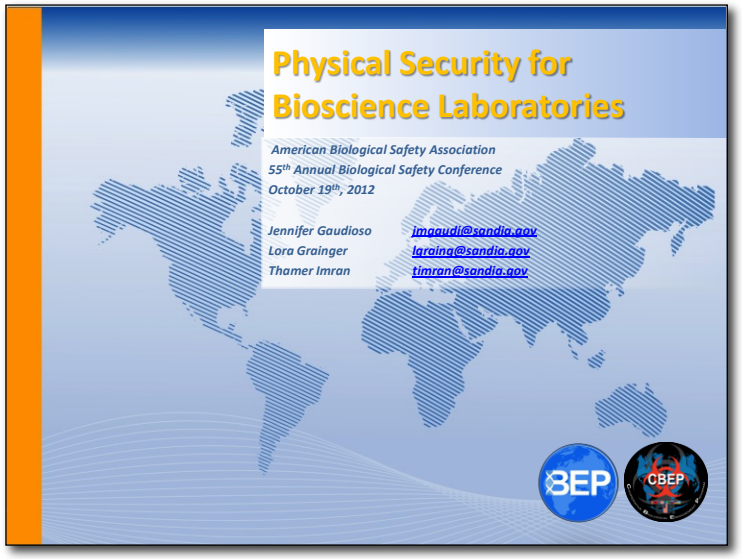
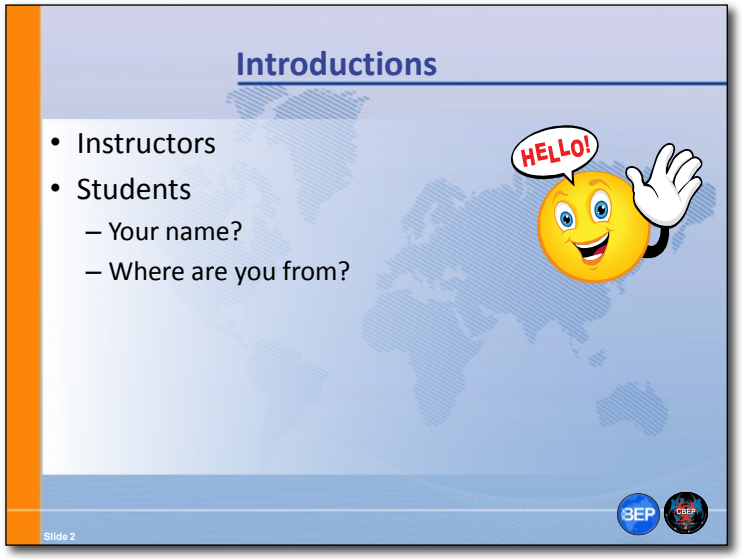
SAND2012-7012P

Physical Security for Bioscience Laboratories

Student Guide



Welcome to Physical Security for Bioscience Laboratories


Introductions
• Instructors
• Students
– Your name?
– Where are you from?
HELLO!
Slide 2

Action Plan

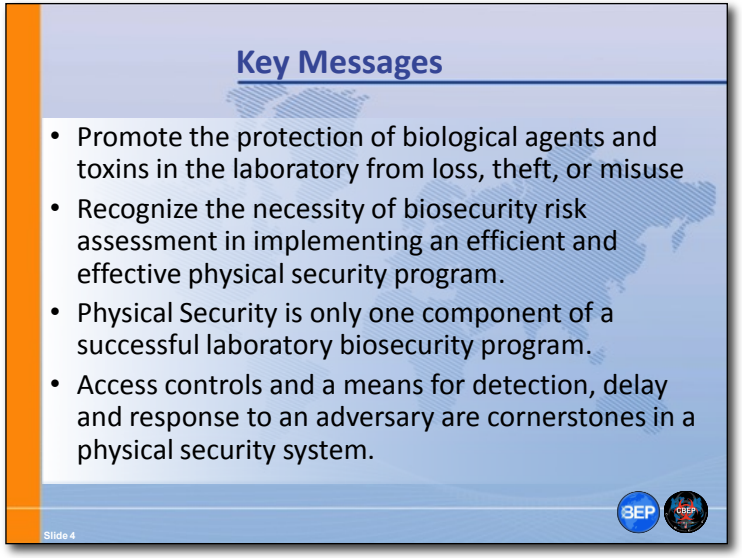
By the end of this lesson, I would like to:					
KNOW		FEEL		BE ABLE TO DO	

Your learning doesn't stop with this lesson. Use this space to think about what else you need to do or learn to put the information from this lesson into practice.

