



Exercising Facility Biosecurity Plans

www.biosecurity.sandia.gov

SAND No. 2009-5485C

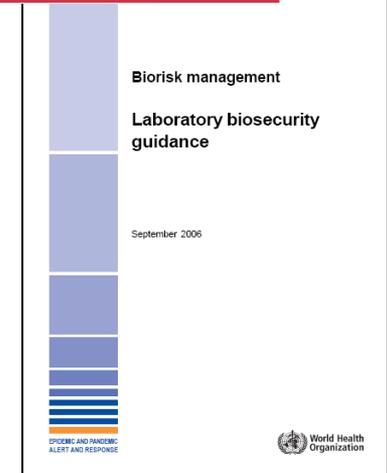
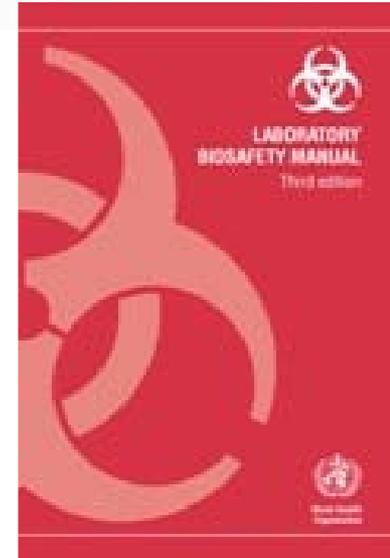
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.





A Focus on the Laboratory

- **Laboratory Biosafety**
 - A set of preventive measures designed to reduce the risk of accidental exposure to or release of a biological agent
- **Laboratory Biosecurity**
 - A set of preventive measures designed to reduce the risk of intentional removal (theft) and misuse of a biological agent – intent to cause harm
- **Fundamentally, there are risks to working with pathogens and toxins**





Discussion

- **What are the primary reasons for implementing biosecurity?**
- **Why is a security plan needed?**
- **Why exercise it?**



“...given the high level of know-how needed to use disease as a weapon to cause mass casualties, the United States should be less concerned that terrorists will become biologists and far more concerned that biologists will become terrorists.”

-World At Risk,

The report of the commission
on the prevention of
weapons of mass destruction
proliferation and terrorism,
December 2008



The Role of Design Basis Threat in Laboratory Biosecurity



What is Design Basis Threat?

- **A DBT establishes the objectives of a facility security system**
 - Defines the assets to be protected
 - Defines the threats to protect those assets against
- **A DBT is necessary to ensure that security resources are used as efficiently as possible**
 - Ensures security system is designed for specific operations
 - **Security for biocontainment facilities should be different than an airport or bank**
 - Avoids blanket protection – protecting everything equally
 - **“Protect pencils like pencils, and diamonds like diamonds”**
 - Keeps the security experts in their lane
 - **Contractors will inevitably act in their own interest**
- **Critical that the DBT be set by policy – by the institution’s owners who are ultimately responsible for all of the institute’s operations and programs**
 - Only the institution’s owners can articulate the institution’s level of risk tolerance



DBT directly affects resources and operations

- **A DBT that reflects a highly risk averse management position**
 - i.e. many assets must be protected from many different threats
 - Security system may be very expensive to install, operate, and maintain
 - Security system may significantly infringe on the institute's operations
- **A DBT that reflects a highly risk tolerant management position**
 - i.e. few assets must be protected from few threats
 - Security system may be relatively inexpensive to install, operate, and maintain
 - Security system may have little impact on the institute's operations
 - Security system may have many vulnerabilities



Establishing a DBT – defining assets

- **The easy part....**
- **Define the assets that should be protected at the institution**
 - Dangerous pathogens
 - Other pathogens
 - Specific equipment
 - Specific facilities
 - Specific information
 - Etc.



