Ministry of Higher Education and Scientific Research

University of Baghdad

College of Science

Department of Biology

Biosecurity
2021-2022

المرحلة الاولى - الدراستين الصباحية والمسائية

الفصل الدراسي الثاني

تدريسي المادة :ا.م.د.فائزه كاظم عمران

Lec. 1 Biosecurity

What is Biosecurity?

Biosecurity is a strategic and integrated approach to analyzing and managing relevant risks to human, animal and plant life and health and associated risks for the environment. It is based on recognition of the critical linkages between sectors and the potential for hazards to move within and between sectors, with system-wide consequences. Reviewing national capacity provision for biosecurity as a whole help identify any gaps in regulations and monitoring. Also, as technologies for the detection of pests and disease develop, it is likely that synergies will emerge between sectors in areas such as virology or detection of low levels of chemical contaminants. Ultimately the aim is to enhance national ability to protect human health, agricultural production systems, and the people and industries that depend on them.

History of Biosecurity

First described in the agricultural and environmental Industries – Biosecurity is the protection of agricultural animals from any type of infectious agent—viral, bacterial, fungal, or parasitic. People can spread diseases as they move within a facility and from one to another.

The events of September 11, 2001, and the anthrax attacks in October of that year reshaped and changed, forever, the way we manage and conduct work in biological and clinical laboratories." Biosafety and biosecurity have dominated the policy discourse and the two have been inexorably intertwined. Biosafety and biosecurity are defined by the World Health Organization (WHO): **Biosafety** comprises "the containment principles, technologies and practices that are implemented to prevent unintentional exposure to pathogens and toxins or their accidental release"; **Biosecurity** is defined as "the protection, control and accountability for valuable

biological materials (including information) in laboratories in order to prevent their unauthorized access, loss, theft, misuse, diversion or intentional release."

Biosecurity as the third component of biorisk management focuses on securing biological materials. The current focus on biosecurity evolved from a series of events that made the need for more focus on security around laboratories clear.

In 1984, members of the Rajneeshee commune in The Dalles, Oregon, purchased a strain of Salmonella from a medical supply company in Seattle, Washington to contaminate ten local salad bars, sickening over 750 individuals. Although not immediately recognized as an attack, this incident was a clear indication of the potential impact of the misuse of biological agents.

In 2001, at least five envelopes containing Bacillus anthracis spores (the etiologic agent of the disease anthrax) were mailed to U.S. Senators and media organizations. At least 22 individuals contracted anthrax as a result of the mailings; five of the individuals died. After a nearly ten year investigation, known as Amerithrax, it was determined through genetic analysis that the spores in the letters were derived from a single spore-batch of Bacillus anthracis (Ames strain), isolated from a cow in Texas and distributed to a number of research laboratories, including the United States Army Medical Research Institute for Infectious Diseases (USAMRIID). On February 19, 2010, the Justice Department, the FBI, and the U.S. Postal Inspection Service formally concluded the investigation into the 2001 anthrax attacks, which determined that Dr. Bruce Ivins, a USAMRIID employee, acted along in planning and executing these attacks.

Lec.2

Differentiating between biosafety and biosecurity

BIOSAFETY:

Describes the containment principles, technologies and practices that are applied to prevent the unintentional exposure to Biological agents and toxins or their accidental release

BIOSECURITY:

Describes protection, control and accountability for valuable biological materials within laboratories, in order to prevent their **loss**, **theft**, **misuse**, **diversion** of, **unauthorized access** or **intentional release**.

Biosafety *protects people from germs –* ***Biosecurity*** *protects germs from people.*

Goals of Biosecurity

The main aim of biosecurity is to protect human health and to increase and protect agricultural produce through the prevention, control and management of biological risk factors. Biosecurity also aims to protect against acts of bioterrorism and to prevent adverse biosecurity events as well as offering advice on appropriate interventions and political and social changes that should be adopted by government regulatory agencies.

