



Biosecurity System Testing and Evaluation



Biosecurity Inspector Training

Staten Serums Institut

31 August – 2 September 2009

www.biosecurity.sandia.gov

SAND No. 2009-5485C

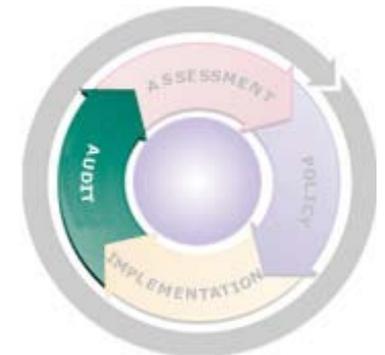
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.





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



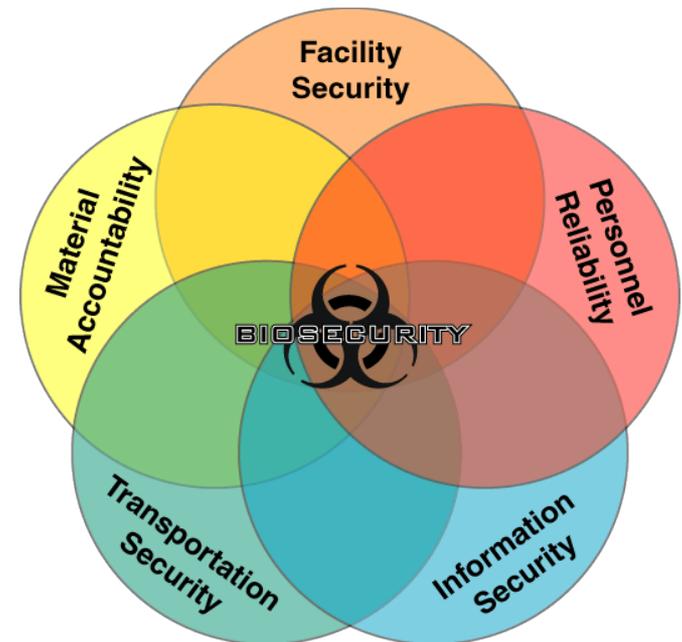


Balanced Protection

- 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 to provide protection to a window into the laboratory which can be opened from the outside.





Internal Inspections: Discussion

- **What are the objectives of an internal inspection?**
- **What should an internal biosecurity inspection focus on?**
- **Who should carry out an internal inspection?**
- **With what frequency?**
- **How should the results of internal inspections be communicated, documented, and followed up?**



External Inspections: Discussion

- **What are the objectives of an external inspection?**
- **What should an external biosecurity inspection focus on?**
- **In Denmark, should there be external inspections carried out by others besides CBB? Why or why not?**
- **What triggers an external inspection? With what frequency are they carried out?**
- **How should the results of external inspections be communicated, documented, and followed up?**



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**



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**



Full Scale Exercises

- **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**



Tabletop vs. Full Scale Exercises: **Discussion**

- **What are the main differences between tabletop and full scale exercises? Consider participants, setting, preparation effort, required memorandums, difference in lessons learned, objectives.**



After Action Review

- **Occurs immediately after the exercise**
- **Useful for all types of exercises**
- **Process should start with event summary**
- **Review of the exercise**
 - Review what was intended
 - Review what actually happened
 - Identify successes and failures
- **Everyone should have the opportunity to provide comment**
- **Design follow-up actions to alter security plans, response actions, or to mitigate identified vulnerabilities**
- **Assign responsibilities for corrective actions**



Biosecurity Scenarios: **To Be Exercised**

- **Develop a list of scenarios that facilities should evaluate through an exercise. Identify whether Tabletop or Full Scale Exercise is more appropriate.**



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**



Biosafety Scenarios: Discussion

- **What biosafety situations could have security implications?**

- **Should these biosafety situations be exercised? How should the security aspects be included in those exercises?**