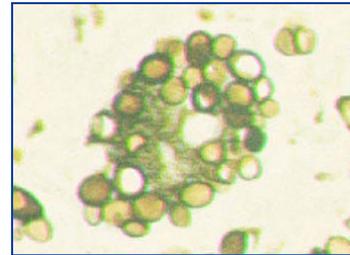


Biological Agent Security Risk Assessment

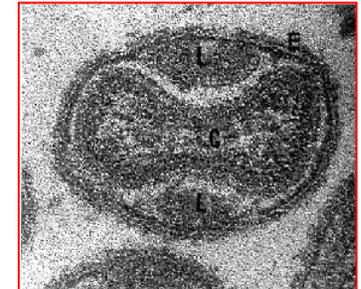
- All pathogens and toxins do not need the same level of protection
- Agents should be placed in a Biosecurity Level based upon their risk of theft and use as a biological weapon
 - Risk should be a function of both weaponization potential and consequences of use
- Weaponization potential is the ease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



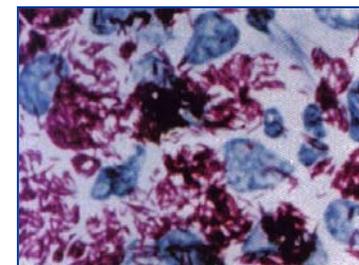
Bacillus anthracis



Coccidioides immitis



Variola major

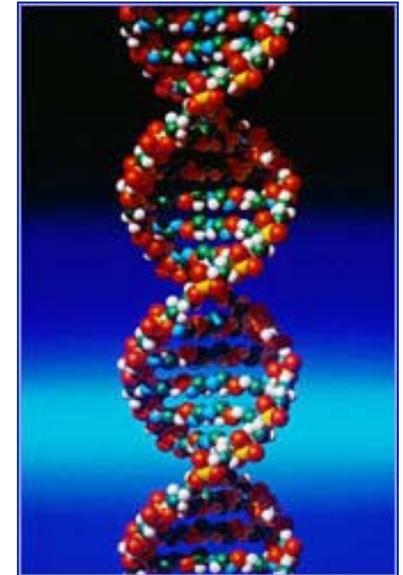


Mycobacterium leprae



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 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 largely on existing biosafety measures**
- **Very few 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)**



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

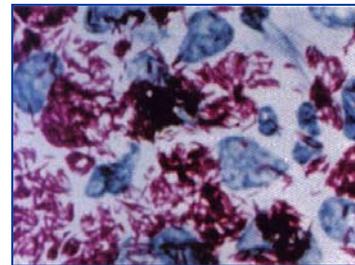
Reynolds M. Salerno, Ph.D.
Principal Member of the Technical Staff
Sandia National Laboratories
PO Box 5800, MS 1373
Albuquerque, NM 87185
Tel. 505-844-8971
email: rmsaler@sandia.gov

www.biosecurity.sandia.gov



LRPT Agent Example: *Mycobacterium leprae*

- **Consequences**
 - **Leprosy**
 - ◆ Not highly virulent, most exposed people do not develop leprosy
 - ◆ Not highly contagious
 - ◆ Completely curable – majority recover without treatment
- **Weaponization potential**
 - Production is a significant challenge
 - Not environmentally hardy
- **Conclusion: low consequences and low weaponization potential**

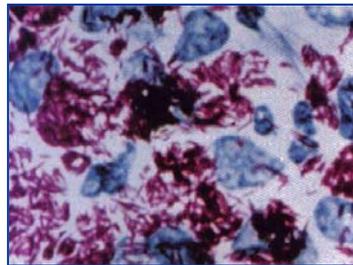


Mycobacterium leprae



Low Risk Security Level

- Doors on unattended laboratories should be locked
- Principal Investigator should be aware of work and individuals in his/her lab
- Laboratory notebooks should document the stocks and use of agents

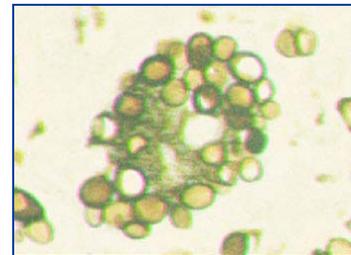


Mycobacterium leprae



MRPT Agent Example: *Coccidioides immitis*

- **Consequences**
 - **Coccidioidomycosis (Valley fever)**
 - ◆ Usually asymptomatic, 30-40% of infected become ill
 - ◆ Not contagious
 - ◆ 5-10 out of every 1000 infected develop life-threatening infection
- **Probability**
 - Requires technical skills to handle
 - Easy to procure (wide endemic area)
 - Easy to grow colonies and produce spores
- **Conclusion: low to moderate consequences and moderate weaponization potential**