Establishing a DBT – defining threats

- **The hard part...**
 - Little information about terrorists' interest in biological weapons, or their methods for acquiring them
 - Few bioscience facilities have been attacked by adversaries
 - Little to no information available about the targeting of bioscience facilities
 - But...it happens
- **Define the threats that the defined assets should be protected against**
 - **Insiders**
 - **Scientists/technicians/animal care givers**
 - **Operations and maintenance personnel/administrative personnel**
 - **Visitors**
 - **Etc.**
 - **Outsiders**
 - **Individuals**
 - **Animal rights groups**
 - **Terrorist groups**
 - **Etc.**



Establishing a DBT – defining scenarios

- Last step is to combine the assets and threats into credible scenarios that the institution's security system should protect against



DBT and Biosecurity Risk Assessment

- **DBT should be given to team responsible for conducting the site security risk assessment or vulnerability assessment**
- **Tasking should be for the security risk assessment team to evaluate the institution against the objectives specified in the DBT**
 - What is the relative risk of the various defined threats attacking the various defined assets?
 - Does the current security system appropriately focus on the defined security scenarios that are highest risk?
 - Are security resources proportionally allocated to mitigate the highest risks?
 - What vulnerabilities exist that need to be corrected? (unacceptable risk)
 - What vulnerabilities exist that do not need to be corrected? (acceptable risk)



What is the Role of the Risk Assessment

- **Purpose: understand uncertain but possible consequences associated with specific hazards**
- **Components:**
 - Hazard identification and estimation
 - Assessment of exposure and/or vulnerability
 - Estimate of risk based on hazards and exposure/vulnerability assessment
 - **Combining likelihood and severity of selected consequences**
 - **Quantitative or qualitative**
- **Discussion: Current risk assessment methods used for biorisks**
 - How are hazards identified and estimated?
 - How are exposures and vulnerabilities assessed?
 - How are the likelihood and severity of consequences determined?



Laboratory Biosecurity Risks for Dangerous Pathogens

$$\text{Risk} = f(\text{Likelihood, Consequence})$$

- **Likelihood**
 - The likelihood of theft from a facility and the likelihood an agent can be used as a weapon
- **Consequences**
 - Of a bioattack with the agent
- **Risks**
 - Persons in area of attack
 - Persons in larger community from secondary exposure
 - Animals in area of attack
 - Animal in larger community from secondary exposure



Following the site security risk assessment

- **The institution should use the risk assessment results to determine whether or how the existing security system should be modified or improved**
- **After any necessary modifications, the institution should have a security system that meets all the objectives of the DBT, and also prioritizes security against the highest risk security scenarios**
- **Then, the institution should write a laboratory biosecurity plan that reflects the full operation of the resulting security system**
- **The security plan should reference the site risk assessment, and the site risk assessment should reference the DBT**
 - Combined, all three documents will help ensure an effective and efficient security system, and should satisfy any external auditors



What goes into a Security Plan



Biosecurity Plan

- ***Biosecurity plans* are procedures and mitigation strategies ultimately designed to protect biological materials and related valuable assets against unauthorized**
 - Access
 - Theft
 - Loss
 - Release
 - Sabotage
- **Incident response plans describe methods by which facilities respond to various incidents**
 - Natural
 - Medical
 - Biosecurity
 - Security
- **Based on facility-wide risk assessment**
- **Coordinate with facility-wide plans and procedures**



Biosecurity Plan Contents

- **Summary of Risk Assessment**
 - Site-specific
 - Agent-specific
 - Facility wide
 - Summarize threats, vulnerabilities, risks
- **Plan language**
 - Refers to the assessments and conclusions
 - Identify and elaborate on resulting security measures
- **Detailed descriptions of procedures and protocols necessary to mitigate unacceptable risks to protect valuable materials**
 - Physical security
 - Information security
 - Material in transit
 - Material accountability and control
 - Personnel
- **Incident Response Plans**



US Select Agent Rule: Security Plan

- **The security plan must**
 - Be designed according to a site-specific risk assessment and must provide graded protection in accordance with the risk of the select agent or toxin, given its intended use.
 - Describe procedures for physical security, inventory control, and information systems control
 - Contain provisions for the control of access to select agents and toxins
 - Contain provisions for routine cleaning, maintenance, and repairs
 - Establish procedures for removing unauthorized or suspicious persons
 - Describe procedures for addressing loss or compromise of keys, passwords, combinations, etc. and protocols for changing access numbers or locks following staff changes
 - Contain procedures for reporting unauthorized or suspicious persons or activities, loss or theft of select agents or toxins, release of select agents or toxins, or alteration of inventory records
 - Contain provisions for ensuring that all individuals with access approval from understand and comply with the security procedures