Some factors influencing biosecurity:

1. Globalization
2. New agricultural production and food processing technologies
3. Increased trade in food and agricultural products
4. Legal obligations for signatories of relevant international agreements
5. Increasing travel and movement of people across borders
6. Advances in communications and global access to biosecurity information
7. Greater public attention to biodiversity, the environment and the impact of agriculture on both
8. Shift from country independence to country interdependence for effective biosecurity
9. Scarcity of technical and operational resources
10. High dependence of some countries on food imports.

What are the Biosecurity hazards?

A variety of biosecurity hazards threaten health and biosafety. Some of these are listed in the table below:

Table 1. Definitions of hazard as unlikable to different biosecurity sectors

Sectors	Definitions of hazard
Food safety	A biological, chemical or physical agent in, or condition of, food with the potential to cause an adverse health effect.
Zoonoses	A biological agent that can be transmitted naturally between wild or domestic animals and humans.
Animal health	Any pathogenic agent that could produce adverse consequences on the immuration of a commodity.
Plant health	Any species, strain or biotype of plant, animal or pathogenic agent injurious to octants or plant products (International Plant Protection Convention (IPPC).
Plant health quarantine	A pest of potential economic importance to the area endangered thereby and not yet present there, or present but not widely distributed and being officially controlled (International Plant Protection Convention IPPC).
"Biosecurity" in relation to plants and animals	A living modified organism (LMO) that possesses a novel combination of relation to genetic material obtained through the use of modem biotechnology that is likely plants and to have adverse effects on the conservation and sustainable use of biological animals' diversity, taking also into account risks to human health (Cartagena Protocol on Biosafety'.
"Biosecurity" in relation to food	A recombinant DNA organism directly effecting or remaining in a food that relation to could have an adverse effect on human health (Cartagena Protocol on food Biosafety).
Invasive alien species	An invasive alien species outside its natural past or present distribution whose introduction and/or spread threatens biodiversity (CBD).

Lec.3 Biosecurity

Biosecurity in laboratories

Pathological agents may be collected, grown, stored or handled in clinical laboratories, diagnostic facilities, public health laboratories, research centers and production facilities. All of these facilities are at risk of biosecurity incidents.

The term "biorisk" refers to the risk associated with biological substances and infectious agents. Biorisk assessments are carried out to identify the acceptable and unacceptable levels of these risks. The methods adopted to manage the occurrence of biorisks is an important field of research.

The reduction of biorisk involves the sharing of expertise and advice regarding the guidance and training that is needed for disease agents to be handled and controlled safely.

There are several non-legislated guidelines that set out the standard of conduct or behavior with respect to a particular biological activity. Organizations and individuals voluntarily agree to abide by these guidelines.

The term "biohazard" refers to a biological substance that poses a risk to health, particularly human health.

Laboratory biosecurity involves responsibility for the protection, control and accountability of biological materials within facilities to prevent their unauthorized access, theft, misuse, loss, or intentional release or exposure. Misuse refers to the use of biological materials for inappropriate or illegitimate purposes. Examples of biological materials that require this management include pathogens and toxins, as well as non-pathogenic organisms such as vaccines, genetically modified organisms (GMOs) and cell components or genetic elements.

While these objectives are related, and both are linked to the Convention, their purposes remain distinct. As a result, biosecurity concepts differ from biosafety concepts. The approaches used to achieve them are often similar or mutually reinforcing, but in some cases may conflict. A common example of conflict arises with the transport of dangerous pathogens: in the interests of biosafety, such pathogens should be clearly labeled during transport, but from a biosecurity

perspective, labelling the pathogen being shipped may increase the risk of theft or diversion.

The two major biological threats that are faced in biosecurity include:

- Naturally occurring infectious diseases such as avian flu
- Biological weapons that are in the hands of states and terrorist organizations

These threats pose a challenge in national safety and providing protection against these them forms the basis of biosecurity.