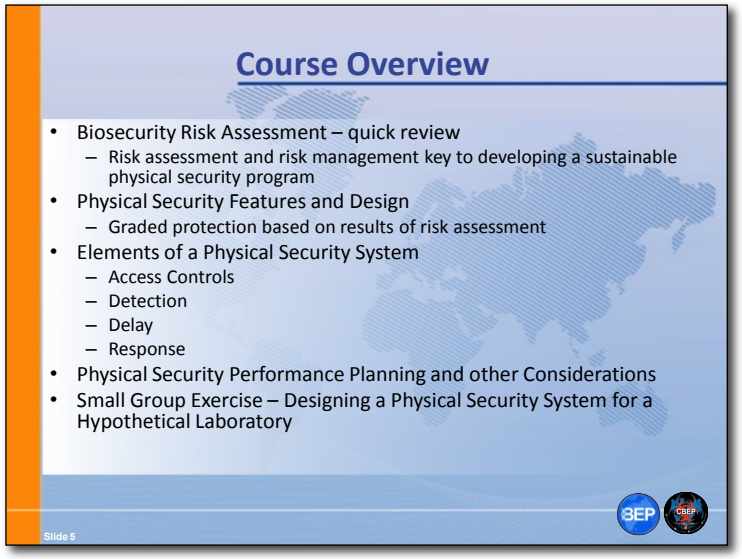
What more do I need to know or do?	How will I acquire the knowledge or skills?	How will I know that I've succeeded?	How will I use this new learning in my job?

Use space on back, if needed

Slide 3

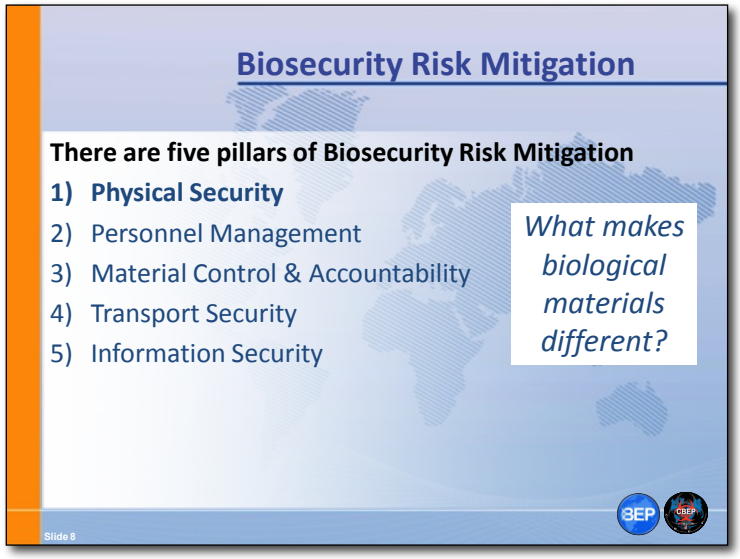

Key Messages
• Promote the protection of biological agents and toxins in the laboratory from loss, theft, or misuse
• Recognize the necessity of biosecurity risk assessment in implementing an efficient and effective physical security program.
• Physical Security is only one component of a successful laboratory biosecurity program.
• Access controls and a means for detection, delay and response to an adversary are cornerstones in a physical security system.
Slide 4