Purpose of SOPs

- **Ensure all relevant individuals understand the process**
- **Document how activities shall be performed**
 - Facilitate consistency
 - Ensure compliance with regulations
- **Types of SOPs**
 - Repetitive technical activities
 - Sample receipt and processing
 - Diagnostic test procedures
 - Administrative procedures
 - The process for proper documentation of training
 - Laboratory Access Authorization
 - Response Activities
 - Building evacuation
 - Suspicious individuals and activities
 - Medical emergencies



Documentation

- **Documentation**
 - Retention times should be determined for all types of documentation
 - Methods of documentation should be determined for each type of information requiring documentation
 - Maintain control of documentation containing potentially sensitive information
 - Personnel records
 - Access control or security systems
 - Biological agent specific information
 - The plan should describe methods of control for potentially sensitive documentation
 - Samples of all forms should be included in an appendix of the plan



Biorisk Documentation: Discussion

- **What are the key topics you would want in a security plan?**



Activity

- **Starting with the key topics outlined as a class, work in your small groups to outline a security plan for a hypothetical facility**



Biosecurity Plan: Physical Security

- **Description of physical security systems**
 - Systems in place
 - System applications
- **Procedures for entry and exit**
 - During business hours
 - After business hours
- **Alarm response procedures**
- **Response actions for security breaches**



Biosecurity Plan: Information Security

- **Descriptions of systems in place to protect information**
 - Electronic
 - Passwords
 - Firewalls
 - Encryption
 - Hard copy records
 - Information classification
 - Mechanisms in place to control sensitive information
 - “Need to know”
 - Backup systems
 - Key control program for mechanical keys
 - Theft, loss
 - Unauthorized duplication



Biosecurity Plan: Material in Transit

- **Procedures for how biological materials are handled**
 - Packaging requirements
 - Internal transfer processes
 - External transfer processes
 - Shipment tracking
 - Material monitored until pick up by appropriate carrier
 - Verify receipt of shipment
 - Verification of receiving persons
 - Legitimate need and proper approval
 - Material receipt procedures



Biosecurity Plan: Material Control and Accountability

- **Inventories**
 - Policies and procedures for conducting and maintaining inventories
 - Appropriate for material
 - Stock cultures
 - Animals
 - Toxins
 - Self-replicating organisms
 - Current
 - Limited access
 - Password
 - Keys



Biosecurity Plan: Personnel

- **Descriptions of provisions for different types of personnel (escorted and unescorted)**
 - Maintenance personnel
 - Visitors
 - Repair personnel
 - Cleaning staff
- **Granting access**
- **Removing access**
- **Suitability screening**
 - Background investigation
 - Credential verification
 - Education verification



Biosecurity Plan: Incident Response

- **Response procedures**
 - Theft, loss, misuse, release
 - Suspicious persons
 - Suspicious activities
 - Suspicious items
 - Natural disasters
 - Medical
 - Life threatening
 - Non-life threatening
 - Power outage/electrical failure
 - Equipment failure
 - Proper reporting mechanisms
 - Proper methods to securing an area
- **Reporting procedures**
 - Theft, loss, release
 - Incidents
 - Documentation



Example – US Select Agent Rule: Incident Response Plan Requirements

- All registered entities must develop and implement a written incident response plan
- The incident response plan must fully describe the entity's response procedures for
 - Theft, loss, or release of a select agent or toxin,
 - Inventory discrepancies,
 - Security breaches (including information systems),
 - Severe weather and other natural disasters,
 - Workplace violence,
 - Bomb threats and suspicious packages,
 - Emergencies, such as fire, gas leak, explosion, power outage, etc.
- Plan must be reviewed annually and revised as needed
- Drills or exercises must be conducted at least *annually* to test and evaluate the effectiveness of the plan



