



---

---

# Introduction to the Security of Pathogens in Laboratory Environments

**Jennifer Gaudio, Ph.D.**

**International Laboratory Biosafety and Biosecurity**

**REDI Center, Singapore**

**April 7, 2005**



SAND No. 2005-1324C  
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.





# Security System Considerations

- **Cannot protect every asset against every conceivable threat**
- **Detection of theft extremely difficult**
  - Microscopic
  - No detectable signature
  - Constantly changing quantities
- **User input necessary**
  - Minimize operational impacts
  - Integrate with biosafety systems
- **Resources are limited and must be allocated effectively**
  - Risk assessment and management





# Risk Management

---

---

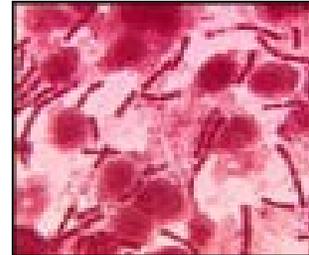
- **Establishes which assets should be protected against which threats**
  - **Assets are items that are:**
    - **Dangerous**
    - **Hard to replace**
    - **Rare**
    - **Critical to operations**
- **Ensures that the amount of protection provided to a specific asset, and the cost for that protection, is proportional to the risk of the theft or destruction of that asset**
- **Begins with a risk assessment**



# Biosecurity Risk Assessment

---

- 1. Evaluate assets**
- 2. Evaluate threat**
- 3. Evaluate risk**





# Evaluate Value of the Assets from an Adversary's Perspective

- **Biological agents**

- **Consequences**

- Lethality
- Morbidity
- Infectivity
- Transmissibility

- **Weaponization potential**

- Environmental hardiness
- Ease of processing
- Ease of distribution
- Ease of growth
- Availability
- Ability to camouflage as a natural outbreak



- **Information related to the security of dangerous biological materials could assist an adversary in gaining access**
- **Operational systems may be targeted to facilitate gaining access to dangerous biological materials**



