Funded by the European Union

EU CBRN Courseware
Centres of Excellence, an Initiative of the European Union
Center for Nonproliferation Studies

Module 4: Biological Safety, Biological Security, and Biological Weapons
Part 4: Methods of Preventing Breaches of Biosecurity in Vital Bioscientific Facilities

The security of biological research laboratories, culture collections, clinical laboratories, and industrial facilities such as vaccine production plants is critical in order to prevent sensitive information or dangerous pathogens from falling into the wrong hands.

As such, the objective of facility biosecurity is to reduce the likelihood that select agents or valuable biological materials could be stolen by terrorists or criminals.

Accomplishing biosecurity involves a cost-benefit consideration because it is next to impossible, as well as very costly, to perfectly secure every aspect of a facility and its assets. It is important to recognize that biological agents can be found elsewhere. Bioscience facilities are not unique repositories of potential biological weapons agents because most agents can be isolated from nature and they also exist in many national culture collections. Moreover, not all agents will be equally attractive to adversaries. Few agents can easily be grown, processed, and weaponized in a laboratory without losing virulence or toxicity, and very few biological weapons agents can cause mass casualties. As such, establishing biosecurity policies requires a methodology to make informed decisions about how to design an effective and efficient biosecurity system.

A qualitative risk and threat assessment is the first step in establishing a biosecurity methodology. This process should involve input from scientists, managers, security professionals, law enforcement and counterterrorism experts. Subsequently, assets should be identified and prioritized according to threat—for example, how attractive a facility might be to an adversary—and risk—for instance, what the consequences of a security breach might be. Next, likely adversaries should be identified and their capabilities assessed. This step is followed by identifying various scenarios for unauthorized access to facilities and evaluating the probability and consequences of each scenario. Finally, a rational decision is made to eliminate or diminish risks by taking measures such as strengthening physical security, conducting background investigations of employees, and developing well thought-out incident response plans.

In identifying threats, facility managers must consider different categories of people who might seek unauthorized entry into a sensitive bioscience facility. Examples of such categories include insiders or employees with authorized access to the facility, visitors to the facility, outsiders with limited facility access and knowledge of security systems,

With the support of

Action implemented by:

outsiders with no access but general knowledge of security systems, outsiders with no access and no knowledge of security systems, and insiders and outsiders who collude or conspire together. It is also important to consider how an adversary could attempt to gain access to a facility, whether alone or in a group, armed or unarmed, covertly or overtly.

In order to consider what adversaries might aim to do if they indeed gained access to a facility, the threat must be matched to the assets that might be affected. For example, an adversary could attempt to steal, destroy, and/or disperse agents; steal and/or destroy information or equipment; destroy a facility's operational systems, or even destroy a facility and injure or kill its workers. The costs related to each of these events need to be estimated as does the costs for instituting measures to prevent them.

The schema presented here is a useful tool for prioritizing risks based on the likelihood, or probability, that an event will occur and linking that event with the magnitude of the consequences, were it to be realized.

Scenarios that have the highest risk—those with the highest probability of being realized and causing the most drastic consequences—should have priority when instituting or enhancing security measures. But even medium- to low-probability scenarios cannot be ignored by facility managers; incident response plans to meet their consequences must also be developed and practiced.

The highest risk scenarios are those that involve attempts to covertly steal select agents. The theft of select agents could have dangerous consequences, regardless of who steals them: insider, visitor, or outsider. Theft of select agents is especially threatening when done covertly because the perpetrator's identity could remain unknown, and the fact that a select agent is missing might not be discovered for some time. Another high risk is the attempt to covertly steal *information* related to select agents that could be used by an adversary to weaponize such agents.

Medium-risk scenarios might involve an outsider aiming to damage or destroy a facility. A low-risk scenario might involve a terrorist commando assault on a facility. Such an attack is considered unlikely because police and military units would be quickly mobilized and deployed by defenders of the attacked facility.

In addition to identifying potential threats and prioritizing risks, a biosecurity regime should focus on six particularly important principles that lay the foundation for defensive measures: personnel reliability, physical security, information security, material control and accountability, material transfer security, and program management.

Personnel reliability begins with hiring trustworthy people and conducting background investigations on employees who work with select agents or who might gain access to them for other reasons (for example, janitors and plumbers). Access should be given only to individuals who have legitimate need to handle select agents primarily for research purposes, provide support for facility operations, have proper training in biosafety and biosecurity procedures, and are registered with the Centers for Disease Control and Prevention or the Animal and Plant Health Inspection Service, the two federal agencies that maintain the select agent list. Visitors to the facility should be pre-screened, provided with a badge upon entry to the facility, and escorted at all times when they are inside the

facility. Additionally, employees should be encouraged to report any suspicious activity to security officers.

Physical security is a system of protective measures designed to deter, detect, and respond to attempts to gain unauthorized access to select agents or sensitive information. A good physical security system involves the use of graded protection areas, or specially defined areas, with security levels assigned based on their proximity to the assets of concern. These graded protection areas should be equipped with intrusion detection devices, access controls, and transaction recordings to monitor who accesses which facilities and when. In case of unauthorized access, the system should have alarm assessment capabilities, physical barriers and delay systems, and capabilities to automatically notify law enforcement of the location of a security breach for timely response.

Material control and accountability involves accounting practices to document the exact type, quantity, and location of materials in a facility, as well as who is responsible for them and more broadly who has access to them. Material control and accountability also documents the handling and/or movement of select agents with precise in and out dates and times.

Material transfer security is similar to material control and accountability in that it is the process of documenting the movement of select agents when they are transferred between protected areas within a facility. Authorization should be requested and received prior to transferring agents, and the entire transfer process should be closely monitored and documented. These procedures help to insure that no materials are lost, stolen, or diverted while they are passing through areas with lower security.

Information and cyber security is of high concern in a world where attempts to gain access to sensitive information through computer hacking are ever increasing. Information related to select agents should be highly controlled and strongly guarded both in electronic formats through the use of password protection and in hard copy format by storing it in safes or locked filing cabinets.

Effective program management is essential for implementing a biosecurity program. Biosecurity program managers maintain documentation of the security plan, incident response plan, security training program, and the self-assessment and auditing program.

In sum, facility biosecurity is necessary in order to reduce the likelihood that select agents or sensitive information could be stolen from bioscience facilities. It is critical that biosecurity measures are not overly burdensome on the research staff, but that they balance the need for scientific freedom with the need for security measures.

Beyond facility biosecurity, countries should bring into force national legislation to criminalize and punish any attempts by their citizens to acquire, develop, produce, and possess biological agents for offensive purposes. Relevant laws should specify that the country's citizens are bound by the Biological and Toxin Weapons Convention, which requires State Parties to create and implement national legislation to ensure that applied microbiology is conducted only for peacefully directed or defensive purposes. In addition, all governments have ongoing responsibilities in implementing United Nations

Security Council Resolution 1540. This resolution enjoins states to make certain that sensitive biological and other materials are kept out of the hands of terrorists and other criminals while at the same time preserving legitimate commercial and peaceful uses of these and related materials. Thus, national legislation should provide for both safeguards to prevent unauthorized access to dangerous biological agents and procedures to protect public safety in the event safeguards are violated. At the same time, the state should ensure that scientists have appropriate access to biological agents for legitimate, peaceful purposes. The law should also direct the country's Ministry of Agriculture to set up standards and procedures to govern the use, possession, and transfer of biological agents that pose a threat to agriculture, livestock, or humans.