Biosecurity Plan: Training

- **Types**
 - Initial training
 - Ongoing training
 - Refresher training
- **Required for all plans and procedures**
- **Consider method to validate successful completion of training**



Biosecurity Plan: Drills and Exercises

- **Plans and procedures should be validated by performing either drills or exercises**
 - After initial development
 - After an event
 - When procedures are changed or new procedures are developed
 - Review and revise on a routine basis
 - Annually
 - Every two to three years at least

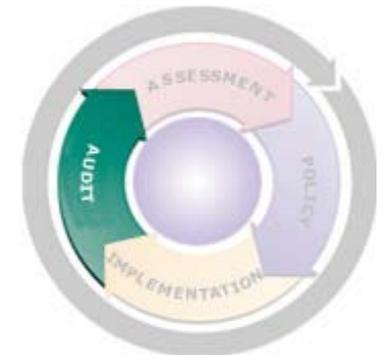


Exercising the Security Plan



Evaluating the Biosecurity System

- Goal of the evaluation is to determine if the security system meets the defined objectives and regulatory requirements
- Audits and inspections
 - Internal and external
 - Does the management system in practice conform to the plans and requirements? Is it being implemented effectively?
- Technical Evaluation
 - Verification of balanced protection
 - Testing the technical functionality of the system
- Evaluation by Exercise
 - Test protocols, personnel, resources
 - **Tabletop exercises**
 - **Full Scale exercises**



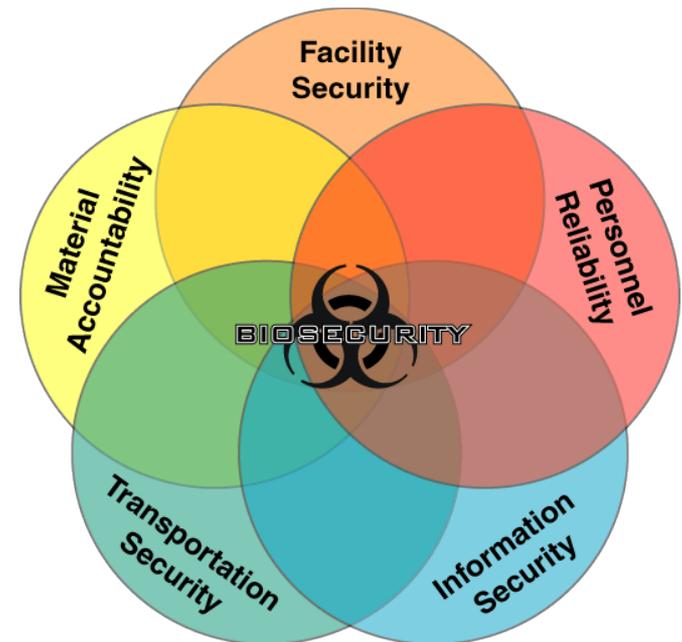


Balanced Protection

- Each component of the biosecurity system must be designed to meet the defined objective
- Each subcomponent must also meet the defined objective

- E.g. Highly sophisticated physical security system but laboratory does not have a personnel reliability program. Person's with poor integrity can have authorized access, therefore bypassing the physical security system

- E.g. Laboratory with access controls, intrusion detection, and alarms on a door has nothing provide protection to a window into the laboratory which can be opened from the outside.





Testing the Technical Functionality of the System

- The system must function technically as designed
 - Performance testing, commissioning
- Each component of the technical security system should be verified and tested and the whole system tested to ensure components work together as intended
 - Detection mechanisms
 - Delay mechanisms
 - Alarm communication
 - Access controls
 - Inventories
 - ...
 - For example, see door test procedures on CD
- Ideally, the security system should be evaluated by a third party
- Consider the frequency for functional testing



Evaluation by Exercise

- The goal of an exercise is to simulate an event and determine the overall effectiveness of the security plan
- Exercises can focus on single components of the security plan or the entire plan
 - The physical security system and response
 - The personnel reliability program
 - Information protection
 - Material control and accountability
 - Transport Security
- Frequency of evaluation by exercise may vary (regulatory requirements?)
- Different types of exercises; differences in complexity
- May require coordination with outside agencies
 - Memoranda of understanding