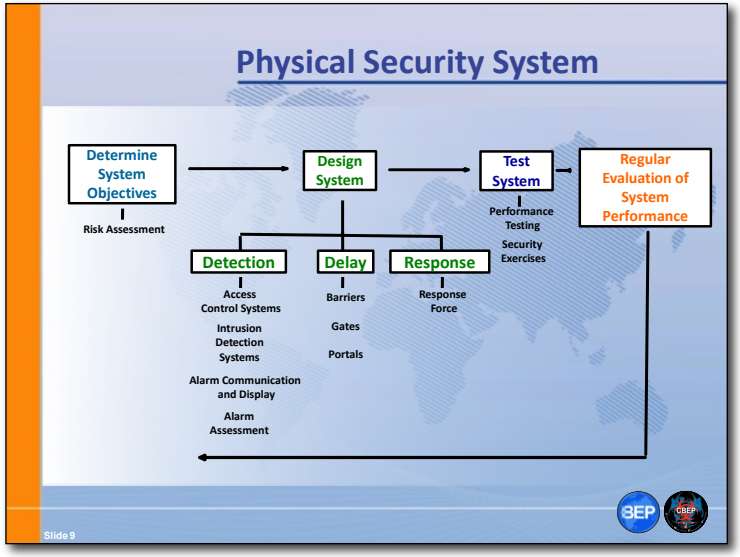
Notes:

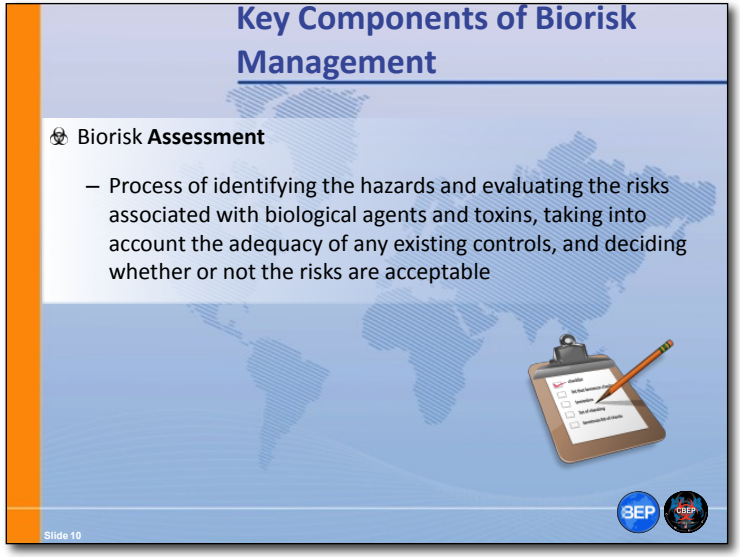

Course Overview
• Biosecurity Risk Assessment – quick review
– Risk assessment and risk management key to developing a sustainable physical security program
• Physical Security Features and Design
– Graded protection based on results of risk assessment
• Elements of a Physical Security System
– Access Controls
– Detection
– Delay
– Response
• Physical Security Performance Planning and other Considerations
• Small Group Exercise – Designing a Physical Security System for a Hypothetical Laboratory
Slide 5

What is Physical Security to you?


Biorisk Management:
The AMP Model
Biorisk Management =
Assessment, Mitigation, Performance
Slide 7

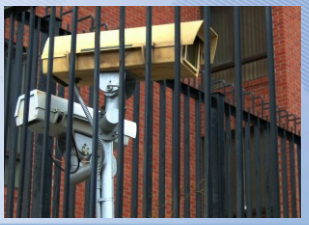

Biosecurity Risk Mitigation
There are five pillars of Biosecurity Risk Mitigation
1) Physical Security
2) Personnel Management
3) Material Control & Accountability
4) Transport Security
5) Information Security
What makes biological materials different?
Slide 8


Physical Security System
Determine System Objectives
Risk Assessment
Design System
Test System
Performance Testing
Security Exercises
Regular Evaluation of System Performance
Detection
Access Control Systems
Intrusion Detection Systems
Alarm Communication and Display
Alarm Assessment
Delay
Barriers
Gates
Portals
Response
Response Force
Slide 9


Key Components of Biorisk Management
Biorisk **Assessment**
– Process of identifying the hazards and evaluating the risks associated with biological agents and toxins, taking into account the adequacy of any existing controls, and deciding whether or not the risks are acceptable
Slide 10

Introduction to Physical Security Risk Assessment

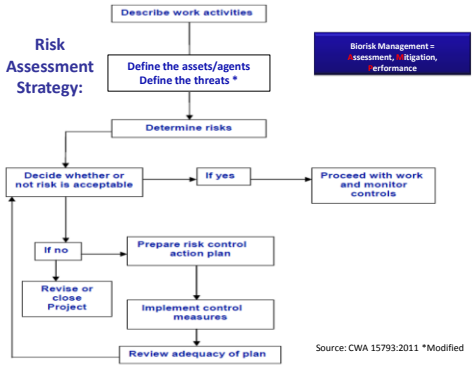
A **biosecurity risk assessment** is an analytical procedure designed to characterize **physical *security*** risks of a laboratory.