# Elements of Risk

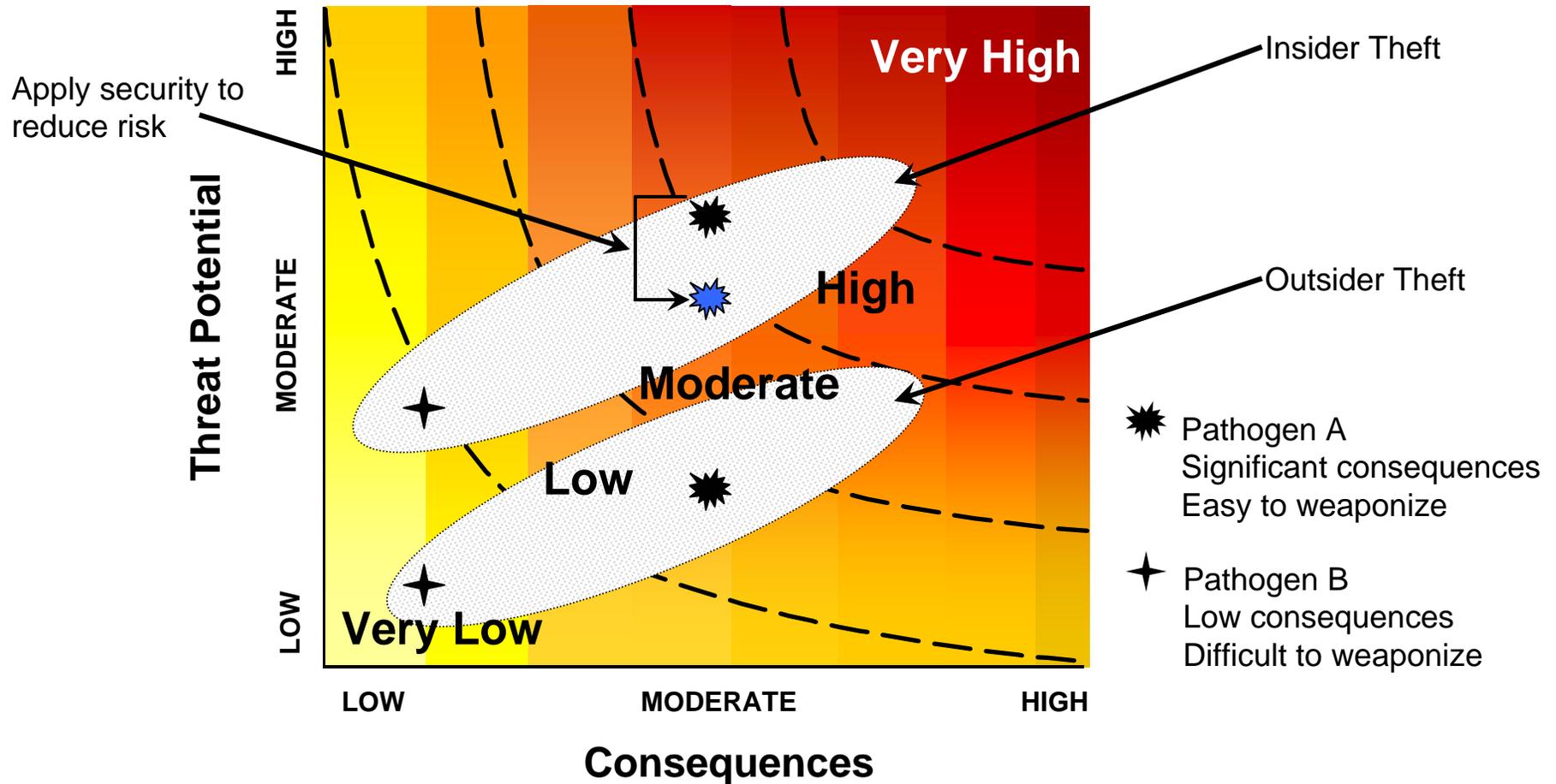
---

---

- **Evaluate adversaries**
  - **Insiders**
    - Authorized access to the facility, and possibly biological materials and/or restricted information
  - **Outsiders**
    - No authorized access
  
- **Evaluate threat potential**
  - **Capabilities**
  - **Tools**
  - **Motivation**
  - **Weaponization potential**
  - **Possibility of being caught**
  
- **Evaluate consequences**
  - **Death and illness**
  - **Economic**
  - **Symbolic**
  - **Social**



