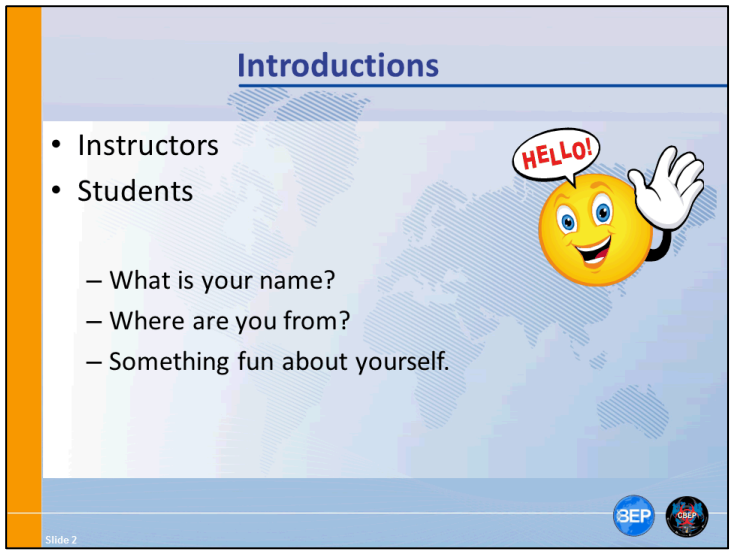
SAND2013-1724P

Laboratory and Field Biosecurity

Student Guide

Welcome to Laboratory Biosecurity


Introductions
• Instructors
• Students
– What is your name?
– Where are you from?
– Something fun about yourself.
HELLO!
Slide 2

Notes:

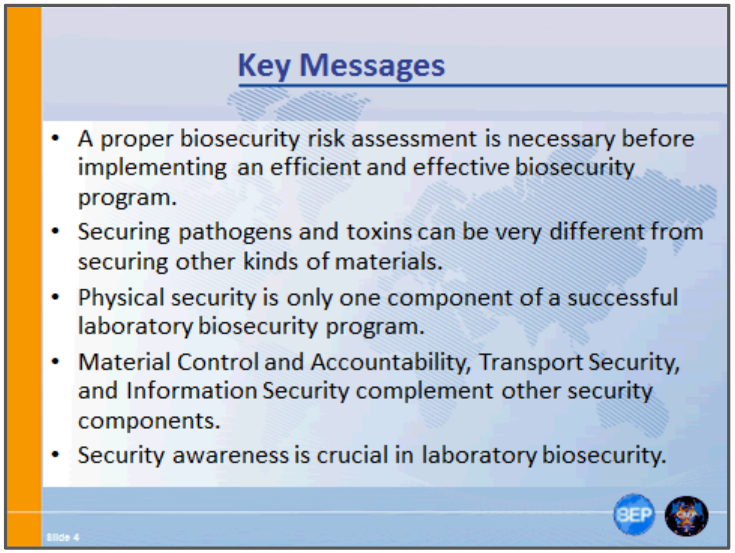
Action Plan

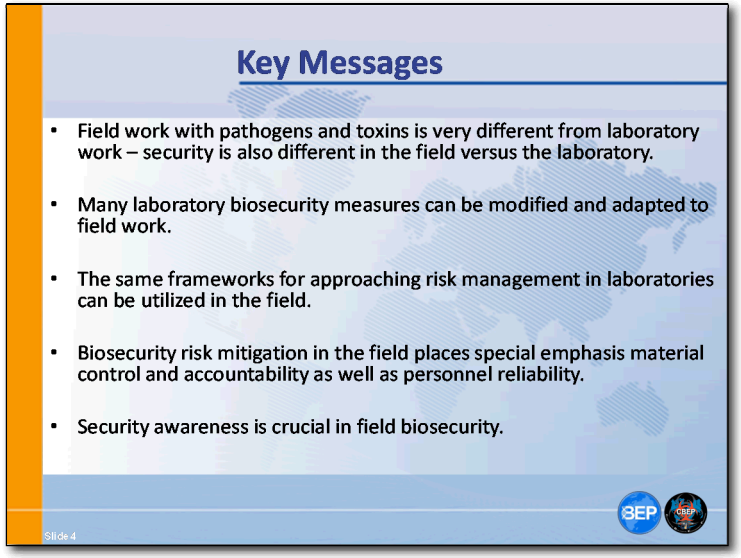
By the end of this lesson, I would like to:					
KNOW		FEEL		BE ABLE TO DO	

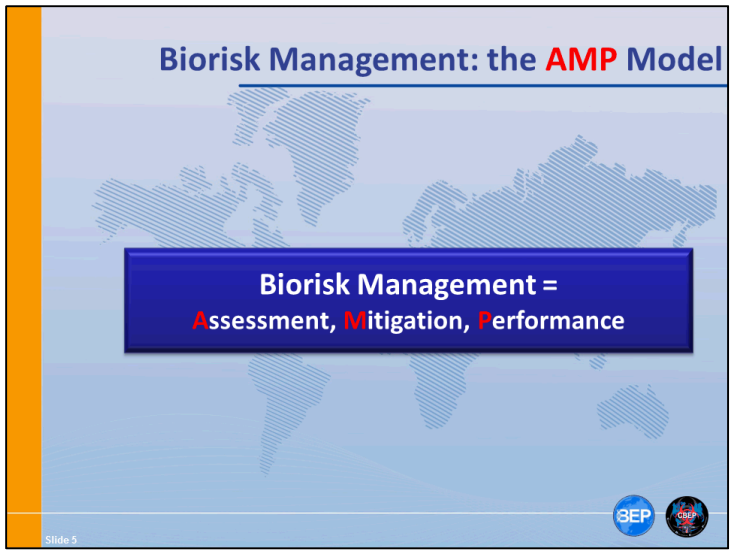
Your learning doesn't stop with this lesson. Use this space to think about what else you need to do or learn to put the information from this lesson into practice.

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?

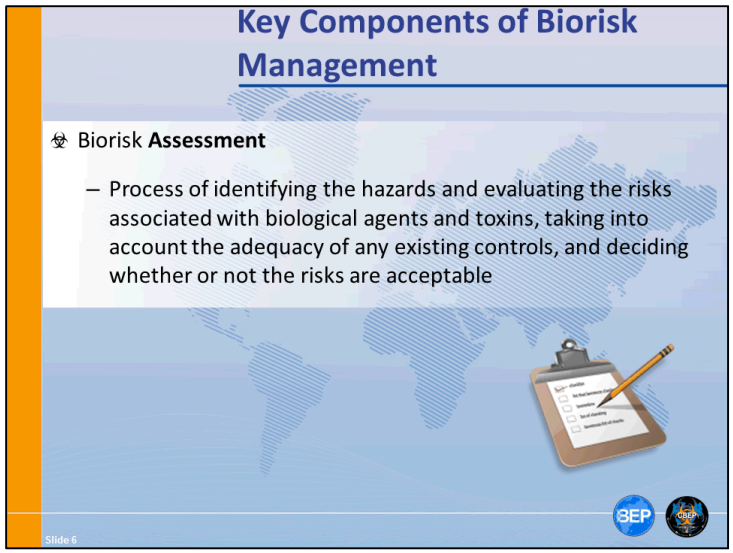
Slide 3


Key Messages
• 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.
Slide 4


Key Messages
• Field work with pathogens and toxins is very different from laboratory work – security is also different in the field versus the laboratory.
• Many laboratory biosecurity measures can be modified and adapted to field work.
• The same frameworks for approaching risk management in laboratories can be utilized in the field.
• Biosecurity risk mitigation in the field places special emphasis material control and accountability as well as personnel reliability.
• Security awareness is crucial in field biosecurity.
Slide 4

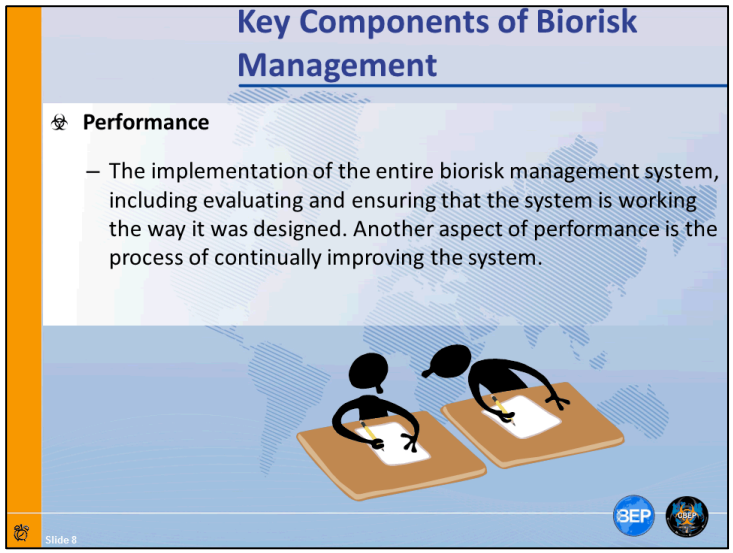


Record refresher notes on the AMP model and biorisk management.