Slide 11

Biosecurity Risk Assessment

Risk Assessment Strategy:



Slide 12

Introduction to Physical Security Risk Assessment

A **biosecurity risk assessment** allows an institution or laboratory to determine the relative risk of security threats and/or vulnerabilities to help **guide physical security mitigation decisions** so these are targeted to the most important risk.

Slide 13

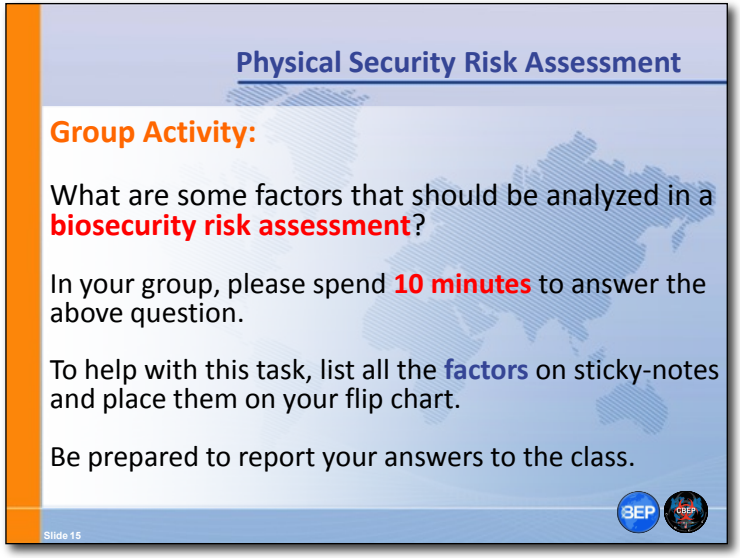
Introduction to Physical Security Risk Assessment

To be comprehensive:

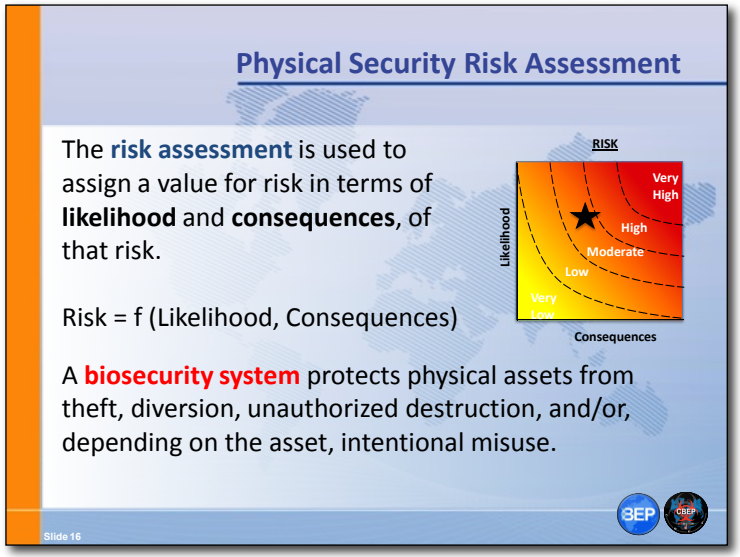
A laboratory **biosecurity risk assessment** should consider every **asset**, **adversary** and **vulnerability** in an institution and its component laboratories and units.

Another useful tool for **physical security risk assessment** is to work through possible **scenarios** to detect any vulnerabilities in the physical security program.

Slide 14



What are some factors that should be considered in a biosecurity risk assessment?


