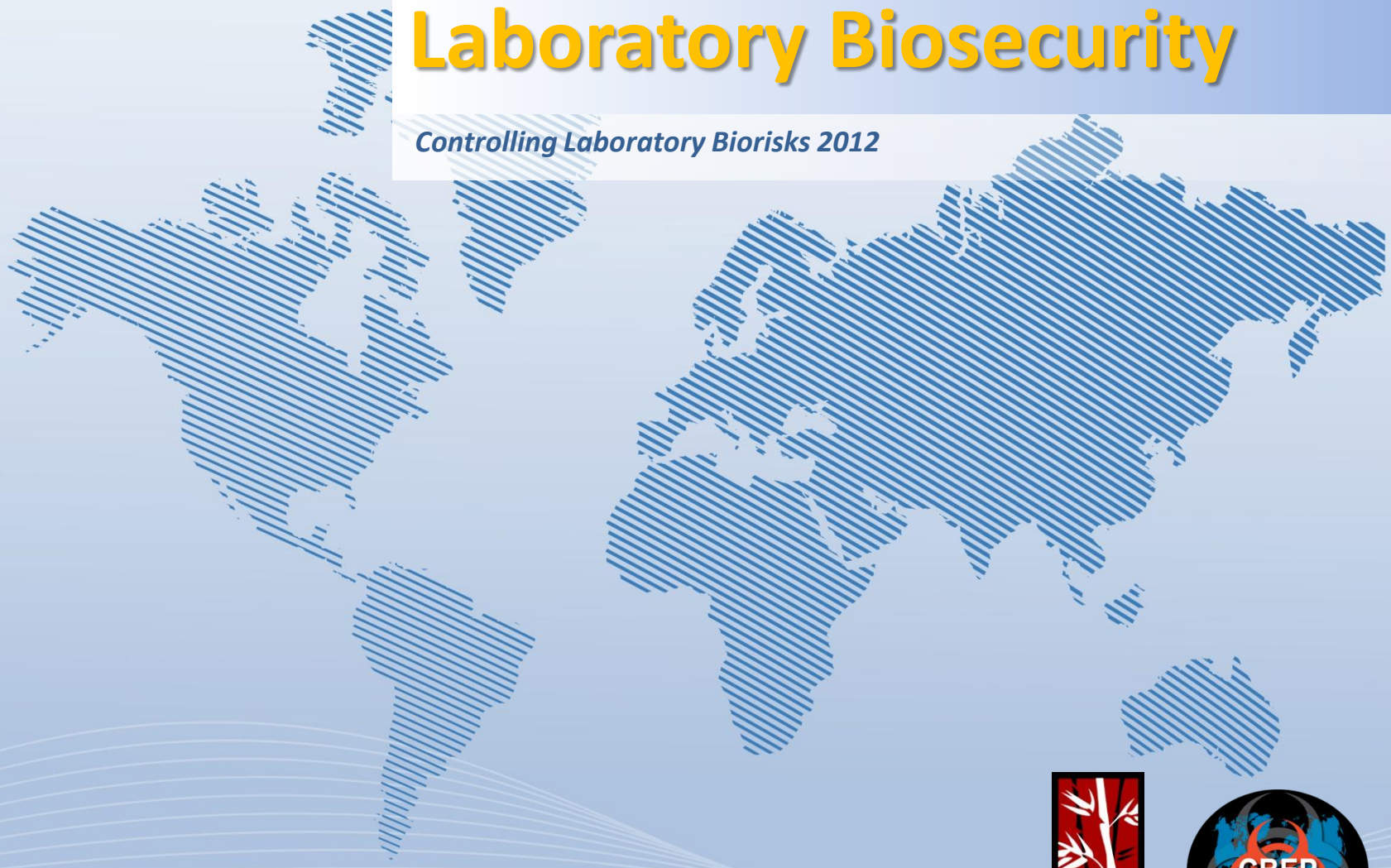
SAND2012-4386C

Laboratory Biosecurity

Controlling Laboratory Biorisks 2012



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

BIOSECURITY ENGAGEMENT PROGRAM

CBEP
COOPERATIVE BIOLOGICAL ENGAGEMENT PROGRAM

Course Objectives

- Protecting biological agents and toxins in the laboratory from loss, theft, or misuse is an important aspect of laboratory operations.
- A proper biosecurity risk assessment is necessary before implementing an efficient and effective biosecurity program.
- Securing pathogens and toxins can be very different from securing other kinds of materials.
- Physical Security is only one component of a successful laboratory biosecurity program.
- Material Control and Accountability, Transport Security, and Information Security complement other security components.
- Security awareness is crucial in laboratory biosecurity.

Laboratory Biosecurity

Question: What is **laboratory biosecurity**?