# Biosecurity Risk: Insider vs. Outsider Threat





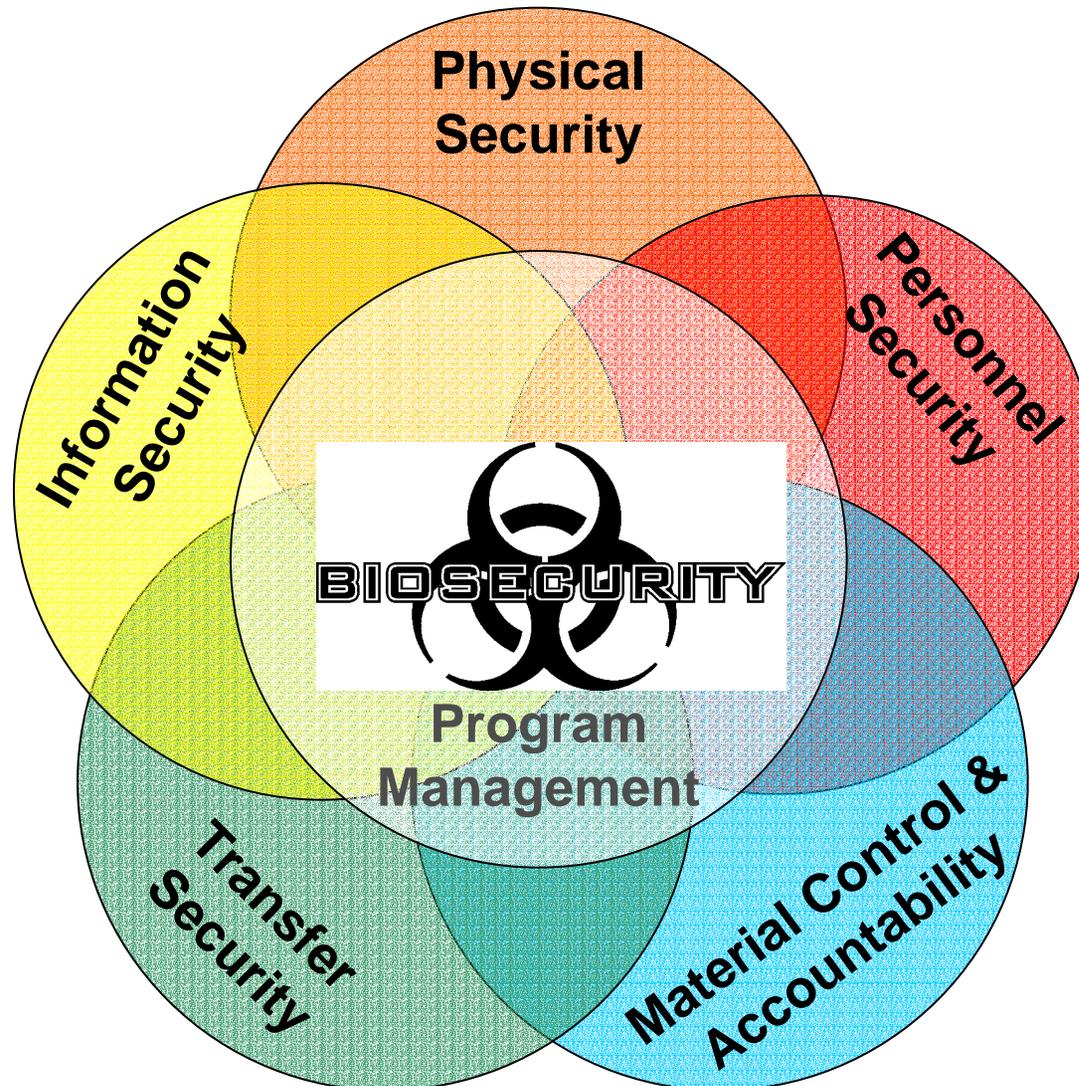
# Management Responsibilities

- Identify which possible but unlikely scenarios the security system should not be required to protect against
- Establish a protection strategy
- Determine the physical security system design
- Develop security policies and procedures
- Allocate resources





# Components of Biosecurity





# Laboratory Biosecurity Plan

---

---

- **Develop laboratory biosecurity plan:**
  - **Facility mission and description**
  - **Risk definition(s)**
  - **Physical security**
  - **Personnel management**
  - **Material control and accountability**
  - **Material transfer security**
  - **Information security**
  - **Biosecurity program management**
  - **Incident response plans and reporting**





# Elements of a Physical Security System

---

- Graded protection
- Access control
- Intrusion detection
- Response force





# Graded Protection: Concentric Layers of Security

## ● Property Protection Areas

### ■ Low risk assets

- Grounds
- Public access offices
- Warehouses

## ● Limited Areas

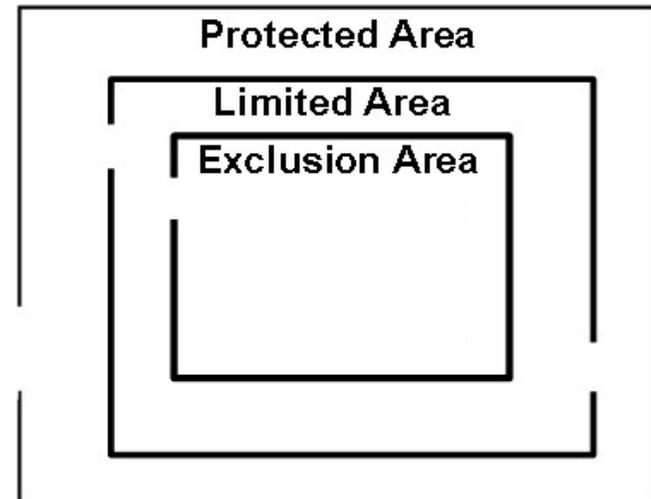
### ■ Moderate risk assets

- Laboratories
- Sensitive or administration offices
- Hallways surrounding Exclusion Areas