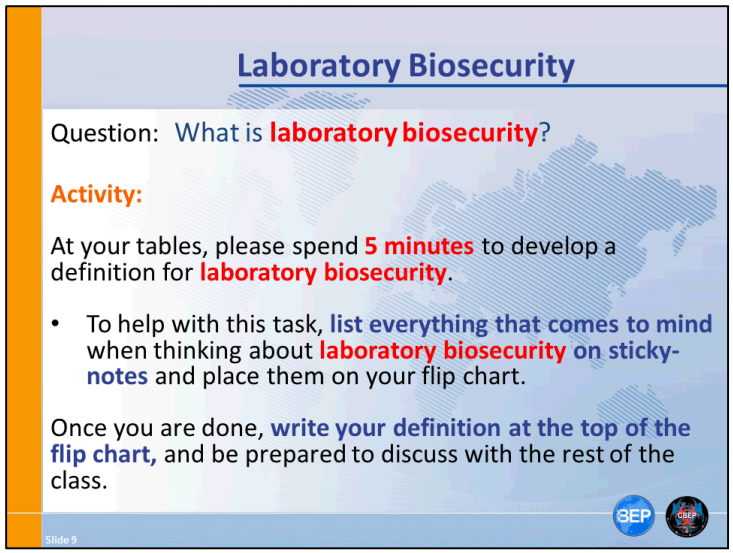
Define Biorisk Assessment:

Define Biorisk Mitigation:



Define Performance:

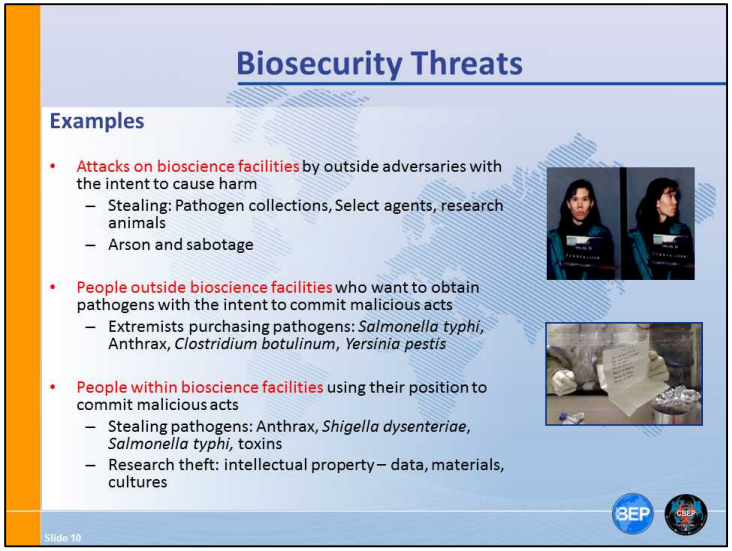
Laboratory Biosecurity



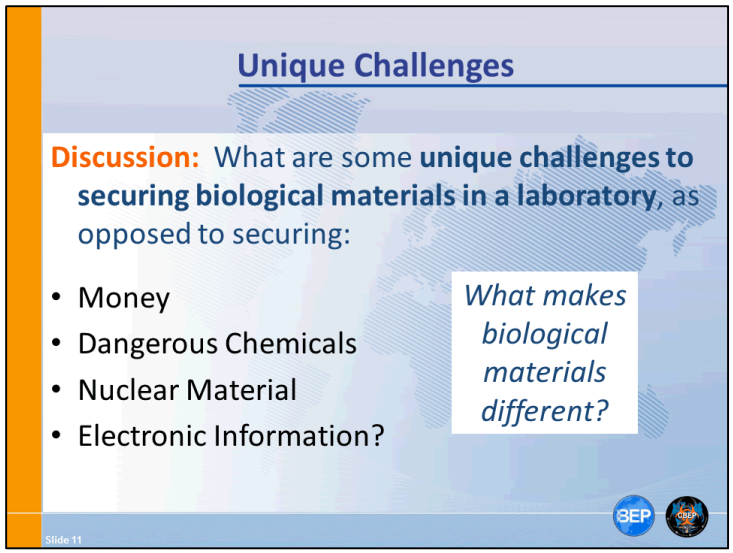
What is Laboratory Biosecurity?

What are some things that come to mind when thinking about laboratory biosecurity?

Laboratory Biosecurity



Notes:



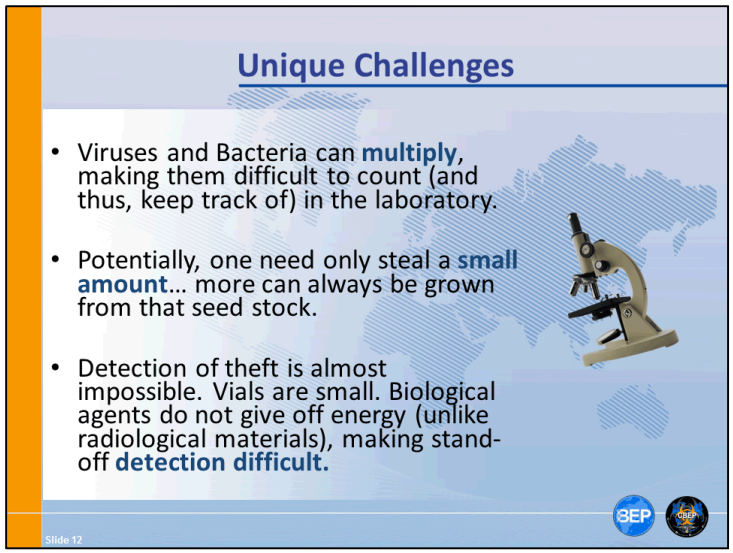
Biological materials pose some challenges with regard to security. How is security for biological materials different than securing:

Money

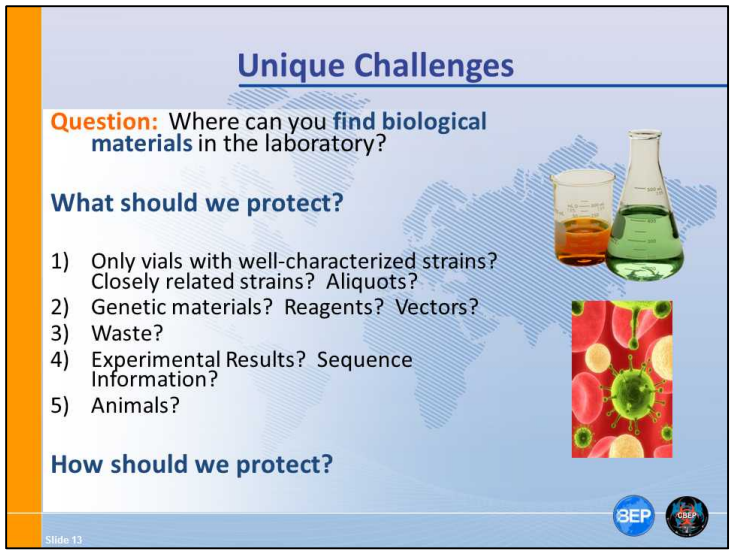
Dangerous Chemicals

Nuclear Material

Electronic Information



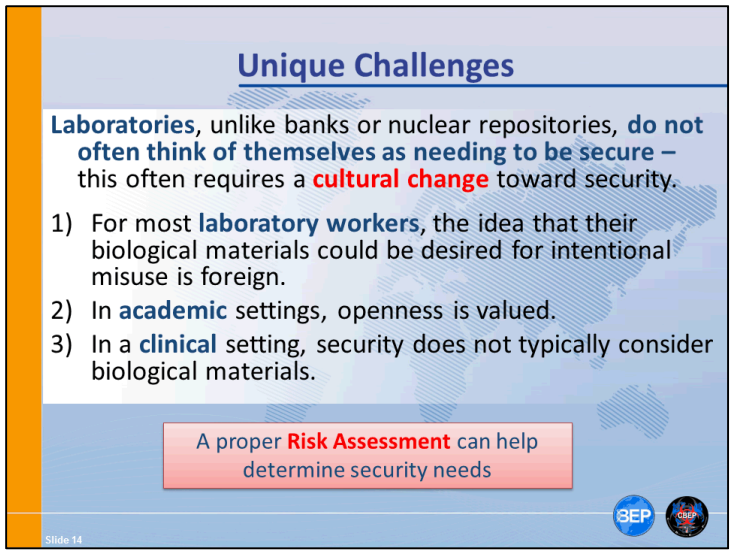
What other complications do biological materials present?