Activity:

At your tables, please spend **5 minutes** to develop a definition for **laboratory biosecurity**.

- To help with this task, **list everything that comes to mind** when thinking about **laboratory biosecurity on sticky-notes** and place them on your flip chart.

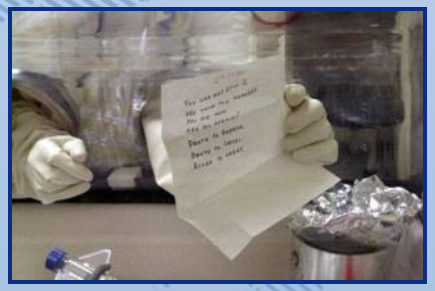
Once you are done, **write your definition at the top of the flip chart,** and be prepared to discuss with the rest of the class.

Biosecurity Threats

Examples

- Attacks on bioscience facilities by outside adversaries with the intent to cause harm
  - Stealing: Pathogen collections, Select agents, research animals
  - Arson and sabotage

- People outside bioscience facilities who want to obtain pathogens with the intent to commit malicious acts
  - Extremists purchasing pathogens: *Salmonella typhi*, Anthrax, *Clostridium botulinum*, *Yersinia pestis*



- People within bioscience facilities using their position to commit malicious acts
  - Stealing pathogens: Anthrax, *Shigella dysenteriae*, *Salmonella typhi,* toxins
  - Research theft: intellectual property – data, materials, cultures

Unique Challenges

Discussion: What are some **unique challenges to securing biological materials in a laboratory**, as opposed to securing:

- Money
- Dangerous Chemicals
- Nuclear Material
- Electronic Information?

What makes biological materials different?

Unique Challenges

- Viruses and Bacteria can **multiply**, making them difficult to count (and thus, keep track of) in the laboratory.
- Potentially, one need only steal a **small amount**… more can always be grown from that seed stock.
- Detection of theft is almost impossible. Vials are small. Biological agents do not give off energy (unlike radiological materials), making stand-off **detection difficult.**

Unique Challenges

Question: Where can you **find biological materials** in the laboratory?

What should we protect?

1) Only vials with well-characterized strains? Closely related strains? Aliquots?
2) Genetic materials? Reagents? Vectors?
3) Waste?
4) Experimental Results? Sequence Information?
5) Animals?

How should we protect?

Unique Challenges

Laboratories, unlike banks or nuclear repositories, **do not often think of themselves as needing to be secure** – this often requires a **cultural change** toward security.

1) For most **laboratory workers**, the idea that their biological materials could be desired for intentional misuse is foreign.
2) In **academic** settings, openness is valued.
3) In a **clinical** setting, security does not typically consider biological materials.

A proper **Risk Assessment** can help determine security needs

Unique Challenges

Group Activity:

A goal of a laboratory is to operate safety and securely, but at times these goals may be at odds with each other.

What are some examples? How do you choose between Safety and Security?

In your group, please spend **10 minutes** to answer the above questions. Put your examples on sticky-notes and place them on your flip chart.

Be prepared to report your answers to the class.

Unique Challenges Summary

Securing biological materials in the laboratory can be challenging because they can **replicate**, are **hard to detect**, are **found everywhere** and the idea of security in the laboratory setting often requires a **cultural change** as well as good **communication about potential risks**.

Key Components of Biorisk Management

- Biorisk **Mitigation**
  - Actions and control measures that are put into place to reduce or eliminate the risks associated with biological agents and toxins

Biosecurity Risk Mitigation

Biosecurity Risk Mitigation is the process whereby **risks** identified and characterized during a risk assessment **are reduced through active intervention**, be it **physical** or **procedural**.

Biosecurity Risk Mitigation should be based on a **Risk Assessment** including analyzing hypothetical scenarios with a defined **agent**, **adversary**, and a particular **way** that adversary will attempt to **steal and/or misuse** the biological material.

Biosecurity Risk Mitigation

There are five pillars of Biosecurity Risk Mitigation

1) **Physical Security**
2) Personnel Management
3) Material Control & Accountability
4) Transport Security
5) Information Security

What makes biological materials different?