## ● Exclusion Areas

### ■ High risk assets

- High containment laboratories
- Computer network hubs





# Physical Security

- **Access control**
  - Ensures only authorized individuals are allowed entry
    - Increasingly strict controls as you move toward assets of highest risk
    - Unique credential: Grants access to specific areas by specific personnel
  
- **Intrusion detection**
  - Detect unauthorized access
    - Guards
    - Electronic sensors
  - Assessment
    - Validation of violation before response
    - Can be direct (guards) or remote (video)





# Personnel Security

---

- Personnel Screening
- Badges
- Visitor Control
- Training





# Screening

---

---

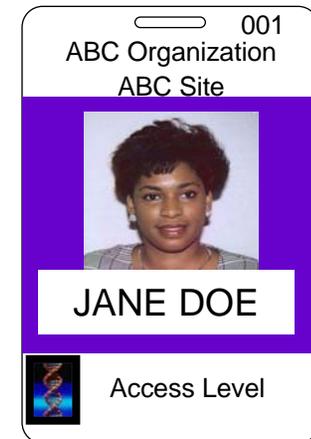
- **Conduct screening for authorized individuals**
  - Increasing level of scrutiny for high risk positions
  - Degree of scrutiny commensurate with need for unescorted access to restricted areas and/or materials
- **Mechanisms:**
  - Verify employment application information
  - Psychological/personality testing
  - Background investigation





# Badges and Visitor Controls

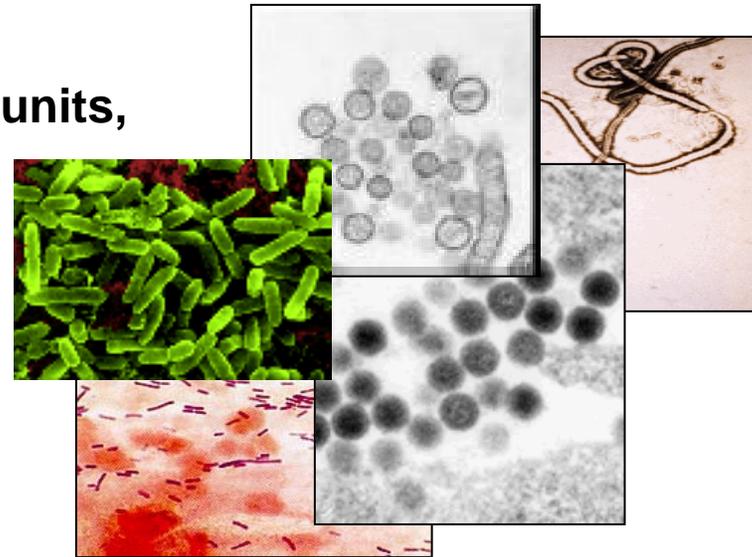
- **Badges**
  - Should be issued to those individuals authorized to be on-site
- **Visitors**
  - **Types**
    - Personal Visitors, Casual Visitors, Working Visitors
  - **Controls**
    - All visitors should have a host at the facility
    - Visitors should be escorted in restricted areas





# Material Control and Accountability

- Defining “material” is complicated
- Agent
  - Name and description
- Quantity
  - Based on containers or other units,  
NOT number of microbes