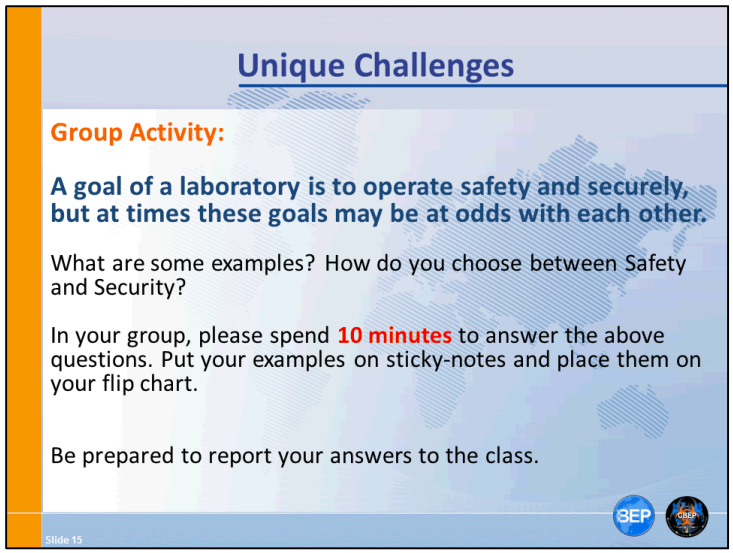
Where can you find biological materials in the laboratory?

What should we protect?

How should we protect?



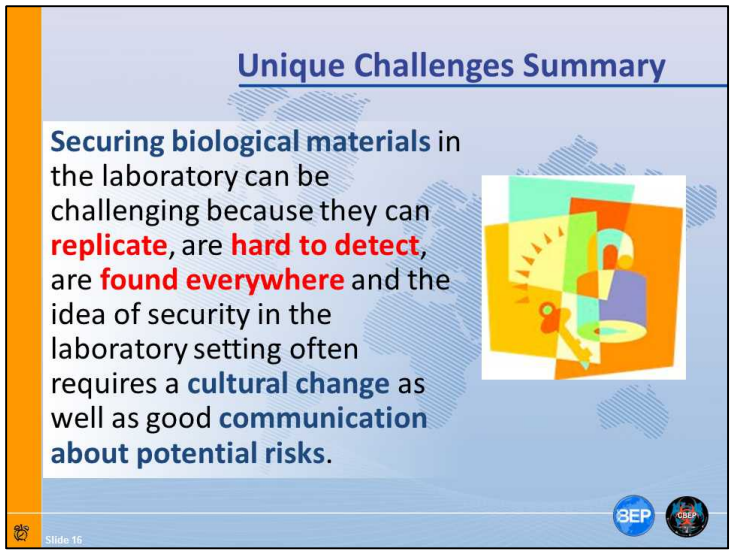
What would be involved in creating a cultural shift toward biosecurity in the laboratory?

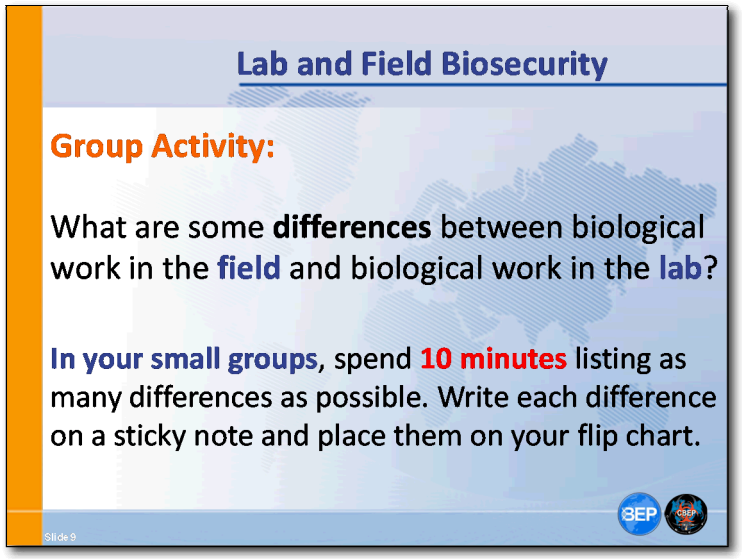


What are some examples when the goals of biosafety and biosecurity might be different?

What are some examples?

How do you choose between Safety and Security?


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.
Slide 16

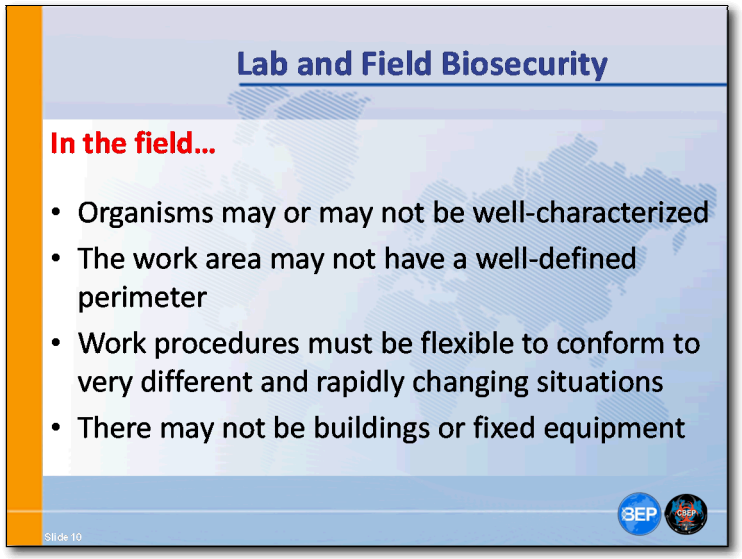


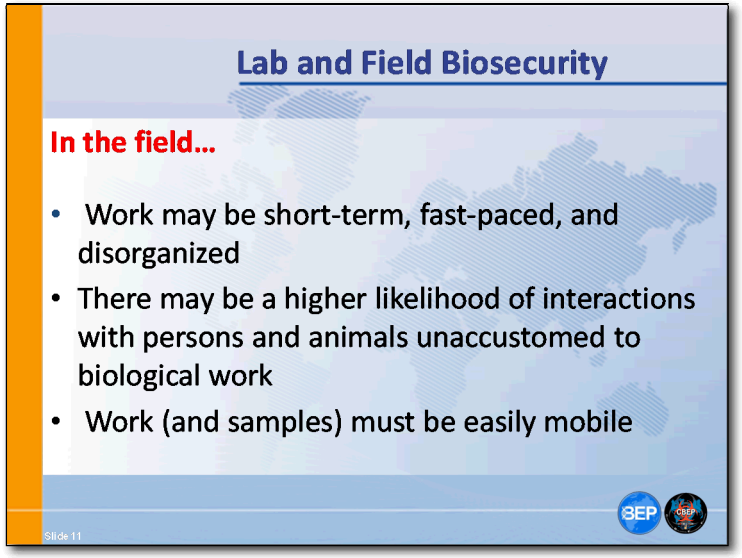
What are some differences between biological work in the field and biological work in the lab?