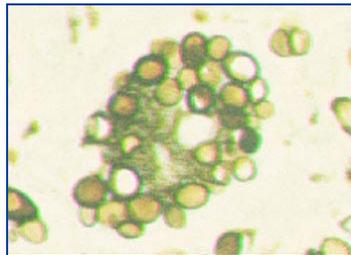


Coccidioides immitis



Moderate Risk Security Level

- **Basic access controls (e.g. controlled keys) for areas where agents are used and stored**
- **Basic personnel suitability check should be completed for all those who enter the controlled area**
- **Materials should be accounted for and inventoried in databases**

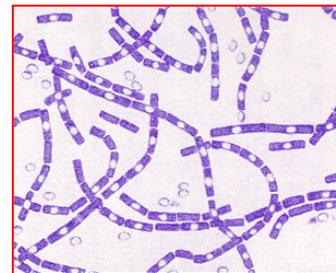


Coccidioides immitis



HRPT Agent Example: *Bacillus anthracis*

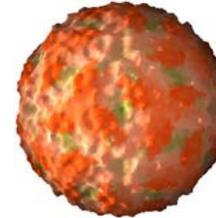
- **Consequences**
 - **Pulmonary anthrax (via aerosolized anthrax)**
 - ◆ High fatality rate
 - ◆ Not contagious, relatively high infectious dose required
 - ◆ Early diagnosis is difficult
- **Weaponization potential**
 - History of weaponization and terrorist use
 - Wide endemic area but many less virulent strains
 - Easy to grow colonies and produce spores
- **Conclusion: moderate to high consequences and relatively high weaponization potential**



Bacillus anthracis

High Risk Security Levels

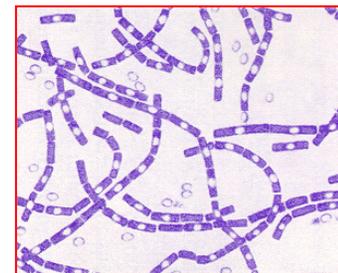
- Electronic access controls
- Personnel screening should include more comprehensive background investigations
- Accountability records should be maintained
- Material transfers should be pre-approved and require a continuous chain of custody
- Information about the security of these agents should be protected
- Biosecurity Officer should oversee the implementation of appropriate biosecurity measures



FMD virus



Yersinia pestis

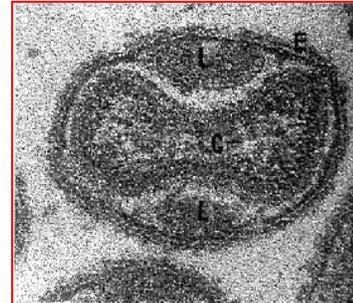


Bacillus anthracis



ERPT Agent Example: Variola major virus

- **Consequences**
 - **Smallpox**
 - ◆ High fatality rate
 - ◆ Contagious
 - ◆ Very few people vaccinated
- **Weaponization potential**
 - History of weaponization
 - Very stable in aerosol
 - Extremely difficult to obtain
- **Conclusion: high consequences and moderate weaponization potential**



Variola major

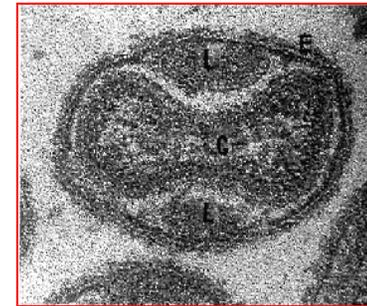


Patient's leg covered in smallpox



Extreme Risk Security Level

- Two- or three-level electronic access controls
- In-depth personnel suitability background checks
- Accountability records should be maintained
- Two authorized individuals should be required for access to repository stocks
- Material transfers should be pre-approved and require a continuous chain of custody
- Information about the security of these agents should be protected
- Local guard force should be able to respond to intrusions
- Biosecurity Officer should oversee the implementation of appropriate biosecurity measures



Variola major



Patient's leg covered in smallpox