Exercise Design

- Identify key 'players'
 - Security management
 - Response force personnel
 - Facility operations
 - Biorisk management (biosafety officers)
 - Others...
- Define scope
 - What is/are the 'threat(s)' for this exercise? (From the DBT)
 - **Who (insider/outsider, type of insider)**
 - **Motivation (sabotage, theft – theft of what...)**
 - **Level of knowledge of threat**
 - What is the state of the facility (time of day, number and location of personnel including response forces, etc)
- Remember, it may not be obvious that an event is intentional



All Exercises

- **Each task in the exercise should be designed and tailored to the specific organization**
 - Objectives
 - Capabilities
 - Resources
 - Plans
 - Limitations
- **The exercise should be flexible**
 - Must meet the needs of the specific organization



Steps to Building an Exercise

- **Establish a base**
 - Establish groundwork necessary for the exercise
- **Develop the exercise**
- **Conduct the exercise**
- **Evaluate and Critique**
- **Follow up and review**



Establish a Base

- **Identify the plan to test**
- **Identify the development team**
- **Consider the type of exercise that best tests the plan and meets training needs within resource boundaries**
 - **Tabletop Exercise (TTE)**
 - **Full Scale Exercise (FSE)**
 - **Resource intensive so consider available resources**
- **Define the scope and specific objectives**



Exercise Design

- **Develop an appropriate exercise to test the plan**
- **Write the exercise**
 - Statement of Purpose
 - Narrative
 - Expected actions
 - Injects and messages
- **Consider additional personnel that may be required to conduct exercise (volunteers, facilitators, etc.)**



Conduct the Exercise

- **Be clear and concise**
- **Foster reality as much as possible**
- **Identify timelines**
- **Capitalize on problem situations**
 - Added stress can be a positive attribute in the exercise



Evaluation and Follow Up

- **After Action Review after the exercise**
- **Evaluate and critique the exercise**
 - What went right
 - What went wrong
 - Discuss additional training that may be necessary
- **Follow up with lessons learned**
 - Modify plan as necessary
 - Perform the exercise again, if necessary, to evaluate incorporated changes
- **Remain flexible and open to constructive criticism**



TABLETOP EXERCISES



Tabletop Exercise

- Facilitated analysis of an event
- Occurs in an informal setting
 - Essentially a “Brainstorming” session to generate constructive discussion among participating agencies
- Designed to examine situations and resolve issues based on existing plans
 - To determine the effectiveness of the security system
 - **Detection, delay, and response**
 - To provide better understanding of each persons roles and responsibilities
 - To highlight problems or limitation of the security system
- Relies on “words” to achieve perspective of the event



Pros and Cons

- **Advantages**

- Modest time commitment
- Simple
- Inexpensive
- Time available to acquaint individuals with the plan and response
- Opportunity to identify capabilities
- Opportunity to identify additional requirements

- **Disadvantages**

- Not realistic
- Plan execution is superficial and does not occur in real time
- Cannot demonstrate system overload or potential logistical issues easily



TTE Objectives

- **Table Top Exercises can test plans**
 - Carried out in an appropriate room or other setting; comprised primarily of dialogue
 - Relevant individuals discuss general issues and procedures in the context of a scenario or event
 - Based on existing operational plans
 - Discuss and identify roles and responsibilities
 - Clarify expectations
 - Gain familiarity of procedures
 - Discuss how fast key players can respond
- **TTE can also identify**
 - Gaps in a plan
 - Potential response problems or issues
 - Potential need for additional resources



TTE Development

- **Individuals from various facility departments and relevant agencies should be part of the process**
 - Assess needs and define scope
 - Roles and responsibilities may be different than what is initially expected
 - Consider other relevant existing plans that may require inclusion
 - Define exercise objectives
 - Write the detailed narrative
 - List expected actions
 - Identify timelines
 - Prepare injects and messages