Physical Security Risk Assessment
The risk assessment is used to assign a value for risk in terms of likelihood and consequences, of that risk.
Risk = f (Likelihood, Consequences)
A biosecurity system protects physical assets from theft, diversion, unauthorized destruction, and/or, depending on the asset, intentional misuse.
RISK
Very High
High
Moderate
Low
Very Low
Likelihood
Consequences
Slide 16

What is RISK?

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

Slide 17

Physical Security

Physical Security is a combination of measures used to protect laboratories and their assets from unauthorized access or malevolent actions.

Slide 18

Physical Security

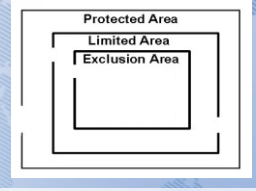
Graded Protection

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

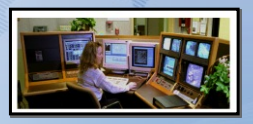


Question:
What are the advantages of this approach?

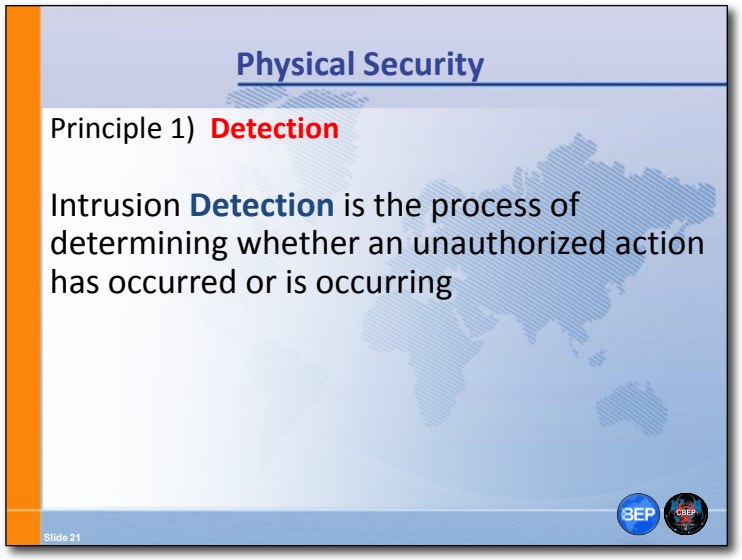
Slide 19

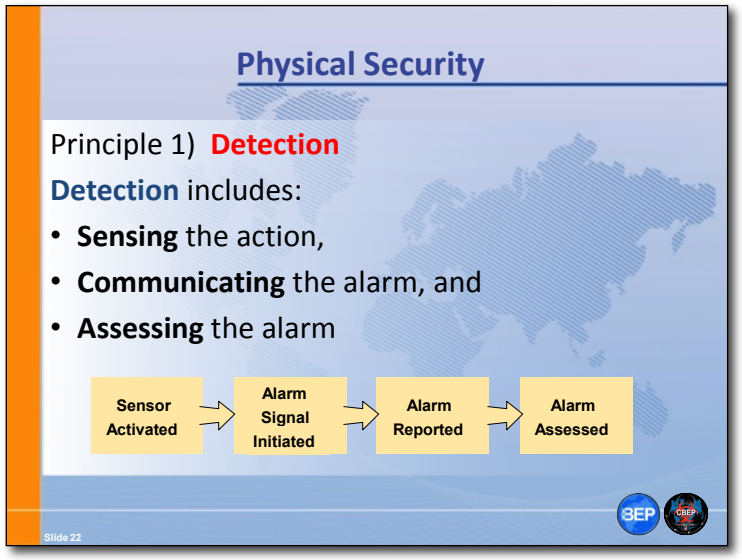
Physical Security

3 Principles of Physical Security:
- **Detection**
  - **Access Controls**
- **Delay**
- **Response**



Slide 20


Physical Security
Principle 1) Detection
Intrusion Detection is the process of determining whether an unauthorized action has occurred or is occurring
Slide 21


Physical Security
Principle 1) Detection
Detection includes:
• Sensing the action,
• Communicating the alarm, and
• Assessing the alarm
Sensor Activated
Alarm Signal Initiated
Alarm Reported
Alarm Assessed
Slide 22

Physical Security

Principle 1) **Detection**

Intrusion detection may be implemented using a range of tools and approaches:

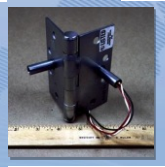
- Intrusion detection sensors
- Audible or visible alarms
- Closed circuit television (CCTV) video cameras and display stations
- Guards
- Properly trained laboratory staff

Slide 23

For Example: Balanced Magnetic Switches

Balanced magnetic switch

Complex balanced magnetic switch



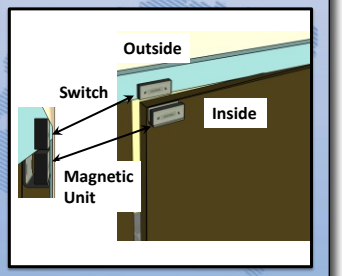
Covert magnetic switch

Slide 24

24

For Example: Balanced Magnetic Switches

- An internal magnet and reed switches are usually mounted on the door/window frame and a balancing (or external) magnet is mounted on the moveable door/window.
- An alarm condition occurs when a change in the magnetic field between the parts is detected.

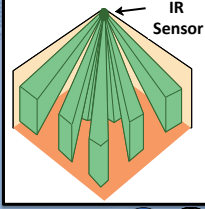


Slide 25 25

For Example: Interior Intrusion Detection

- Microwave
  - Most sensitive to movement toward or away from sensor
  - Nuisance alarms include: movement of metallic objects, fluorescent lighting, insects, movement outside of room
- Passive infrared
  - Most sensitive across field of view
  - Nuisance alarms include: heaters, thermal gradients, animals, sunlight, vibrations
- Limited applications in bioscience facilities:
  - Most appropriate for low use, high risk areas
    - E.g. Storage area for culture collection with very high risk pathogens

Microwave sensor



Slide 26 26

Physical Security

Access Control

Access Control is the mechanism used to determine and control authorized entry into and exit from secured areas.

Access Control:

- **Allows** entry and exit of **authorized** persons.
- **Prevents** entry of **unauthorized** persons.

Slide 27

Physical Security

Access Control

Authenticate authorized personnel based on:

- **Something you have**
  - Key
  - Card (Credential)
- **Something you know**
  - Personal Identification Number (PIN)
  - Password
- **Something you are**
  - Biometric feature (i.e., fingerprints)

Slide 28

Physical Security

Access Control

Combining access control requirements may be used to increase security

Slide 29

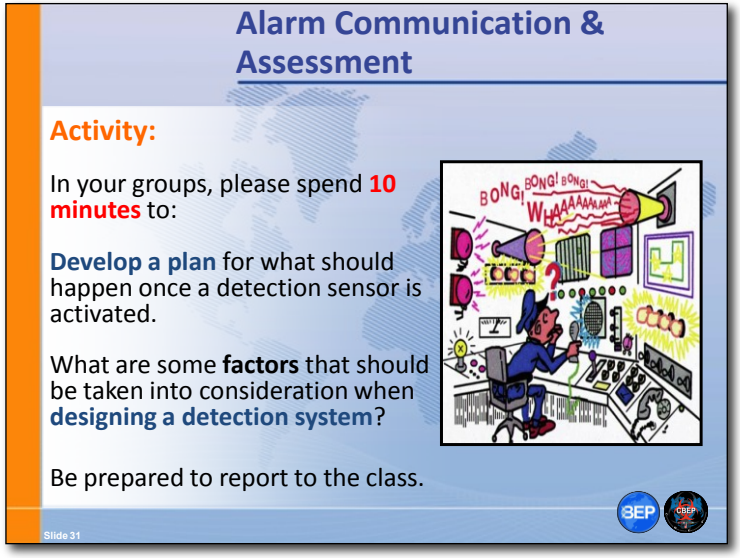
Physical Security

Access Control Systems

- Can be low or high tech
- Give varying levels of assurance of person's identity
  - Risk assessment!
- Have error rates and enrollment issues
  - 1-3% of the population is incompatible with any biometric device
  - Must have secondary method for those who cannot pass automated inspection
- Needs to accommodate peak loads
- Should be designed for both entry and exit

Slide 30

30



What is your plan for when a detection sensor is activated?

What are some factors that should be considered when designing a detection system?