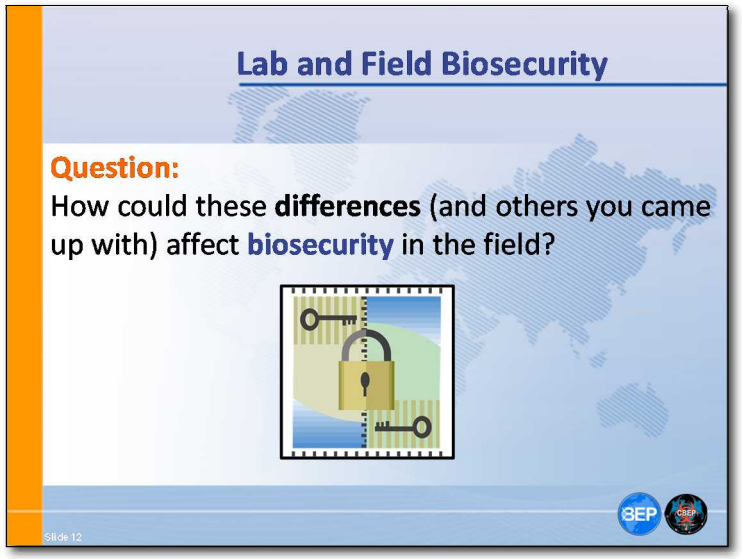
Are the conditions more mutable in the lab or the field?

Which of these unpredictable conditions might concern you?

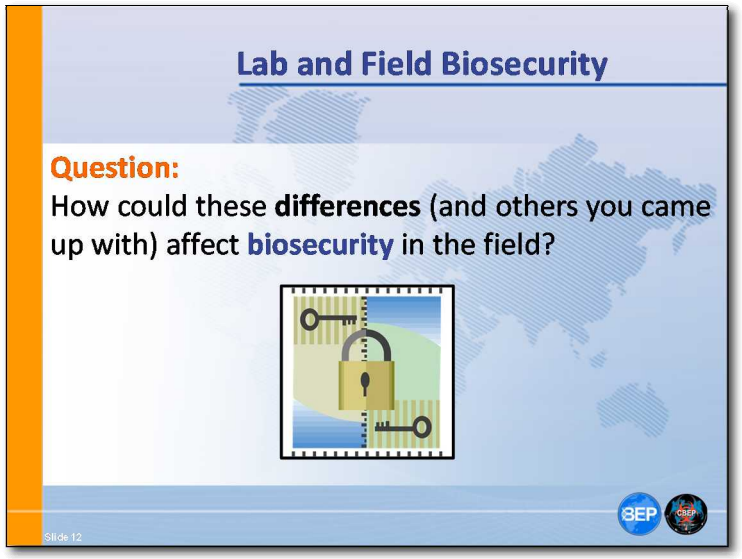
How may this present a challenge to Biosecurity?


Lab and Field Biosecurity
In the field…
• Organisms may or may not be well-characterized
• The work area may not have a well-defined perimeter
• Work procedures must be flexible to conform to very different and rapidly changing situations
• There may not be buildings or fixed equipment
Slide 10


Lab and Field Biosecurity
In the field…
• Work may be short-term, fast-paced, and disorganized
• There may be a higher likelihood of interactions with persons and animals unaccustomed to biological work
• Work (and samples) must be easily mobile
Slide 11

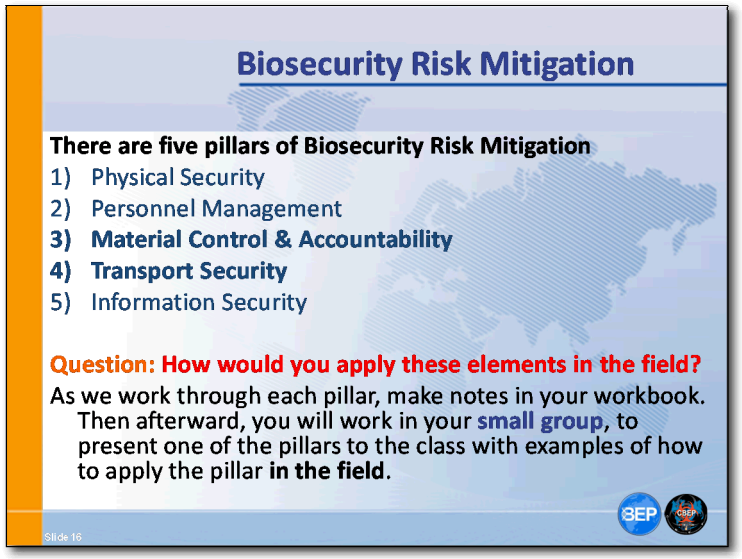


What is unique about field Biosecurity?



What is unique about field Biosecurity?


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


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
Question: How would you apply these elements in the field?
As we work through each pillar, make notes in your workbook. Then afterward, you will work in your small group, to present one of the pillars to the class with examples of how to apply the pillar in the field.
Slide 16

Biosecurity Risk Mitigation – Field Examples

	Physical Security	Personnel Management	Material Control & Accountability	Transport Security	Information Security
Definition					
Examples					

Slide 17

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?

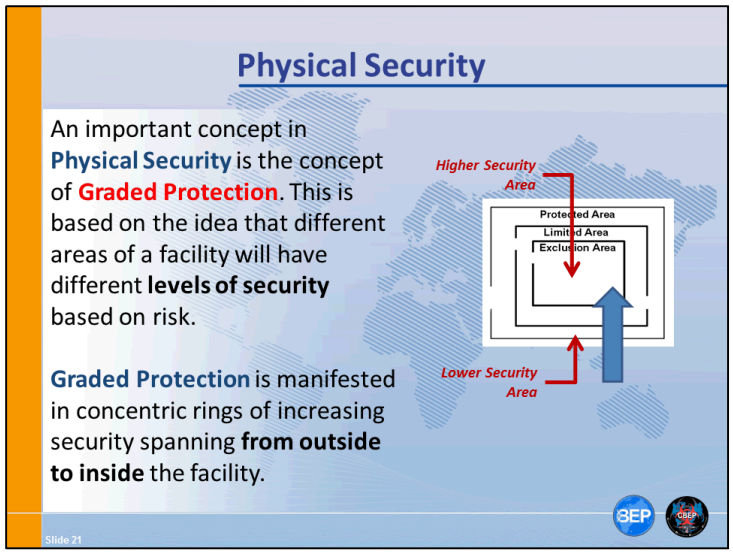
Slide 19

Physical Security

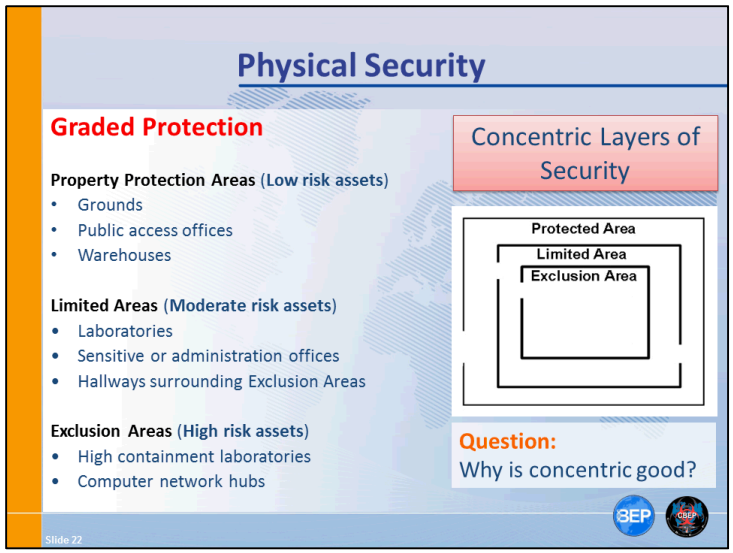
The first "pillar" is **Physical Security**

Physical Security is the assurance of safety from physical intrusion

Slide 20



What are some examples of graded protection?



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.



Slide 23

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

Slide 24

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.