Laboratory Risks

A broad spectrum of risks may be present in a typical biological laboratory, including risks to individuals working in the laboratory, to the community, and to the environment. To successfully mitigate these risks, it is critical to understand the components of risk. Risk, in general, is defined as a function of the likelihood an adverse event involving a specific hazard and/or threat will occur, and its consequences. Risk can also be defined more simply as a function of likelihood and consequences. Likelihood and consequences occur at two different time periods of risk. The likelihood of risk affects whether or not the incident happens, and thus precedes the event. The consequences of risk occur after the incident has happened and affects the severity of the incident. This concept is illustrated in Figure 1.

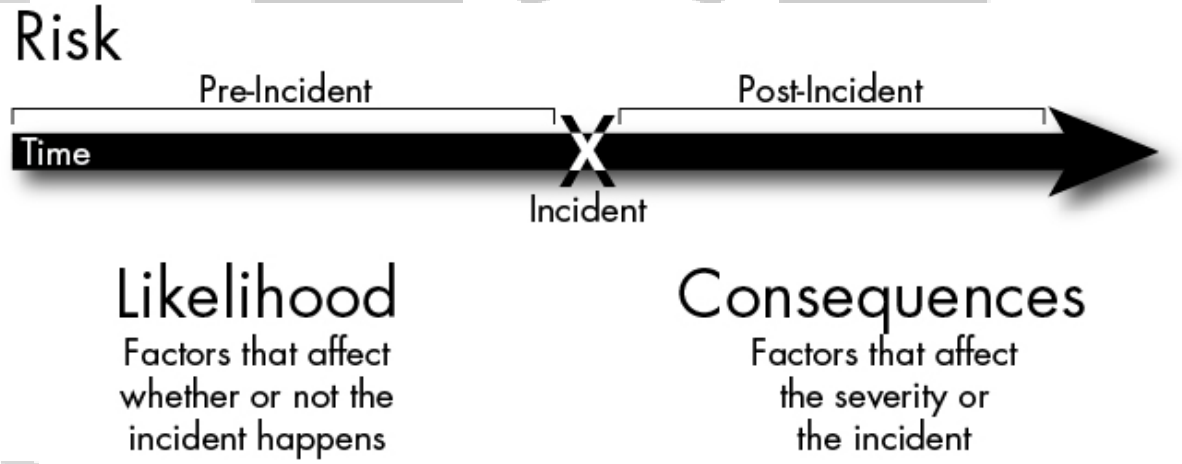

Figure 1. Likelihood and consequences of risk. The likelihood component of risk includes factors that affect whether or not the incident happens and occurs before the actual incident occurs; the consequences component of risk considers factors that affect the severity of an incident after it has occurred.

At the most basic level, understanding a particular risk, therefore, involves answering the following questions:

1. What can go wrong?

2. How likely is it?
3. What are the consequences?

For a laboratory, answering "what can go wrong?" can be a daunting task, but at the simplest level, these include risks posed by the biological agents themselves (e.g. infection via accidental or malicious exposure) and risk to the institution due to theft of intellectual property, valuable property, valuable biological materials, etc. There are also risks inherent to the activities of working with such agents, such as pricking or puncturing the skin with an infected needle or inhaling airborne pathogen particles from poor pipetting technique. All the risks present in a biological laboratory are collectively called "biorisks."

Lec.4

Biosecurity risks

Biosecurity risks are a type of biorisk based upon malicious intent. These risks are primarily focused on theft of a biological agent(s), equipment, or information, but can also include misuse, diversion, sabotage, unauthorized access, or intentional unauthorized release. The overall biosecurity risk varies with the intent of the adversary (or threat) aiming to do the malicious act. Factors that affect the likelihood and consequences of biosecurity risk are presented in Figure 2.