TTE Considerations

- **Should be used to test existing plans**
- **Discuss communication to identify potential issues**
 - Terminology
 - Back up if communications become compromised
- **Exercises can start as simple discussions internally**
 - Introductory overview of the plan and process
 - Make everyone familiar with the plan so all can participate appropriately
 - Everyone is familiar with respective roles and responsibilities, expectations
- **Larger TTE can involve some props with discussion**



FULL SCALE EXERCISES



Full Scale Exercises (FSE)

- Exercise that is as close to the real event as possible
- Interactive event designed to test multiple facets of a plan
- Designed to achieve a realistic perspective of an event through simulation
 - Resource and personnel allocation
 - Communication effectiveness
 - Efficiency of efforts
 - Decisions and actions performed in real time
- Expands the Tabletop Exercise to the field and adds reality



FSE Purpose

- **Test coordination of the facility and responding agencies**
- **Enables facility to evaluate performance of many functions and activities simultaneously**
- **Identify gaps or deficiencies in the plan, personnel, and other resources**
- **Can also demonstrate facility readiness and ability to respond quickly and appropriately to the plethora of events that could occur**
- **Evaluates the active mobilization of personnel, equipment, and resources**



FSE Characteristics

- **FSE occurs in a realistic setting**
- **Realism achieved by acting out roles**
- **Individuals respond as they would in the real event**
- **Coordination of multiple agencies is required**
- **Evaluation of multiple functions and activities simultaneously**
- **Action results from on scene decisions made in real time**
- **Evaluate resource and personnel allocation**
- **Evaluate effectiveness and efficiency of communication devices and efforts**
- **Additional requirements may include**
 - Simulated victims
 - Simulated adversaries



FSE Design

- **Start small then build to more complex exercises due to logistical effort and expense required**
- **Similar steps as TTE but more in depth information is required**
- **Narrative is shorter since much of the FSE is real; written descriptions aren't required**
- **Messages can be visual or written**
- **Special considerations**
 - Site selection
 - Scene management (props and materials)
 - Personnel (victims, facilitators, volunteers)
 - Resources (equipment number and type)
 - Hazard identification and safety during the exercise must be considered in advance



Running the FSE

- **May require specific personnel**
 - Volunteers to act out specific roles
 - Evaluators
 - Facilitators
 - Safety Officer
- **Exercise may be announced or start “without notice”**
 - Certain agencies will require notification of pending event to realize the event is not real, such as dispatchers for police, etc.



FSE Considerations

- **Requires significant amount of time for development**
- **Requires significant time, effort, and resources to carry out exercise; exercise can have long duration**
- **Requires coordination of all participating agencies**
- **Determine “call off” actions should a real emergency or situation occur**



Biosecurity Scenarios: **To Be Exercised**

- Working in your group, review the security plan you outlined earlier,
- Please identify how would you exercise the components you identified?
 - **Which do not need to be exercised?**
 - **Which can you use a table top?**
 - **Which should you conduct a full scale exercise?**



After Action Review

- **Occurs immediately after the exercise**
- **Process should summarize event**
- **Review of the exercise**
 - Review what was intended
 - Review what actually happened
- **Everyone should have the opportunity to provide comment**



Purpose

- **Identify success or failure of the exercise and plan future activities**
 - Did the exercise meet the objectives?
 - Did participants fulfill expected roles?
 - Were protocols followed? Were problems identified with protocols?
 - Did the exercise adequately test the plan, participating individuals, agencies?
 - Discuss what went right
 - Discuss what went wrong
 - **Discuss potential problems**
 - **Identify additional required resources**
 - **Modify roles/responsibilities where necessary**
 - Start the process to identify solutions to possible issues
- **Can be used to aide in future exercise planning**



Conclusion

- **A DBT establishes the objectives of a facility security system**
 - Defines the assets to be protected
 - Defines the threats to protect those assets against
- ***Biosecurity plans* are procedures and mitigation strategies ultimately designed to protect biological materials and related valuable assets**
- **The biosecurity risk assessment helps to identify the likelihood and the possible consequences associated with specific hazards**
- **The security plan should reference the site risk assessment, and the site risk assessment should reference the DBT**
- Goal of evaluating the security system and exercising the security plan is to determine if the security system meets the defined objectives and regulatory requirements