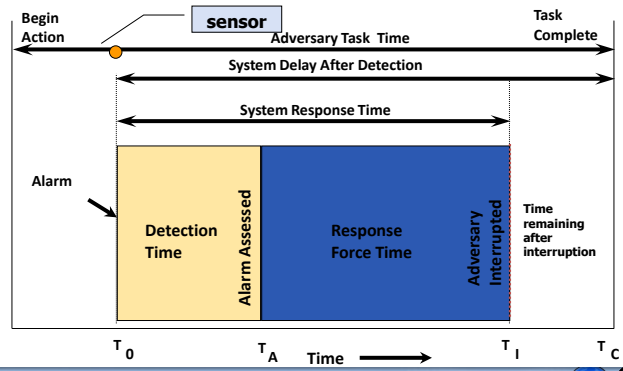
Physical Security

Principle 2) **Delay**

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

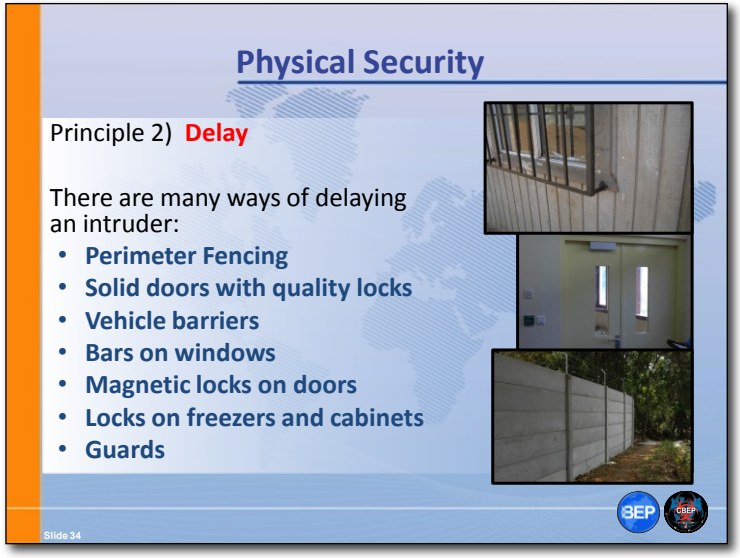
Slide 32

For Example: Adversary Time vs. Response Time



Slide 33

33



What are some other examples of DELAY?

Physical Security

Principle 3) **Response**

Response is the process of alerting, transporting, and staging a security force to interrupt or neutralize an adversary, before the adversary can accomplish their objective.

Slide 35

Physical Security

Principle 3) **Response**

Response is based on a **risk assessment**.

Options include:

- Implementing a **guard force** in the facility.
- Establishing a line of communication with a local **police force**.

What are some **factors** to consider when **implementing a response plan?**

Slide 36

Key Components of Biorisk Management

Performance

– The implementation of the entire biorisk management system, including evaluating and ensuring that the system is working the way it was designed. Another aspect of performance is the process of continually improving the system.

Slide 37

Physical Security Performance

- **Maintenance** – regularly scheduled by trained professionals to verify operation.
- **Physical Inspection** – ensure connections, power levels and manufacturer recommendations
- **Performance Test** – Overall systems tests, which include not just tests on the functioning of mechanical components but also security drills for personnel, can provide information as to the functioning state of a system. Review of alarm record including nuisance alarms.

Slide 38

Physical Security Plans

A **Physical Security Plan** should be developed at the institutional level and incorporate all of the physical security measures to be employed in a particular facility.

Decisions should be made based on a **risk assessment**, as well as on the **effectiveness, cost, and availability** of different mitigation measures. It should also be revised periodically based on **changing risks, resources**, and other circumstances.