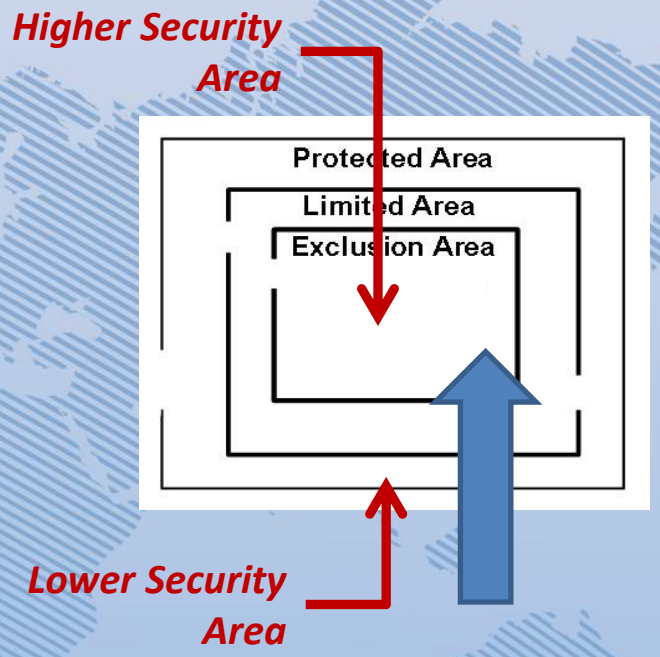
Physical Security

The first “pillar” is **Physical Security**

Physical Security is the assurance of safety from physical intrusion

Physical Security

An important concept in **Physical Security** is the concept of **Graded Protection**. This is based on the idea that different areas of a facility will have different **levels of security** based on risk.



Graded Protection is manifested in concentric rings of increasing security spanning **from outside to inside** the facility.

Physical Security

Graded Protection

Property Protection Areas (**Low risk assets**)

- Grounds
- Public access offices
- Warehouses

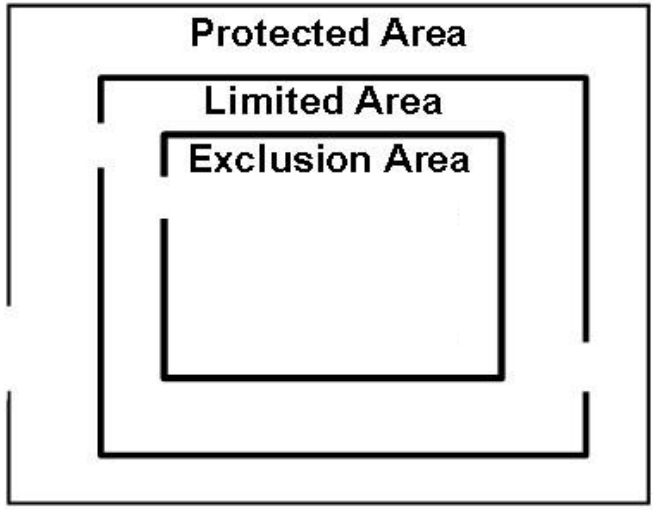
Limited Areas (**Moderate risk assets**)

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

Exclusion Areas (**High risk assets**)

- High containment laboratories
- Computer network hubs

Concentric Layers of Security



Question:

Why is concentric good?

Physical Security

3 Principles of Physical Security:

- **Detection**
- **Delay**
- **Response**

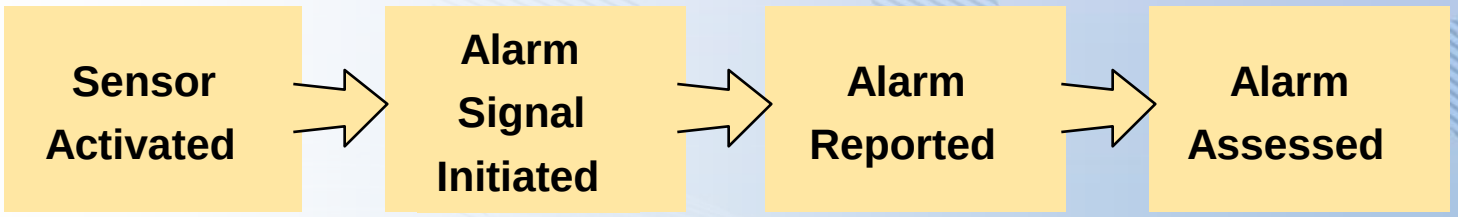
We will also cover **Access Control**, which is another important, overall, aspect of physical security.

Physical Security

Principle 1) **Detection**

Intrusion **Detection** is the process of determining whether an unauthorized action has occurred or is occurring

Detection includes sensing the action, communicating the alarm, and assessing the alarm



Physical Security

Principle 1) **Detection**

For Example:

Intrusion **Detection** can be as complicated as a **closed-circuit television system**, infrared and **motion sensors**, and **guards** patrolling throughout the facility.

Or, it could be as simple as good **training** of laboratory staff and a procedure to call someone in case a suspicious person is noticed in the laboratory.

Physical Security

Principle 2) **Delay**

Delay is simply the act of slowing down an intruder's progress in your facility long enough so that the adversary may be detected, assessed and responded to.