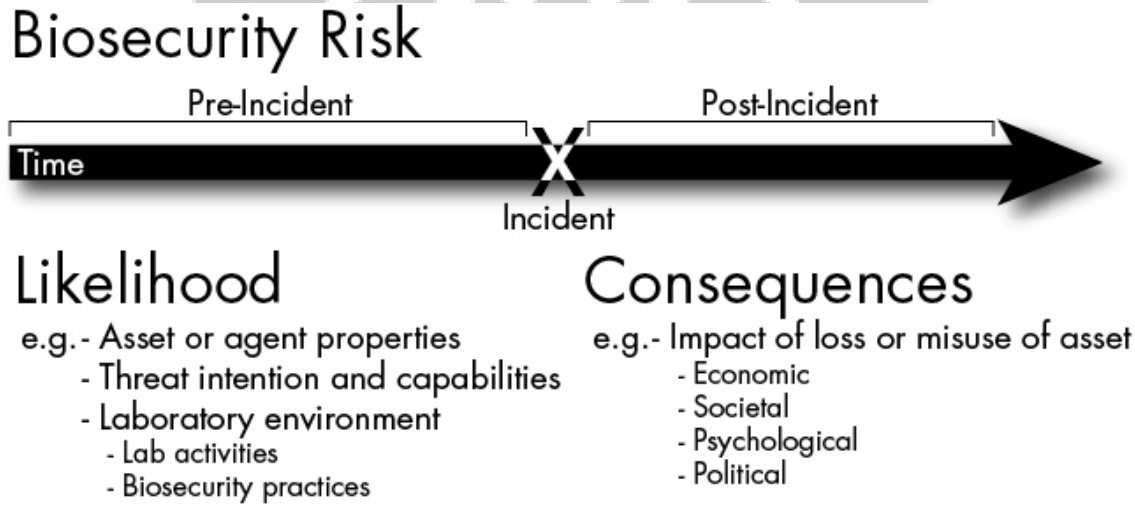

Figure 2: Biosecurity risk

In assessing a biosecurity risk, the malicious intent is typically focused upon an item of value, or asset, within the laboratory. In a biosecurity risk assessment, it is critical to define what assets exist within the laboratory. Once the assets are identified, a biosecurity risk can be defined as the likelihood that the asset can be acquired from a laboratory and the consequences of the loss of that asset (to include misuse of the asset following acquisition). Unlike biosafety risks, biosecurity risks are often difficult to identify and characterize because they are dependent upon intent of the individual(s) interested in illicitly attaining and/or using the asset (threat).

Some of the assets which may exist within a biological institution include VBM, VLM (e.g. equipment), intellectual property, informational assets, and intangible assets (such as the institution's reputation). There are many biosecurity risks based upon these assets in biological institutions, and depending upon the situation and the asset, the risks may impact the researcher(s), the facility, the human and animal community, and the economy.

For example, theft of equipment, such as a centrifuge, may present a significant risk to the laboratory researcher who routinely uses the centrifuge for his/her cutting-edge research.Without the centrifuge, the researcher cannot complete his/her work. The impact of this theft could include a financial risk to the researcher if the researcher purchased the centrifuge with his/her research funds. In addition, the loss would present a professional risk to the researcher as his/her work is subsequently halted until a new centrifuge is purchased or borrowed, and during this time, a competing researcher has completed and published the research results first. The biological facility would be impacted by a financial and operational loss. Additionally, the animal and/or human communities may also be at risk if the centrifuge was used maliciously to release an agent into the environment.

Category A Definition

The U.S. public health system and primary healthcare providers must be prepared to address various biological agents, including pathogens that are rarely seen in the United States. High-priority agents include organisms that pose a risk to national security because they

- can be easily disseminated or transmitted from person to person;
- result in high mortality rates and have the potential for major public health impact;
- might cause public panic and social disruption; and
- require special action for public health preparedness.