Slide 39

Potential Conflicts Between Biosafety and Biosecurity

- Emergency alarm – electronic locks
  - Safety – doors fail open
  - Security – doors fail secure
- Emergency egress
  - Safety – move people into the safest location as quickly as possible
  - Security – prevent people from moving into or through restricted areas
- Keys required inside laboratory areas
  - Safety – contamination concern
  - Security – multiple layers of access

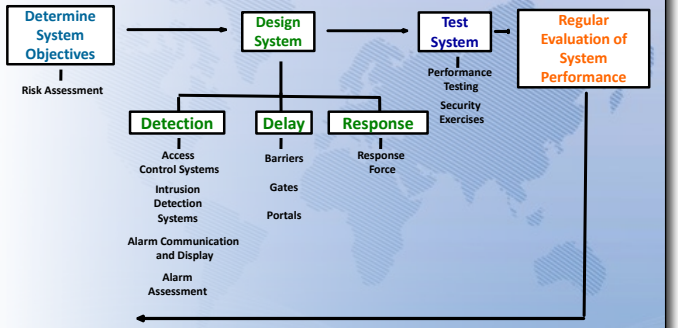
Slide 40

Conclusions

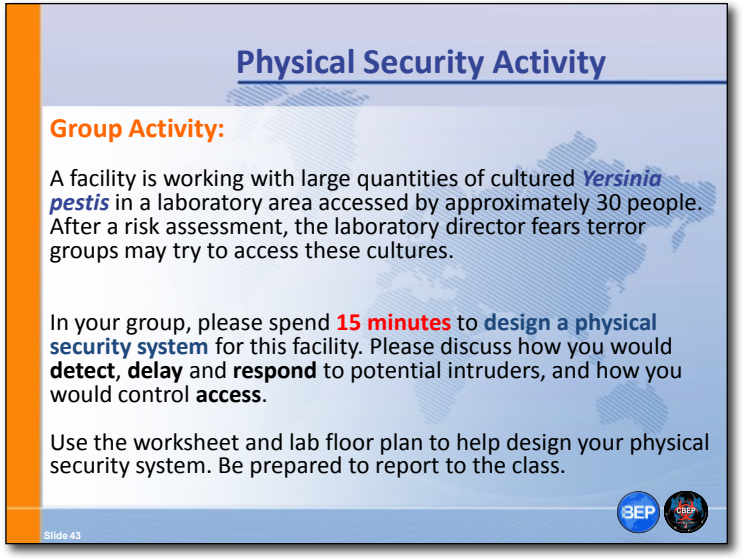
- Physical security systems will vary based on:
  - Resources
  - Choice of technology
  - Security system strategy
    - Physical security is more substantive for deny or contain than deter
  - Risk Assessment!
- Physical security systems should be performance based
  - Low and higher technology options
- **Must consider unique aspects and requirements of bioscience laboratories**

Slide 41

Physical Security System



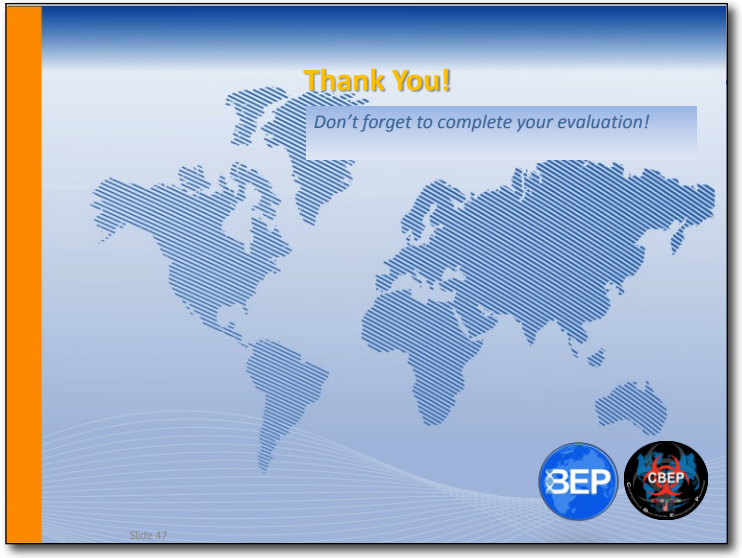
Slide 42


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 the worksheet and lab floor plan to help design your physical security system. Be prepared to report to the class.
Slide 43

Notes:


Review
Review
For 10 minutes, let's discuss what we have learned about Physical Security.
What did we learn?
What does it mean?
Where do we go from here?
Slide 44

Notes:


Thank You!
Don't forget to complete your evaluation!
BEP
CBEP
Slide 47