There are many ways of delaying an intruder

- **Guards**
- **Perimeter Fencing**
- **Solid doors with locks**
- **Bars on windows**
- **Magnetic switches on doors**

Physical Security

Principle 3) **Response**

Response is the act of alerting, transporting, and staging a security force to interrupt and neutralize an adversary.

Response is tied to the overall system objective

Deny: To prevent an adversary from reaching the target/objective

Contain: To 'catch' an adversary before they leave with the target or before they accomplish the objective

Physical Security

Principle 3) **Response**

For Example:

Based on your **Risk Assessment** and **scenario analysis, Response** can range from implementing a **guard force** in your facility to establishing a line of **communication** with your local **police force**.

Physical Security

Access Control

Access Control is another important aspect of biosecurity. It is the mechanism to determine and control authorized entry into secured areas. **Access Control** also provides capability to delay or deny unauthorized personnel.

Question: Is there a scenario in which someone would want to allow a person to bypass access controls?

Physical Security

Access Control

For Example, access granted based on:

Something you have

Key

Card (Credential)

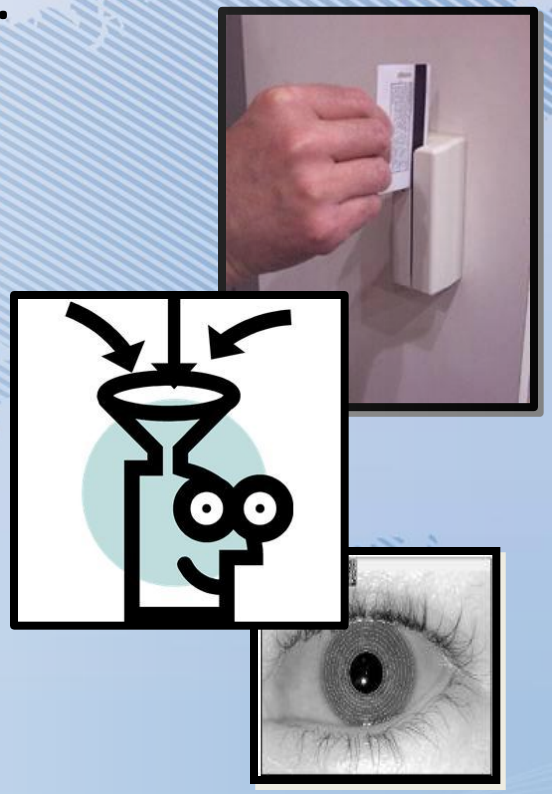
Something you know

Personal Identification Number (PIN)

Password

Something you are

Biometric feature (i.e., fingerprints)



Physical Security Activity

Group Activity:

A facility is working with large quantities of cultured ***Yersinia pestis*** in a laboratory area accessed by approximately 30 people. After a risk assessment, the laboratory director fears terror groups may try to access these cultures.

In your group, please spend **15 minutes** to **design a physical security system** for this facility. Please discuss how you would **detect**, **delay** and **respond** to potential intruders, and how you would control **access**.

Use your flip charts to design your physical security system and be prepared to report to the class.

Physical Security

Discussion:

What do you do in your laboratories at home to prevent people from entering areas they are not supposed to?

Physical Security Summary

Physical Security is the most "traditional" pillar of biosecurity. When people hear "security", they often think of guards, gates, and guns.

For many **laboratories**, however, physical security may not be the most important aspect of biosecurity. Not too many people from the outside may want to get in, even if there are "desirable" microorganisms. **As an outsider, if you don't know anything about a laboratory, it may be difficult to find what you are looking for even if physical security is not very good.**

Of course, every system must be designed not on intuition, but after a **robust risk assessment**.

Biosecurity Risk Mitigation

There are five pillars of Biosecurity Risk Mitigation

1) Physical Security
2) **Personnel Management**
3) Material Control & Accountability
4) Transport Security
5) Information Security

What makes biological materials different?

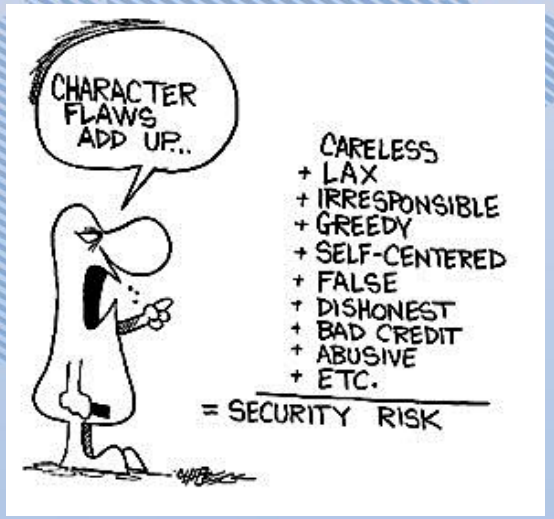
Personnel Management

The second “pillar” is **Personnel Management**

Personnel Management in the context of biosecurity, it is the assurance that the people that are given access to sensitive biological materials **should** have that access.