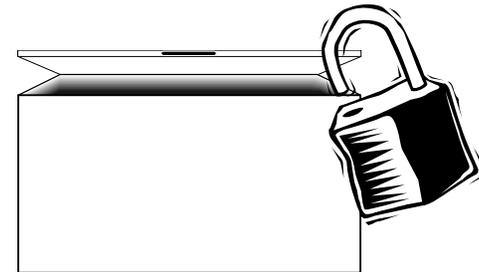
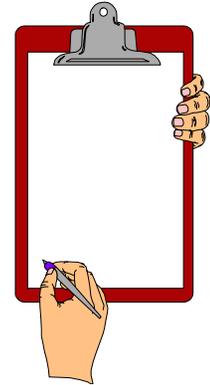


# Material Control and Accountability

---

---

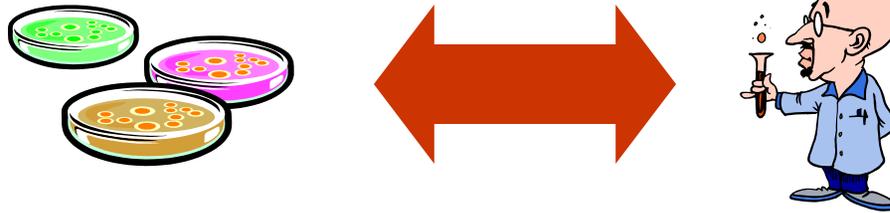
- **Control is either...**
  - Engineered / Physical
  - Administrative
- **Containment is part of material control**
  - Containment Lab / Freezer / Ampoule
- **Procedures are essential for material control**
  - For both normal and abnormal conditions





# Material Control and Accountability

- All material should have an associated “accountable person”

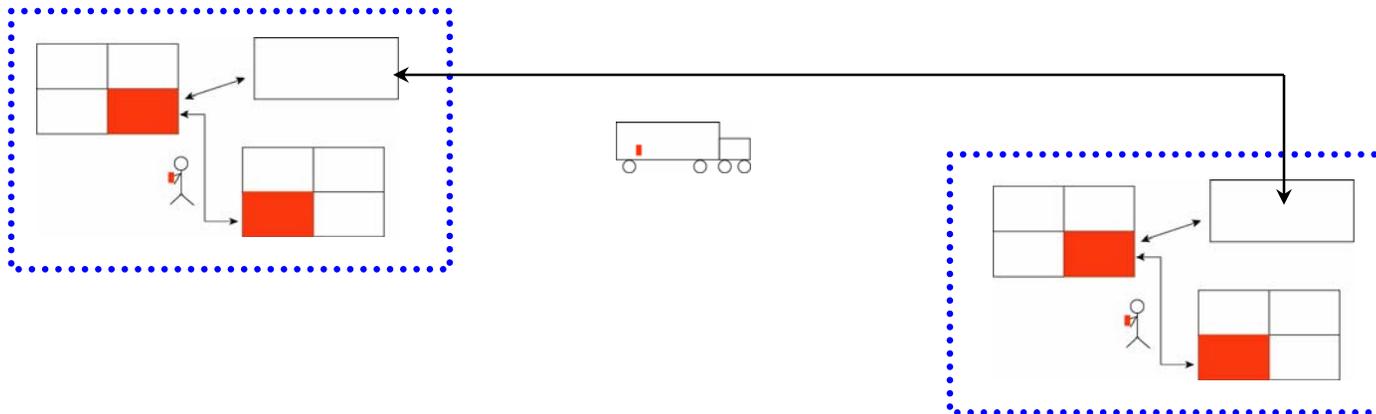


- Procedures should ensure accountability



# Material Transport Security

- **Why?**
  - Dangerous pathogens and toxins are vulnerable to theft during movement outside of protected areas
- **Who?**
  - Facilities, carriers, and states all responsible
- **The goal of transport security is**
  - To mitigate the risk of theft during transport





# Chain of Custody: Principles

---

---

- **Aims to protect sample by documenting**
  - All individuals who have control of sample
  - Secure receipt of material at appropriate location
- **Chain of custody documentation includes**
  - Description of material being moved
  - Contact information for a responsible person
  - Time/date signatures of every person who assumes control