Agents/Diseases

- Anthrax (Bacillus anthracis)
- Botulism (Clostridium botulinum toxin)
- Plague (Yersinia pestis)
- Smallpox (variola major)
- Tularemia (Francisella tularensis)
- Viral hemorrhagic fevers, including
    - Filoviruses (Ebola, Marburg)
    - Arenaviruses (Lassa, Machupo)

Category B Definition

Second highest priority agents include those that

- are moderately easy to disseminate;
- result in moderate morbidity rates and low mortality rates; and
- require specific enhancements of CDC's diagnostic capacity and enhanced disease surveillance.

Agents/Diseases

- Brucellosis (Brucella species)
- Epsilon toxin of Clostridium perfringens
- Food safety threats (Salmonella species, Escherichia coli O157:H7, Shigella)
- Glanders (Burkholderia mallei)
- Melioidosis (Burkholderia pseudomallei)
- Psittacosis (Chlamydia psittaci)
- Q fever (Coxiella burnetii)
- Ricin toxin from Ricinus communis (castor beans)
- Staphylococcal enterotoxin B
- Typhus fever (Rickettsia prowazekii)
- Viral encephalitis (alphaviruses, such as eastern equine encephalitis, Venezuelan equine encephalitis, and western equine encephalitis])
- Water safety threats (Vibrio cholerae, Cryptosporidium parvum)

Category C Definition

Third highest priority agents include emerging pathogens that could be engineered for mass dissemination in the future because of

- availability;
- ease of production and dissemination; and
- potential for high morbidity and mortality rates and major health impact.

Agents

- Emerging infectious diseases such as Nipah virus and hantavirus

Lec.5 Biosecurity

Laboratory biosecurity program

A comprehensive laboratory biosecurity program involves:

1. Identification of VBM.

2. Associated agent-based microbiological risk assessment and laboratory biosecurity risk assessment.

3. Bioethical and scientific analysis of research projects before they are authorized.

4. Allocation of responsibilities and authorities among staff and facility managers.

5. Communication between parties involved.

6. Development of and training on emergency plans.

7. Tailored biosecurity training for employees of the facility and for external first responders.

All these steps should be the result of a transparent and documented reasoning process that carefully evaluates the impact of biorisk management breaches, and prepares and plans for worst-case scenarios.

Responsibility for VBM (Valuable Biological Material)

Laboratory biosecurity should mainly be based on:

1. Control and accountability for VBM.

2. Defining their storage location.

3. Describing and scrutinizing their use; identifying personnel (and visitors) who should be granted access to them.

4. Documenting their transfer.

5. Certifying their inactivation and disposal.

6. Sharing this information with appropriate counterparts within the facility.

Laboratory biosecurity measures should be adapted to the needs of the institutions or facilities adopting them. Their identification should be the result of a biosecurity risk assessment that includes input from scientific personnel and laboratory management, biosafety officers, maintenance staff, IT staff, administrators and law-enforcement representatives.

Local law enforcement may be the police or other local, regional or national security force that is trained to manage security issues. Facilities that handle dangerous pathogens and toxins should ensure that all emergency response personnel, including local law enforcement, are aware of the safety issues on-site and the procedures to be followed if an incident occurs.

The facility should establish a clear working relationship with the local lawn forcemeat agency to provide a response to security incidents on-site. A clear protocol should be drawn up detailing the circumstances under which law-enforcement personnel may be summoned, the protocol to follow once on-site, and the scope of authority for all parties involved. Regular on-site training and orientation for the local law-enforcement agency is also recommended.

At facility level, it is recommended that the ultimate responsibility for VBM should lie with the laboratory/facility manager or director, who should be responsible for providing the appropriate conditions to minimize breaches in biosafety and laboratory biosecurity. The facility manager may delegate this responsibility to the principal investigator for routine activities. However, the facility manager will respond in case of biosafety or biosecurity breaches.

At international level, national authorities should be ultimately responsible for breaches in biosafety and laboratory biosecurity that may be at the origin of public health emergencies of international concern .