Personnel Management

The Objectives of a Personnel Management Program are to:



Understand that human factors can significantly impact the success of biorisk management.

- To reduce the risk of theft and fraud
- To reduce the risk of scientific misconduct
- Etc..

To support the procedural and administrative access control requirements

Personnel Management

For Example: These are some factors that can influence **Human Performance**

- **Job**
  - Setting
  - Values
- **Individual**
  - Personalities
  - Values
- **Organization**
  - Expectations
  - Assessments

Personnel Management

Personnel Training – Security Awareness

Promoting **security awareness** in employees is one of the most important ways breaches in security can be recognized.

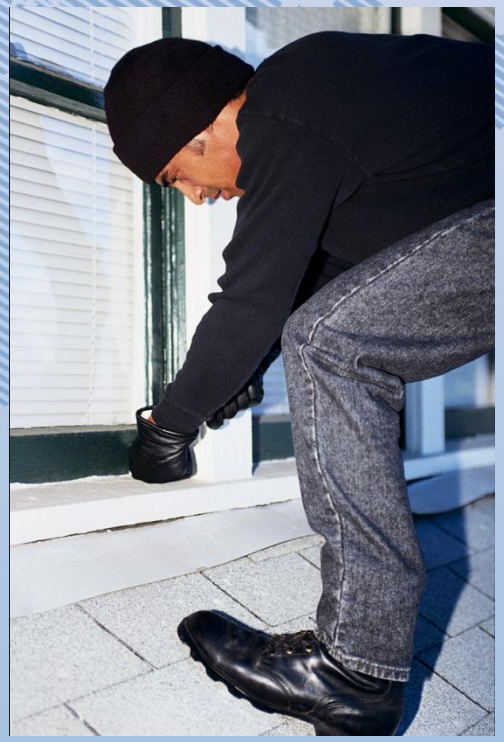
Lab workers should be **aware** of who should be and should not be in their work areas.

For Example:
A person with the wrong type of badge, or simply someone you don't recognize in your part of the building, should be asked: "who are you?" and, if necessary, reported to building security.

Personnel Management

Question:

What are some factors to consider when assessing the **risk** of **insider** versus **outsider** threat?

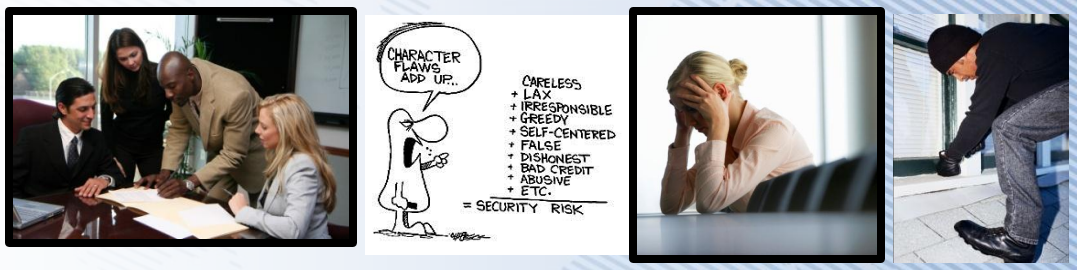


An **insider** is a person who has authorized access to a facility, its units (such as laboratories), and its assets.

An **outsider** is a person who does not have authorized access.

Personnel Management

Discussion:



What do you do in your laboratories to promote a secure work environment in terms of human performance and security awareness?

Biosecurity Risk Mitigation

There are five pillars of Biosecurity Risk Mitigation

1) Physical Security
2) Personnel Management
3) **Material Control & Accountability**
4) Transport Security
5) Information Security

What makes biological materials different?

We will also discuss a sixth topic:

6) Security Awareness

Material Control & Accountability

The third “pillar” is **Material Control & Accountability**

Material Control & Accountability is the assurance that there is an awareness of what exists in the laboratory, where it is, and who is responsible for it.

Material Control & Accountability

The Objective of **MC&A** is to:

- **Ensure the complete and timely knowledge of:**
  - What materials exist
  - Where the materials are
  - Who is accountable for them

- **Objective is NOT to detect whether something is missing.** This could be impossible. The objective is to create an environment that discourages theft and misuse by establishing oversight.

- Most laboratories already control and track their samples for scientific reasons. The emphasis here is that this is also important from a security perspective.