Slide 25

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**

Slide 26

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

Slide 27

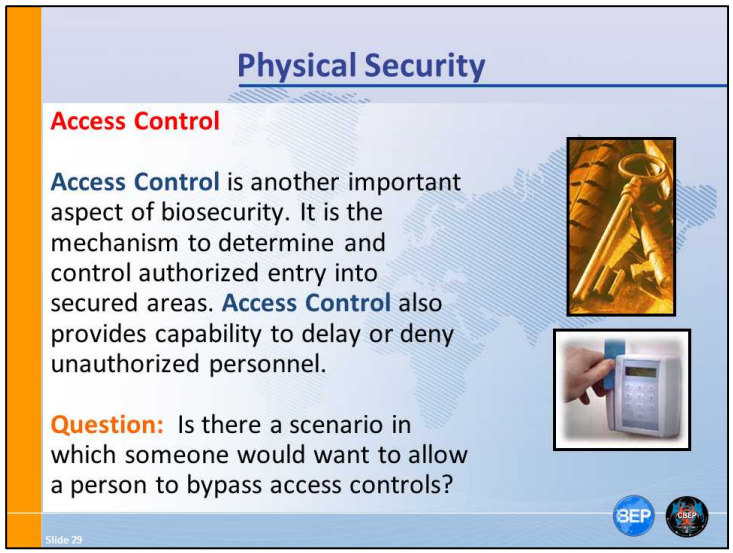
Physical Security

Principle 3) **Response**

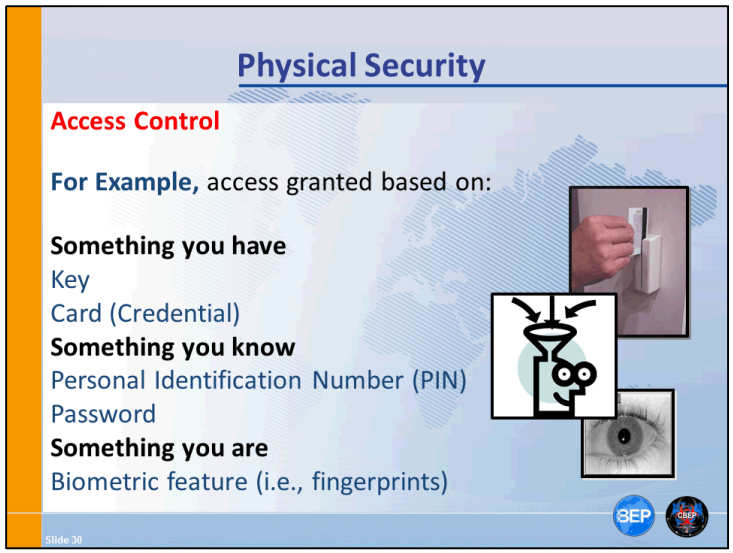
For Example:

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**.

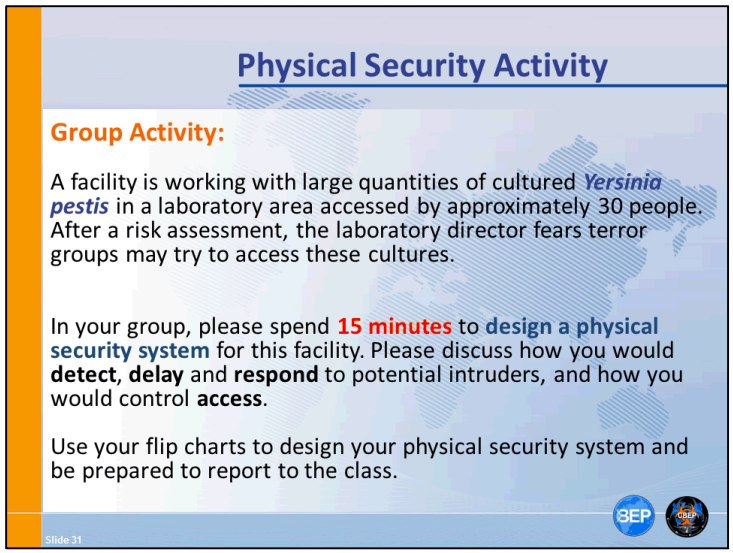
Slide 28



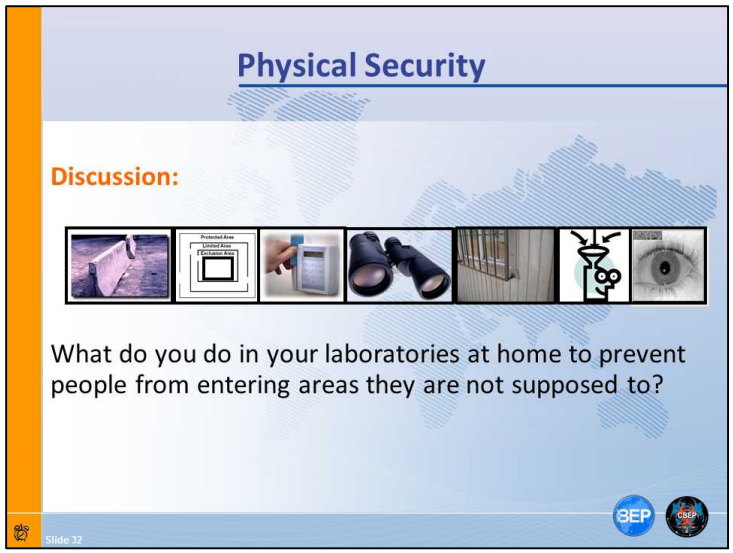
Is there a scenario in which someone would want to allow a person to bypass access controls?


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)
Slide 30

Notes



Plan out your physical security system:


Physical Security
Discussion:
What do you do in your laboratories at home to prevent people from entering areas they are not supposed to?
Slide 32

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 33

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.

Slide 34

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

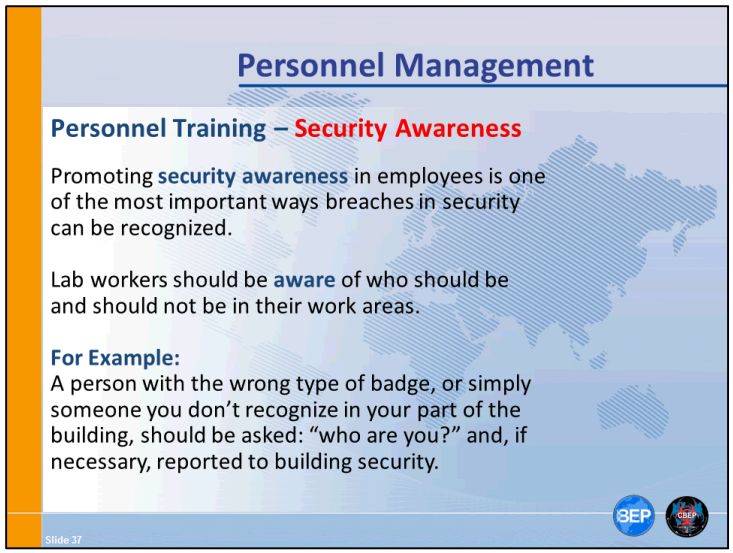
Slide 35

Personnel Management

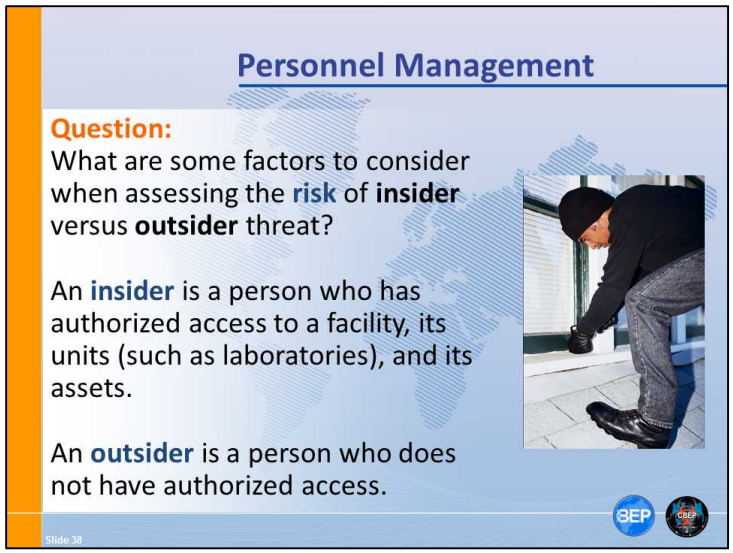
For Example: These are some factors that can influence **Human Performance**