Lec. 6

Elements of a Strong Biosecurity Program

1. Security Risk Assessment.
2. Threat Assessment.
3. Vulnerability Assessment.
4. Physical security (gates, guards, guns) .
5. IT (information technology) system security.
6. Employee security/ accountability.
7. Access control.
8. Transfer of agents.
9. Incident and injury policies.
10. Emergency response policies.
11. Security breach policies.
12. Intent?

Biosecurity

The Virtual Biosecurity Center (VBC)

Founded in 2011, is a global multi-organizational initiative spearheaded by the Federation of American Scientists (FAS) committed to countering the threat posed by the development or use of biological weapons and the responsible use of science and technology. The VBC is the 'one stop shop' for biosecurity information, education, best practices, and collaboration.
The VBC offers:

- Comprehensive biosecurity news and events, an education center and library updated on a continuous basis with the most current information;
- The Global Forum on Biorisks, a collaborative online forum and tool for informing policy and empowering partnerships among professional biosecurity communities around the world;
- Calendar of global conferences to raise awareness and develop plans to address both current and future biosecurity issues;
- Outreach activities on cutting-edge topics with interactive webcasts;
- Education and partnership to bridge the gap between the scientific, public health, intelligence and law enforcement communities;
- Funding opportunities and coordination including graduate fellowships;
- Translations into more than 50 languages including the 6 UN languages.

The release of a dangerous biological agent, whether intentional, accidental or caused by a natural outbreak, could cause millions of casualties and result in far-reaching economic impacts. Now more than ever, biosecurity awareness, public health preparedness, and education on the responsible use of science and technology are crucial components for dealing with these threats. The VBC was developed with a grant from the National Counter Proliferation Center (NCPC) of the Office of the Director of National Intelligence (ODNI), and the Carnegie Corporation of New York.

Lec. 7

Participating Organizations المنظمات المشاركة

Participating Organizations are governmental and non-governmental organizations, biosecurity policy centers, biosafety associations, and university policy centers from around the world that have agreed to share their activities and educational materials through the VBC.

Participating Organizations:

African Biological Safety Association (AfBSA).
American Association for the Advancement of Science (AAAS) .
American Biological Safety Association (ABSA).
Australian Biosecurity Intelligence Network (ABIN).
BIO (Biotechnology Industry Organization).
International Federation of Biosafety Associations (IFBA)
National Academy of Sciences (NAS)
National Biosafety Association (ANBio)
National Institutes of Health, Office of Biotechnology Activities
Organisation for Economic Co-operation and Development (OECD)

Developing a Biosecurity Program

The need for a biosecurity program should reflect actual risk management practices based on risk assessment at the specified location. A biosecurity risk assessment should be based on an analysis of the potential and consequences of the loss of ambiguity and potential use of pathogens and toxins. More importantly, the use of the BIO program should be used as a basis for decision making and risk management.

A Biosecurity Risk Assessment and Management Process

There are several models available for the **Biosecurity Risk Assessment** program. Most of these models share many characteristics such as asset identification, threat, vulnerability and side effects. Here is an example of how the BRA program works: In this example, the risk assessment and management program are divided into five steps and each step-in turn can be divided into other secondary steps:

1. **Determination and prioritization of biomaterials and poisons**
2. **Identification and ranking of threats and risks from biomaterials and toxins**
3. **Risk analysis of specific security scenarios**
4. **Design and development of an integrated risk management program**
5. **Regular assessment of the objectives and protection standards of the institution concerned.**

Below we give an example of these five steps:

Step 1: Determination and prioritization of biomaterials and poisons

1. Identification of the biological materials found in the organization, in terms of form, location, and quantities, including non-divisible materials (ie toxins).
2. Assess the potential for abuse of these biological materials.
3. Assess the consequences of misuse of these biological materials.
4. Arrange biological materials on the basis of consequences of misuse (hazard of harmful use).