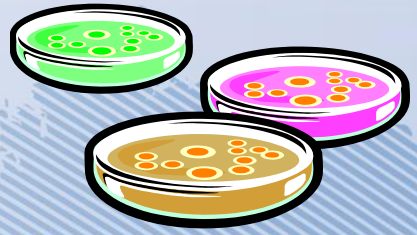
Material Control & Accountability

Key Issues in MC&A

- What materials are subject to MC&A measures?
- What operating procedures are associated with the materials?
  - Where can they be stored and used?
  - How are they identified?
  - How is inventory maintained?
- What records need to be kept for those materials? What timeliness requirements are necessary for those records?
- What does accountability mean?
- What documentation and reporting requirements?

Material Control & Accountability

Material Control & Accountability



What information should we keep track of?

Agent	Quantity	Form	Detail	Scope
Which agents?	Any amount of a replicating organism can be significant.	Repository Stocks, Working Samples, yes…	Materials as Items	Laboratory Strains? Wild-type?
Only viable organisms? Whole org. or just DNA?	For toxins, must define a threshold amount.	What about: In host? Contamination?	Each vial as a separate inventory record?	Clinical Samples?

Material Control & Accountability

Material **Control** & 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 & Accountability

Material Control & **Accountability**

All material should have an associated "accountable person" who is ultimately responsible for the material.

- The person best in a position to answer questions about the associated material
- Not someone to blame!
- Ensure that no material is "orphaned"

MC&A Scenario

Scenario:

3 vials of Equine Encephalitis Virus are reported missing from a high security facility. This virus infects horses, but can be spread to humans through mosquitoes, where it can be deadly in ~1 out of 100 cases. The vials were under the control of a senior scientist who had retired a few years ago and were first identified as missing when a new computer-based inventory system was implemented at the laboratory. The senior scientist thinks that there is a “strong possibility” that the samples were destroyed 8 years ago when one of the freezers in the facility broke down and everything in the freezer had to be destroyed. Unfortunately, a complete inventory of the destroyed samples was never performed. Investigators have not found any evidence of criminal activity.

MC&A Scenario

Group Activity:

In your groups, please spend **10 minutes** to answer the following questions about the scenario.

1. What MC&A-related gaps and/or problems can you identify?
2. How could this have been prevented?
3. What should the role of leadership and/or management be to address these gaps and or problems?

Use your flip charts to design your physical security system and be prepared to report to the class.

Material Control & Accountability

Discussion:

How is Material Control & Accountability implemented in your laboratory?

Biosecurity Risk Mitigation

There are five pillars of Biosecurity Risk Mitigation

1) Physical Security
2) Personnel Management
3) Material Control & Accountability
4) **Transport Security**
5) Information Security

What makes biological materials different?

Transport Security

The fourth "pillar" is Transport Security

Transport Security is the assurance that the same rigorous processes that protect biological materials in the laboratory follow those materials when they are transported outside laboratory areas.

Transport Security

Transport Security

- Aims to reduce the risk of illicit acquisition of *high-risk* biological agents
- Relies on chain of custody principles and end-user agreements

High risk agents are routinely shipped worldwide for diagnostic and research activities

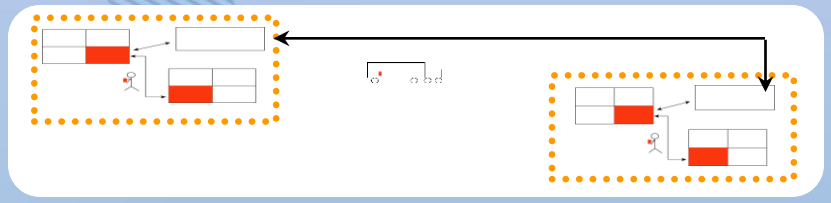
- A local, national, and international concern
- There is a need to develop a common standard, harmonize regulations for security

Transport Security

For example: **Transport**

… is the movement of biological material outside of a restricted area

- Research labs
  - Sample transfers are necessary for study and further research
- Public health labs and diagnostic labs
  - Sample transfers are necessary for diagnosis and analysis



Transport can occur…

- Across international borders
- Within a country
- Within a facility

Transport Security

Internal Transport

- Movement of materials to and from restricted areas **within a facility**
- May involve **Personnel** from
  - Labs
  - Shipping areas
  - Receiving areas
  - Disposal areas (e.g. autoclave and incinerator rooms)
- In order to move materials safely and securely…
  - Pre-approval process
  - Chain of custody

Transport Security

External Transport

- Movement of materials **from one facility to another**
- May involve commercial carriers
- Occurs within a wide array of international and state regulations and standards

Question: When using a commercial carrier (UPS, FedEx) to ship biological materials, at what point should your responsibility for securing the material end?