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

Slide 36


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.
Slide 37

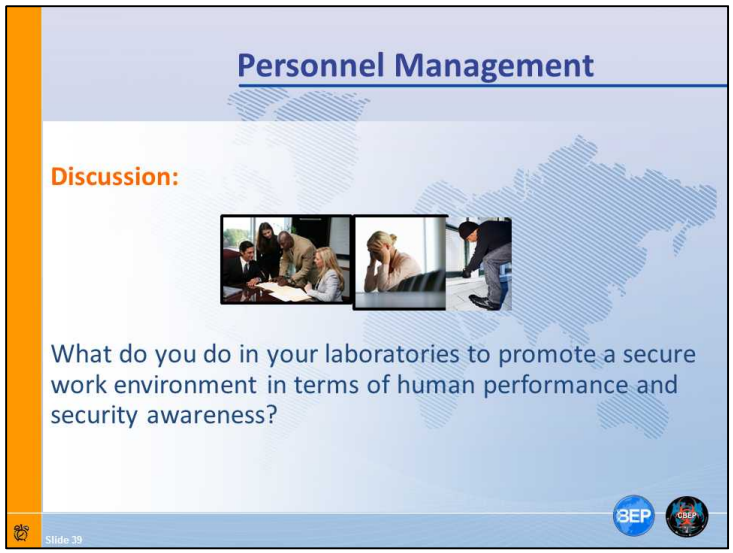
Notes:



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

Insider

Outsider


Personnel Management
Discussion:
What do you do in your laboratories to promote a secure work environment in terms of human performance and security awareness?
Slide 39

Notes:

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

Slide 40

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 field, where it is, and who is responsible for it.

Slide 24

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.

Question: Why might MC&A be *particularly* important for field biosecurity?

Slide 25

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?

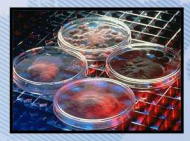
Slide 26


Material Control & Accountability
Material Control & Accountability
Question: What Material should we keep track of in the Field?
Slide 27

Material Control & Accountability

Material **Control** & Accountability

- **Control is either…**
  - Engineered / Physical (Locks)
  - Administrative (Chain of Custody)
- **Containment is part of material control**
  - Containment During Transport / Freezer / Ampoule
- **Procedures are essential for material control**
  - For both normal and abnormal conditions



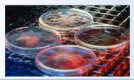
Slide 28

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"



Slide 29

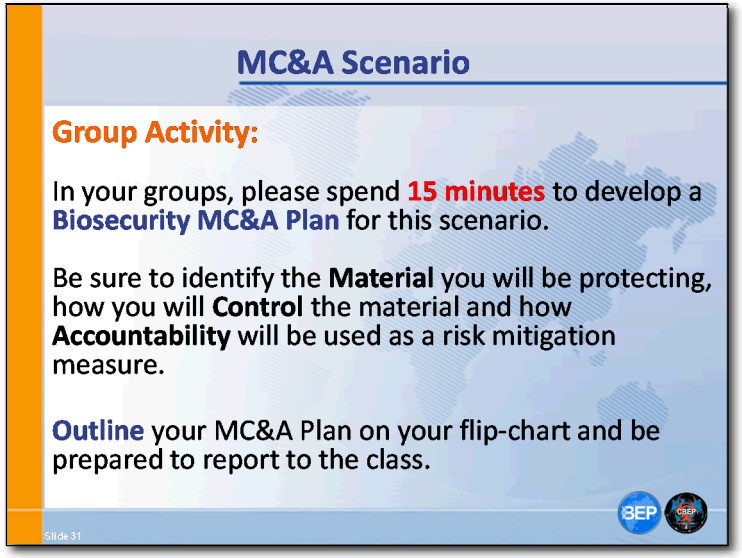
Material Control & Accountability

Scenario:

Your team of 3 researchers and 12 assistants is in the field collecting fleas, ticks and dead rodents at the site of a suspected outbreak of *Yersinia pestis*.

You are working in a remote region, where petty crime is endemic and there has been some civil unrest involving separatist groups with ties to international terrorist organizations. However, your work site is located in an isolated wooded area. Your work area is very large and you have several vehicles and tents in one clearing where you will keep your equipment and plan to store samples. You expect to be in the field 5 days.

Slide 30



Biosecurity MC&A Outline:

Material:

Control:

Accountability:


Material Control & Accountability
Discussion:
How is Material Control & Accountability implemented when you are working in the Field?
Slide 32

Notes:

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?

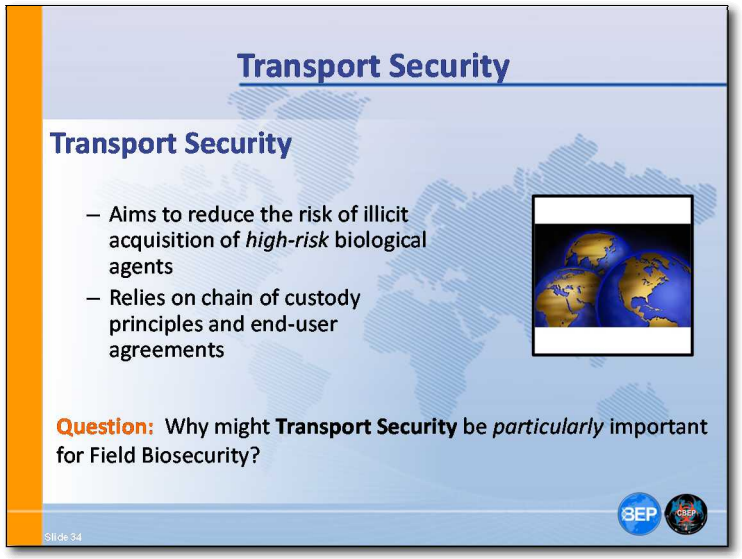
Slide 50

Transport Security

The fourth "pillar" is Transport Security

Field Transport Security is the assurance that risk mitigation controls and processes are in place to protect biological materials during transport from the field to the laboratory.

Slide 33


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
Question: Why might **Transport Security** be *particularly* important for Field Biosecurity?
Slide 34

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

Slide 35

Transport Security

External Carrier

If using an external carrier, the same procedures used for securing materials for transport out of a laboratory should be employed in the field, whenever possible.

Field Personnel

If field personnel will be transporting samples, internal guidelines for doing so, in many ways similar to the requirements for MC&A in the field, should be developed to ensure samples are moved securely.

Slide 36

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?