Step 2: dentification and ranking of threats and risks from biomaterials and toxins

1. Identification of types of insiders that may pose a threat to biological materials in the organization
2. Identification of species of strangers (if any) that may pose a risk to the biological material in the organization
3. Evaluate the motives, means and opportunities available to multiple opponents**.**

Lec. 8

Step 3: Risk analysis of specific security scenarios

Develop a list of possible biosecurity scenarios, or undesirable events that

can occur within the organization (each scenario is a combination of the pathogen, the resistance mechanism, and the follower procedure): -

1. Access to the specific pathogen within the laboratory.
2. Preventive measures taken to prevent them
3. How current protection measures (vulnerabilities) can be breached

Step 4: Design and development of an integrated risk management program

1. The development of the management of the biosecurity risk profile and the documentation of any biosecurity scenarios represents unacceptable risks and should be mitigated against those risks that can be adequately addressed through existing protection controls.
2. The Department develops a biosecurity plan to describe how the institution deals with those unacceptable risks and how Mitigation including:

1. Written security plan, standard operating procedures, and incident response plans.
2. Written protocols to train staff on potential risks.
3. ensures that the resources needed to achieve and document protection measures are managed in the Biosecurity Plan

Step 5: Regular assessment of the objectives and protection standards of the institution concerned.

The Department regularly re-evaluates and makes the necessary adjustments to:

1. Biological Security Risk Statement.
2. Risk Assessment Process Biosecurity
3. Institution Plan for Biosecurity Program
4. Biosecurity Systems of the Enterprise

Biosecurity Lec. 9

Applied biosecurity in practice

Implementing biosecurity encompasses many aspects of laboratory activities and resources. It aims to ensure the integrity and security of all pathogens, toxins and sensitive information. Applied biosecurity has a number of key components:

- Employee accountability.
- Material control.
- Development of standard operating procedures.
- Compliance with biosecurity procedures.
- Physical security.
- Access control.
- Information security.
- transport security;
- Proper routines for security-incident reporting and response.
- Maintaining continuous evaluation and revision.
- Providing training and education.

Employee accountability

Responsibility for biosecurity is shared by the employer and the employee. However, the facility director or head of department has the ultimate responsibility and accountability for the materials, equipment and information at a facility, the activities performed within it and the actions of the staff. It is difficult for one employee to have complete overview of all activities, and thus responsibilities are commonly delegated to laboratory managers and principal investigators. In turn,

they can designate employees with proper qualifications and authorization to oversee specific agents or all agents in one laboratory. These employees must:

• oversee and manage infectious pathogens, toxins, sensitive information and equipment;

• ensure that these are accounted for at all times; and

• conduct record keeping, auditing and reporting.

Material control

Proper inventory practices are essential for effective material control and must cover pathogens and toxins from the time that they arrive at a facility or laboratory to their final destruction or shipping. Proper inventory practices must include the confirmation of receipt by the designated party. Proper biosafety practices and regulations do partially address inventory control, but this is far from common practice. Access to areas where biological materials are used or stored must be limited to those with proper clearance.

The employees who have access to and work with biological materials must be responsible for basic inventory tasks because they are familiar with the type and amount of biological materials present and their location and state. Rules and procedures for inventory control must be developed by laboratory managers or principal investigators, together with management and the biosafety and biosecurity officer. Inventories of pathogens and toxins vary in complexity, but they should Include relevant information such as:

• Types of material (name, strain, serotype, taxonomy etc.);

• Forms of material (solution or pellet, freeze dried, paraffin embedded etc.);

• Quantities of material (number of vials, amounts of liquid, post-experiment quantities);

• Locations of material (in short- or long-term storage or in use);

• Contact or responsible employee;

• Employees who have access to the materials;

• Modifications of the original biological properties of material (i.e. genetically modified microorganisms and genetically modified organisms);

• Confirmation, date and method of destruction or inactivation of material; and

• Dates of transfer of material (delivery and departure) and end-user or recipient receipts.

Various methods can be used to coordinate and manage material inventories.
• Local laboratory lists of material can be created and managed by those accountable for them and passed on to an employee at a higher level of authority.
• A general material list for the whole facility can be maintained, coordinated and managed by the appointed biosafety and biosecurity officer.