Transport Security

Chain of Custody (CoC)

Aims to protect sample by documenting…

- All individuals who have control of sample
- Secure receipt of material at appropriate location

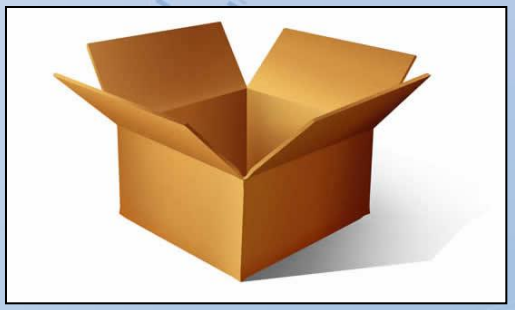
Chain of custody documentation includes…

- Description of material being moved
- Contact information for a responsible person
- Time/date signatures of every person who assumes control

Transport Security

So, we want to keep our high-risk samples secure during transport. What should you do?

- Require a responsible authority to pre-approve all transport
- Advise eligible receiving party of transport
- Document transport in lab records
- Ensure only trustworthy people handle the samples
- Physically secure samples in transit with special packaging and/or locks
- Control movements and document in delivery records
- Use timely shipping methods
- Maintain a Chain of Custody
- Request notification of receipt



Other ideas?

Transport Security

For Example: **When Transporting..**

Moderate risk agents…

- Internal transport personnel screened
- Recipient screened for legitimacy
- Safe receipt notification

High risk agents…

- Moderate plus
  - Chain of custody
  - Physical controls on storage containers

A proper **Risk Assessment** can help determine transport security needs

Transport Security

Group Activity:

Your lab must transport 10 vials of infectious ***Coxiella burnetii*** to a laboratory in another country (i.e., the table clockwise from you).

Spend **15 minutes** to **Develop a Procedure** for securing the sample during transport (including documentation). Then act it out with the receiving lab. (Remember, you'll be receiving samples too!)

Consider how might you apply **Physical Security**, **Personnel Management**, and **Material Control & Accountability** to a sample of valuable biological material on the move?

Transport Security

Discussion:

How are biological materials secured in your laboratory during transport?

Biosecurity Risk Mitigation

There are five pillars of Biosecurity Risk Mitigation

1) Physical Security
2) Personnel Management
3) Material Control & Accountability
4) Transport Security
5) **Information Security**

What makes biological materials different?

Information Security

The fifth "pillar" is **Information Security**

Information Security is the assurance that the **sensitive** and **valuable** information stored in a laboratory is protected from theft or diversion.

Question: What kind of information do you think this might include? Work for **5 minutes** with your group and share your ideas with the class.

Information Security

Information Security may not the most obvious area of biosecurity, but a failure here could have very severe consequences in terms of securing pathogens and toxins.

Document control and **computer security** is necessary to reduce risks in a facility. However, these can also be intrusive. Any policies implemented should be based on a **robust risk assessment**.

Information Security

The Objective of **Information Security** is to:

Protect information that is too sensitive for public distribution

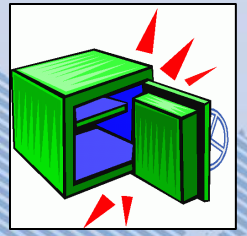
- Label information as restricted
- Limit distribution
- Restrict methods of communication
- Implement network and desktop security

Biosecurity-related sensitive information

- Security of dangerous pathogens and toxins
  - Risk assessments
  - Security system design
- Access authorizations

Information Security

Identification, Control, and Marking



Identification

- Designated sensitivity level
- A review and approval process aids in the identification of sensitivities
  - Critical prior to public release of information

Control

- Individual responsible for control of sensitive information
  - Physical security
  - Communication security
- In the US, in order to refuse public access upon request, information must be exempt from the Freedom of Information Act

Marking

- Sensitivity level designation
  - Top and bottom of each page / cover sheet
- Marking and control methods should be well understood by those working with information

Information Security

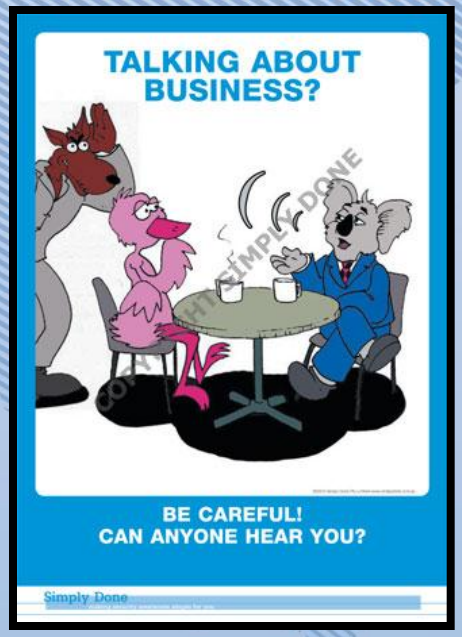
Communication and Network Security

Communication Security

- 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 Security

- Firewalls
- User authentication
- Virus protection
- Layered network access
- Desktop security
- Remote and wireless access controls
  - Encryption
  - Authentication



Information Security

Security Considerations for Network Systems

Administrators have full control
- The ultimate insider

Protect the system using procedures
- Two person control
- Configuration management
- Password control

Restrict operator privileges

Provide physical protection for equipment

Backup equipment and procedures must be provided to maintain security

Emergency power and uninterruptible power supply required for computers

Information Security

Group Activity:

Spend **15 minutes** to **Design an Information Security Policy** for a laboratory working with both a high-risk and a moderate-risk pathogens.