Slide 37

Transport Security

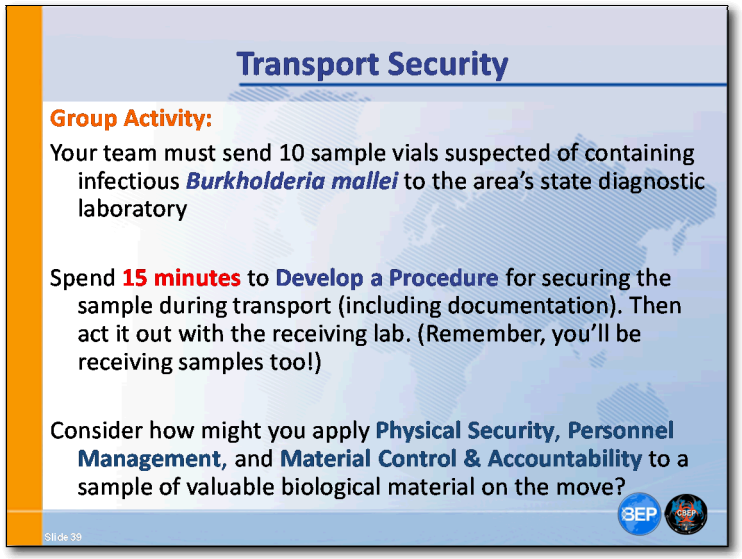
For Example: **When Transporting..**

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

Slide 38

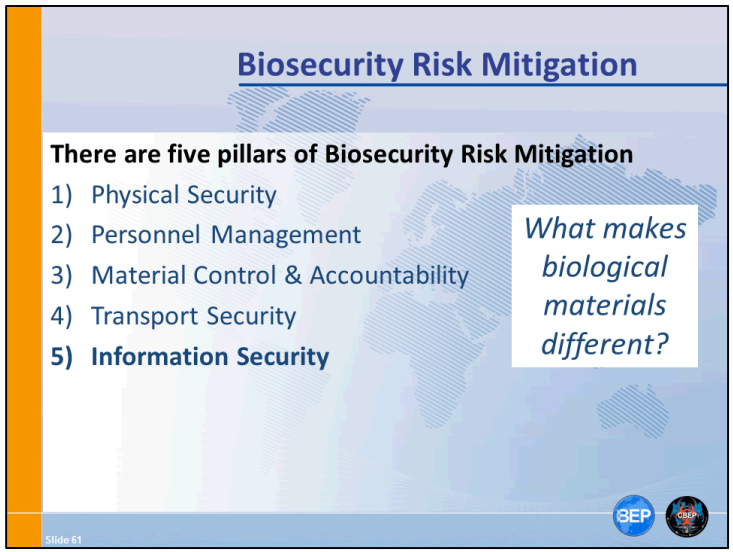


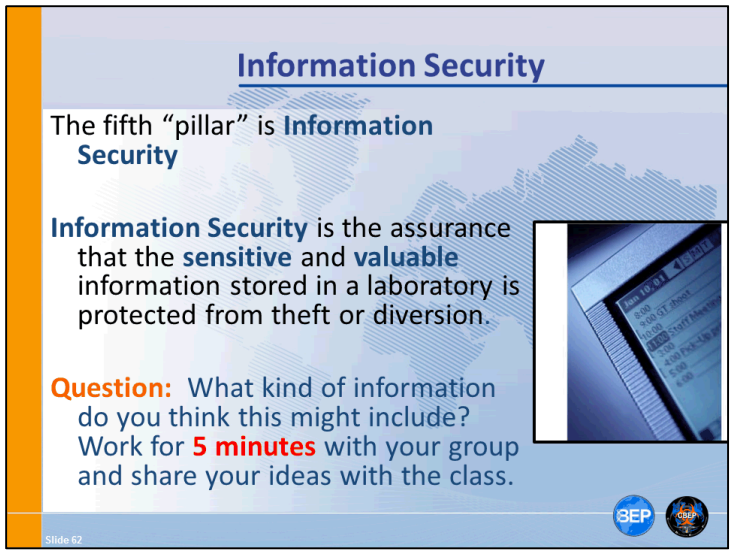
Transport Procedure:

Standard Operating Procedure Pattern

Conditions		
Who should use the SOP?		
When should it be used?		
Why should the SOP be used?		
Where should it be used?		
Context		
Input(s):		
Output:		
Preparation:		
Actions: What steps must be taken to move from the input to the output?		
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Documentation		
Cross-references		
Regulatory dependencies/sources		


Transport Security
Discussion:
How do you secure biological materials in the field during transport?
Slide 40


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 61

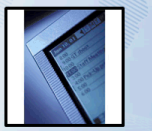


What are some examples of information security?

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**.



Slide 63

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

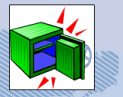
Biosecurity-related sensitive information

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

Slide 64

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

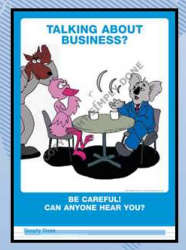
Slide 65

Information Security

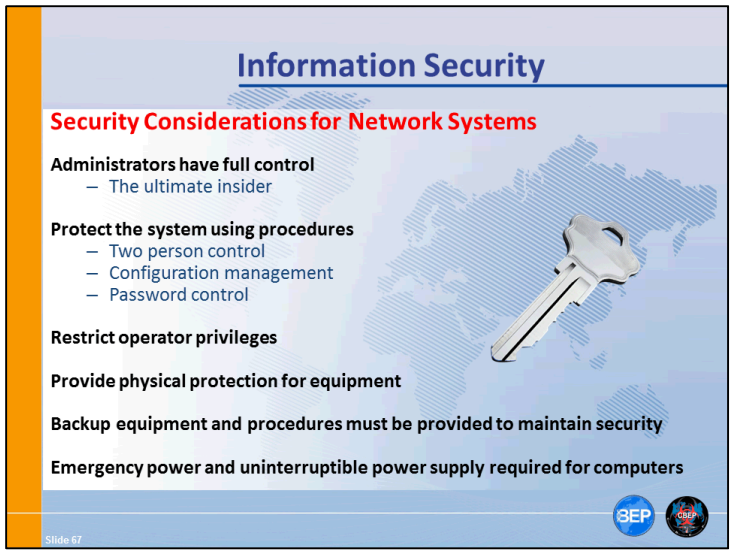
Communication and Network Security

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

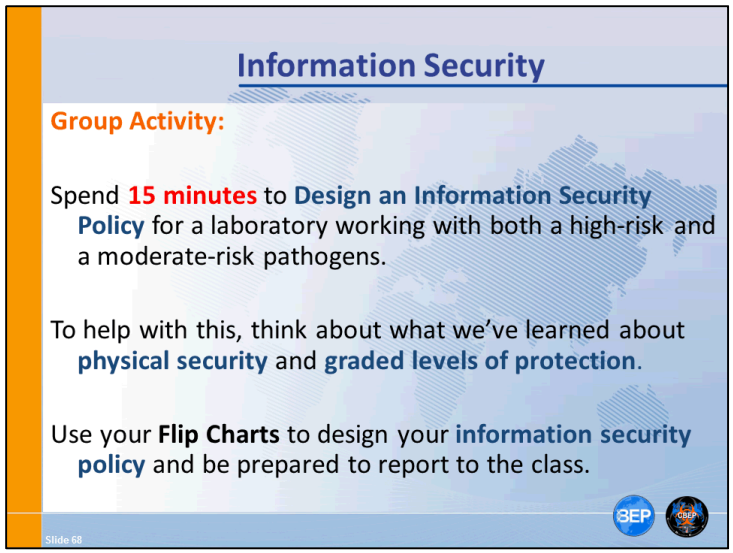
Network Security
- Firewalls
- User authentication
- Virus protection
- Layered network access
- Desktop security
- Remote and wireless access controls
  - Encryption
  - Authentication



Slide 66



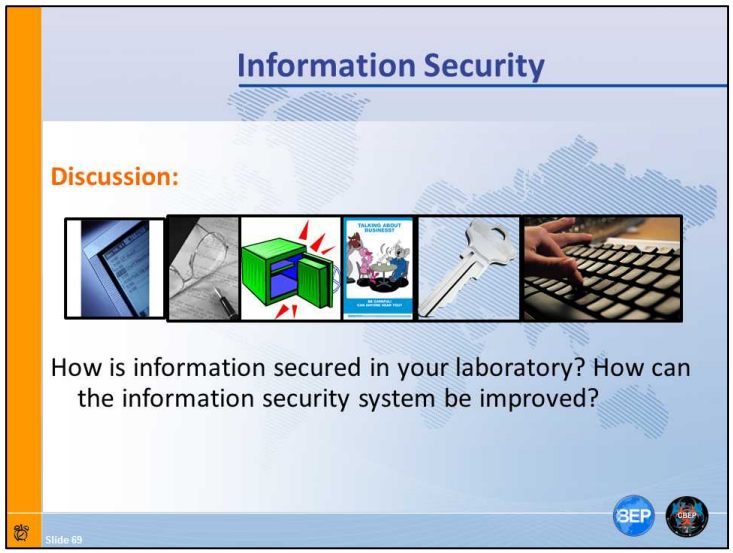
How is network access assigned?



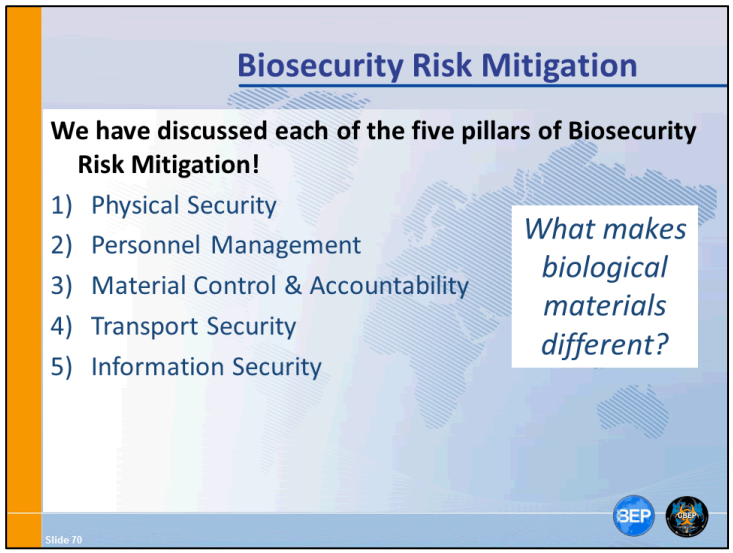
Your Information Security Policy:

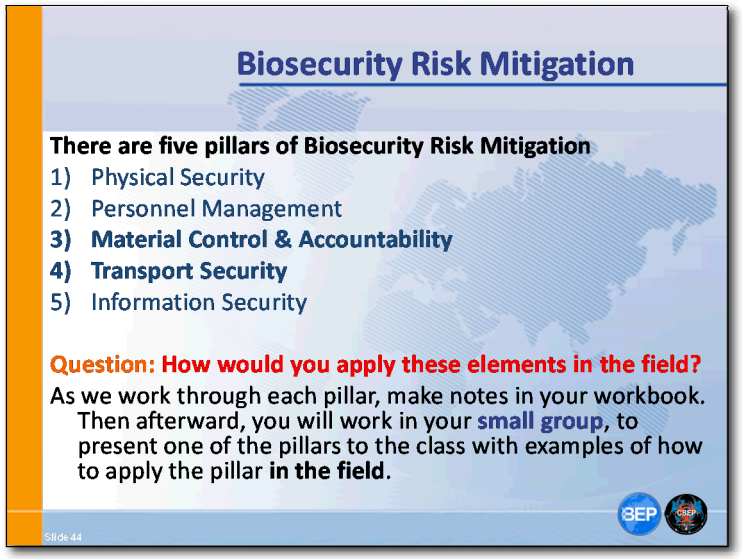
High risk pathogens:

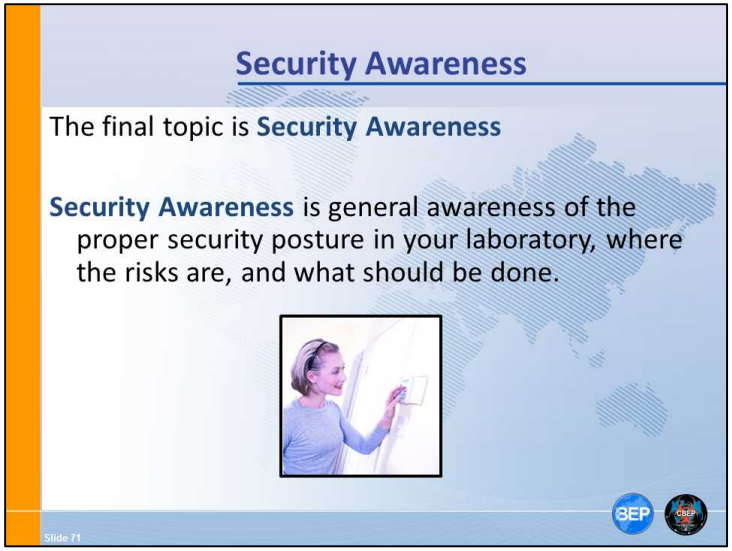
Low risk pathogens:


Information Security
Discussion:
How is information secured in your laboratory? How can the information security system be improved?
Slide 69

Notes:


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?
Slide 70


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
Question: How would you apply these elements in the field?
As we work through each pillar, make notes in your workbook. Then afterward, you will work in your small group, to present one of the pillars to the class with examples of how to apply the pillar in the field.
Slide 44


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.
Slide 71

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**.

Slide 72

Security Awareness

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

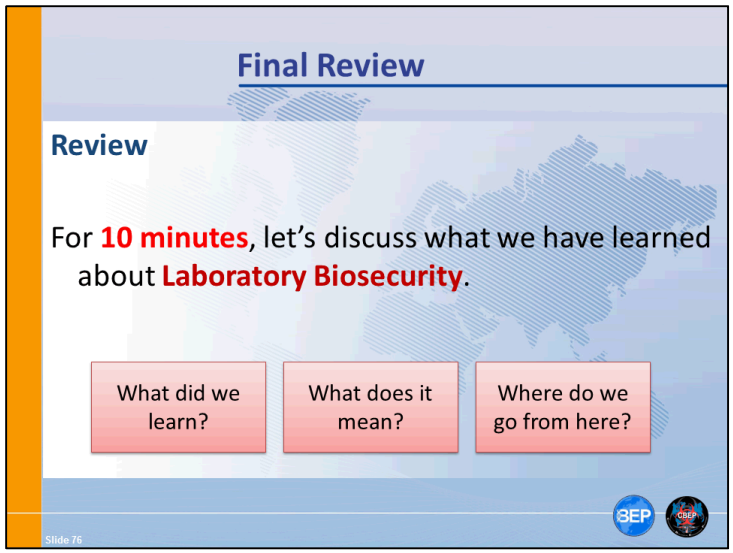
1) Report if someone strange is walking around
2) Keep an eye on sample storage areas and assign security responsibilities to each other
3) Keep sensitive information safe
4) Provide suggestions for improving security
5) Take training more seriously
6) Etc…

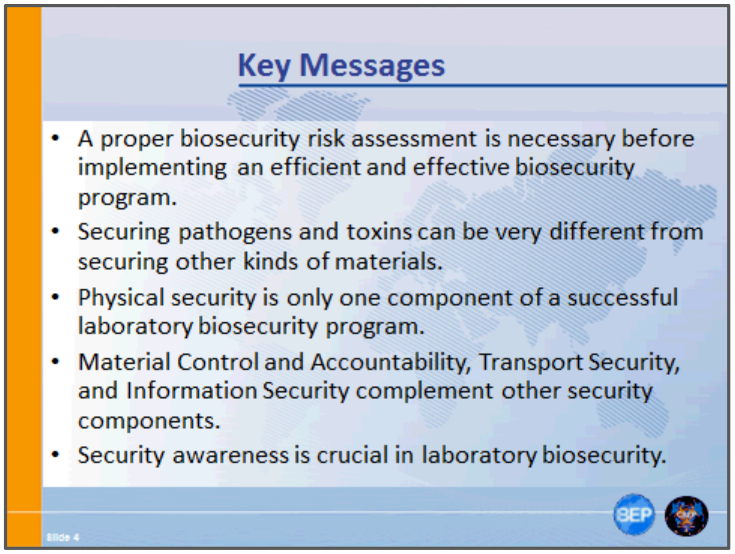
Slide 73

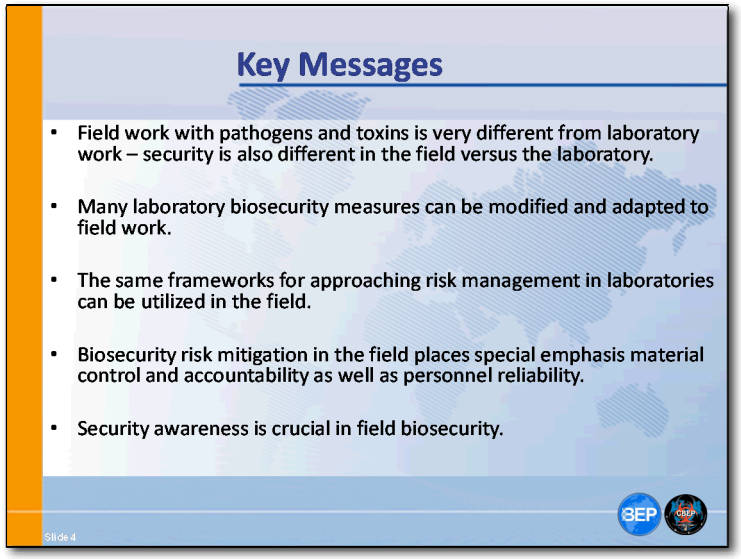
How does security awareness tie in to the other pillars?


Security Awareness
Discussion:
How might you promote a culture of increased security awareness in your facility?
Slide 75

Notes:


Final Review
Review
For 10 minutes, let's discuss what we have learned about Laboratory Biosecurity.
What did we learn?
What does it mean?
Where do we go from here?
Slide 76


Key Messages
• 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.
Slide 4


Key Messages
• Field work with pathogens and toxins is very different from laboratory work – security is also different in the field versus the laboratory.
• Many laboratory biosecurity measures can be modified and adapted to field work.
• The same frameworks for approaching risk management in laboratories can be utilized in the field.
• Biosecurity risk mitigation in the field places special emphasis material control and accountability as well as personnel reliability.
• Security awareness is crucial in field biosecurity.
Slide 4


Thank You!
Don't forget to complete your evaluation!
BEP
CBEP
Slide 35