Lec. 10

Physical security

The aim of physical security is to restrict access to those with professional qualifications and who have the immunizations that allow them to work with specific pathogens and delay, deny and detect access by unauthorized individuals. Physical security is closely associated with biosafety and facility design. However, even the most sophisticated physical security is only one component of a secure workplace. The level of security of a laboratory or facility is ultimately determined by the employee's awareness of the need for security and behaviour that reflects such an awareness.
Physical security entails:
•monitoring and managing perimeters and security boundaries;
•establishing and enforcing access restrictions;
•installing and maintaining alarm and surveillance equipment;
•determining and preserving adequate containment levels; and
• provide prompt alerts of breaches or intrusions.

Information security

Information that enables access to a facility or to biological materials is sensitive and must be kept secure.19 Security measures may also be required for other sensitive information, such as:
• inventory lists of pathogens and toxins;
• sensitive equipment, including its location;
• security routines;
• access lists;
• patient sample data; and
• employee contact information.

Transfer and transport security

Transfers of dangerous pathogens and toxins must follow national and international guidelines that are based on the UN regulations for the two most hazardous categories of material (categories A and B).21 The UN regulations
focus on the safety of the employees involved in transporting the materials and the integrity of the containment (see case studies 3–6 for examples of violations of proper procedures or mistakes). Adequate containment must also be ensured for transports over shorter distances, such as between neighbouring facilities or within a facility. When materials are transferred in a facility or between facilities the properly packaged material must not be out of sight, even for a moment. This ensures the integrity of the transfer all the way to its final destination. Professional handling must be used for longer transports and there are many companies that handle dangerous goods and possess ADR (safe international transport of dangerous goods by road) certification. The primary security problem in long distance transfers is that the sender cannot personally supervise the transfer but must rely on the company to do so.

Case 1. Live *Bacillus anthracis* shipped by mistake In May 2004 live *Bacillus anthracis* was shipped from the Southern Research Institute in Frederick, Maryland, USA, to the Oakland Children's Hospital & Research Center in Oakland, California, USA. The sender had verified that the samples were not viable. However, the death of 49 mice that were infected using the *Bacillus anthracis* samples revealed the viability of the samples.

Case 2. British journalists order a sequence of modified smallpox DNA On 14 June 2006, *The Guardian* reported that journalists had successfully ordered online and received a plastic vial containing the 78bp sequence of DNA coding for the smallpox virus coat protein modified with three mutations from VH Bio Ltd. The vial, which arrived in an A5-size Jiffy bag, cost £33. The company was unaware that the sequence belonged to the smallpox genome.

Case 3. Bacillus anthracis requested from the University of Gothenburg The University of Gothenburg, Sweden, which has one of the largest bacteria depositories in the world, has on two occasions since the 2001 mailing of the

anthrax-contaminated letters in the United States received requests for Bacillus anthracis that were deemed suspicious. The requests were forwarded to the Swedish security police for investigation. The University of Gothenburg
has stated that its depository has never held or offered Bacillus anthracis.

Case 4. Yersinia pestis shipped to Tanzania In September 2002 Thomas Butler, a professor at Texas Tech University, Lubbock, Texas, USA, knowingly transferred the human pathogen Yersinia pestis (bubonic plague) to Tanzania without obtaining the required US Department of Commerce licence. He described the pathogen as 'laboratory materials' on the waybill and failed to fill out relevant sections of the Shipper's Export Declaration requirement. Butler was therefore considered to have deliberately evaded provisions of the US Export Administration Regulations. On 10 March 2004 Butler was sentenced to two years imprisonment with three years supervised
release. He was also required to pay criminal fines and make restitution for export violations and false statements.

In such cases, the sender must establish a chain of custody that:

- identifies the individuals involved in the transfer; and
- outlines the provisions to address potential problems.