To help with this, think about what we've learned about **physical security** and **graded levels of protection**.

Use your **Flip Charts** to design your **information security policy** and be prepared to report to the class.

Information Security

Discussion:

How is information secured in your laboratory? How can the information security system be improved?

Biosecurity Risk Mitigation

We have discussed each of the five pillars of Biosecurity Risk Mitigation!

1) Physical Security
2) Personnel Management
3) Material Control & Accountability
4) Transport Security
5) Information Security

What makes biological materials different?

Security Awareness

The final topic is **Security Awareness**

Security Awareness is general awareness of the proper security posture in your laboratory, where the risks are, and what should be done.

Security Awareness

For Example: **Security Awareness**

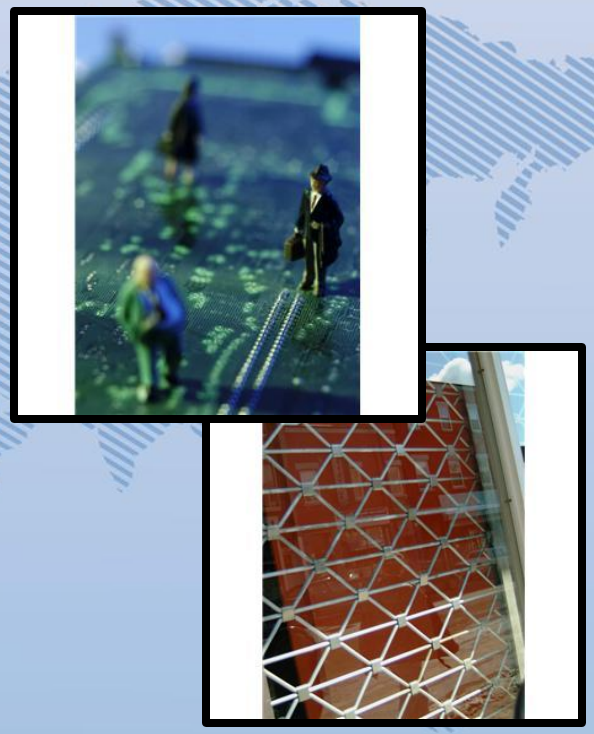
Most bioscience facilities are not accustomed to worrying too much about security, so appropriate security awareness may require a very difficult **cultural shift**.

Security Awareness will be easier to achieve if personnel in your laboratory trust that a **biosecurity risk assessment** is **accurate** and **robust**.

Security Awareness

If the people in your facility are **aware** of **the true biosecurity risks** they face, they will be more likely to:

1) Report if someone strange is walking around
2) Keep an eye on sample storage areas and assign security responsibilities to each other
3) Keep sensitive information safe
4) Provide suggestions for improving security
5) Take training more seriously
6) Etc…



Security Awareness

Question: How might **Security Awareness** tie into the five pillars of biosecurity we have already discussed? Work for **5 minutes** with your group and share your ideas with the class.

1) **Physical Security**
2) **Personnel Management**
3) **Material Control & Accountability**
4) **Transport Security**
5) **Information Security**

Security Awareness

Discussion:

How might you promote a culture of increased security awareness in your facility?

Course Objectives

- A proper biosecurity risk assessment is necessary before implementing an efficient and effective biosecurity program.
- Securing pathogens and toxins can be very different from securing other kinds of materials.
- Physical Security is only one component of a successful laboratory biosecurity program.
- An important component of laboratory biosecurity is Personnel Management.
- Material Control and Accountability, Transport Security, and Information Security complement other security components.
- Security awareness is crucial in laboratory biosecurity.

Thank You!

Don't forget to complete your evaluation!

BIOSECURITY ENGAGEMENT PROGRAM

CBEP
COOPERATIVE BIOLOGICAL ENGAGEMENT PROGRAM

Review

Day 1 Review Activity

What did we learn today? Each table will now summarize the following:

1. Biosecurity Risk Assessment: Why?
2. Unique Challenges in Laboratory Biosecurity: What are they?
3. Physical Security: Why a graded approach?