# Facility Responsibilities

---

---

- **Personnel management**
  - For people who have access to dangerous pathogens and toxins or information during transfers
  
- **Establish chain of custody (CoC)**
  - Record all individuals who have contact with the dangerous pathogens and toxins
  
- **Provide physical security**
  - For packages that need temporary storage
  
- **Protect transport documentation**
  
- **Determine who is able to authorize, transport, and receive dangerous pathogens and toxins**



# 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**





# Identification, Control, and Marking

- **Identification**
  - Users of information should know the information's designated sensitivity level
  - Levels of sensitivities should be based on standards
    - Low, Moderate, High
  - A review and approval process aids in the identification of sensitivities
    - Critical for public release of information
- **Control**
  - The control of moderately and highly sensitive information should be the direct responsibility of the individual with the information
  - This includes the physical security of the information and places where the information is stored
- **Marking**
  - Moderately and highly sensitive information should be labeled in a consistent manner
    - Sensitivity level designation
    - Top and bottom of each page / cover sheet
  - Marking and control methods should be well understood by those working with information

**Moderate**

DEPARTMENT OF GOOD WORKS  
Washington, D.C. 20006

December 1, 1995

MEMORANDUM FOR: David Smith, Chief  
Division 5

From: Susan Goode, Director

Subject: (U) Recommendations for  
Resolving Funding Problems

1. (S) This is paragraph 1 and contains "Secret" information taken from paragraph 2 of the source document. Therefore, this portion will be marked with the designation "S" in parentheses.

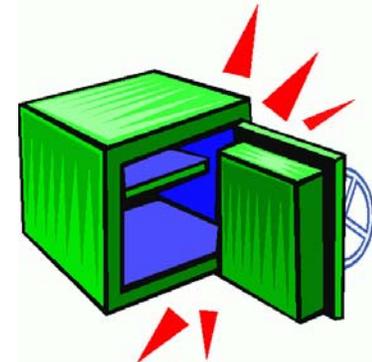
2. (U) This is paragraph 2 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

3. (U) This is paragraph 3 and also contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

Derived from: Memorandum dated 11/1/95  
Subj: Funding Problems  
Department of Good Works  
Office of Administration

Declassify on: December 31, 2000

**Moderate**





# Communication and Network Security

---

---

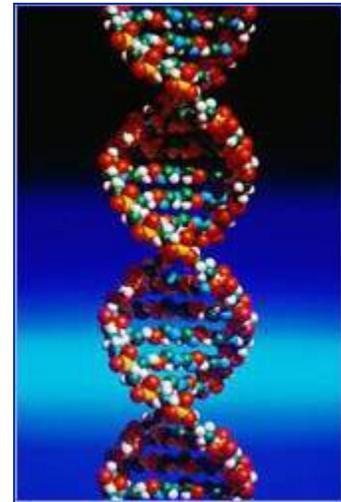
- **Insecure transmission of information can lead to accidental release**
  - **Mail, email, or fax security is required**
  - **Limited discussions in open areas**
  - **Information should only be reproduced when needed and each copy must be controlled as the original**
- **Network Management**
  - **The network on which all information is transmitted and systems on the network should be protected**
    - **Infrastructure**
    - **Servers**
    - **Network layered access**
    - **Desktop security**
    - **Remote access**
    - **Wireless**



# Summary

---

- **Necessary to take steps to reduce the likelihood that the *high risk agents* 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**
- **WHO developing guidance on Laboratory Biosecurity that provides an overview of these principles**





# Contact Information

---

---

**Jennifer Gaudio, Ph.D.  
Sandia National Laboratories  
PO Box 5800, MS 1371  
Albuquerque, NM 87185  
USA  
Tel. 505-284-9489  
email: [jmgaudi@sandia.gov](mailto:jmgaudi@sandia.gov)**

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