Section VI

Principles of Laboratory Biosecurity

Since the publication of the 4th edition of BMBL manual in 1999, significant events have brought national and international scrutiny to the area of laboratory security. These events, including the anthrax attacks on U.S. citizens in October 2001 and the subsequent expansion of the United States Select Agent regulations in December 2003, have led scientists, laboratory managers, security specialists, biosafety professionals, and other scientific and institutional leaders to consider the need for developing, implementing and/or improving the security of biological agents and toxins within their facilities. Appendix F of BMBL 4th edition provided a brief outline of issues to consider in developing a security plan for biological agents and toxins capable of serious or fatal illness to humans or animals. In December 2002, Appendix F was updated and re-released as a security and emergency response guidance for laboratories working with Select Agents.[1] A further updated and revised Appendix F is included in the 5th edition of BMBL and is focused exclusively on Select Agent Laboratories and includes current references for the USDA and CDC Select Agent Programs.

This section describes laboratory biosecurity planning for microbiological laboratories. As indicated below, laboratories with good biosafety programs already fulfill many of the basic requirements for security of biological materials. For laboratories not handling select agents, the access controls and training requirements specified for BSL-2 and BSL-3 in BMBL may provide sufficient security for the materials being studied. Security assessments and additional security measures should be considered when select agents, other agents of high public health and agriculture concern, or agents of high commercial value such as patented vaccine candidates, are introduced into the laboratory.

The recommendations presented in this section are advisory. Excluding the Select Agent Regulations, there is no current federal requirement for the development of a biosecurity program. However, the application of these principles and the assessment process may enhance overall laboratory management. Laboratories that fall under the Select Agent regulations should consult Appendix F (42 CFR part 73; 7 CFR 331 and 9 CFR 121).[4,5,6]

The term “biosecurity” has multiple definitions. In the animal industry, the term biosecurity relates to the protection of an animal colony from microbial contamination. In some countries, the term biosecurity is used in place of the term biosafety. For the purposes of this section the term “biosecurity” will refer to the protection of microbial agents from loss, theft, diversion or intentional misuse. This is consistent with current WHO and American Biological Safety Association (ABSA) usage of this term.[1,2,3]

Security is not a new concept in biological research and medical laboratories. Several of the security measures discussed in this section are embedded in the biosafety levels that serve as the foundation for good laboratory practices throughout the biological laboratory community. Most biomedical and microbiological laboratories do not have select agents

or toxins, yet maintain control over and account for research materials, protect relevant sensitive information, and work in facilities with access controls commensurate with the potential public health and economic impact of the biological agents in their collections. These measures are in place in most laboratories that apply good laboratory management practices and have appropriate biosafety programs.

BIOSAFETY AND BIOSECURITY

Biosafety and biosecurity are related, but not identical, concepts. Biosafety programs reduce or eliminate exposure of individuals and the environment to potentially hazardous biological agents. Biosafety is achieved by implementing various degrees of laboratory control and containment, through laboratory design and access restrictions, personnel expertise and training, use of containment equipment, and safe methods of managing infectious materials in a laboratory setting.

The objective of biosecurity is to prevent loss, theft or misuse of microorganisms, biological materials, and research-related information. This is accomplished by limiting access to facilities, research materials and information. While the objectives are different, biosafety and biosecurity measures are usually complementary.

Biosafety and biosecurity programs share common components. Both are based upon risk assessment and management methodology; personnel expertise and responsibility; control and accountability for research materials including microorganisms and culture stocks; access control elements, material transfer documentation, training, emergency planning, and program management.

Biosafety and biosecurity program risk assessments are performed to determine the appropriate levels of controls within each program. Biosafety looks at appropriate laboratory procedures and practices necessary to prevent exposures and occupationally-acquired infections, while biosecurity addresses procedures and practices to ensure that biological materials and relevant sensitive information remain secure.

Both programs assess personnel qualifications. The biosafety program ensures that staff are qualified to perform their jobs safely through training and documentation of technical expertise. Staff must exhibit the appropriate level of professional responsibility for management of research materials by adherence to appropriate materials management procedures. Biosafety practices require laboratory access to be limited when work is in progress. Biosecurity practices ensure that access to the laboratory facility and biological materials are limited and controlled as necessary. An inventory or material management process for control and tracking of biological stocks or other sensitive materials is also a component of both programs. For biosafety, the shipment of infectious biological materials must adhere to safe packaging, containment and appropriate transport procedures, while biosecurity ensures that transfers are controlled, tracked and documented commensurate with the potential risks. Both programs must engage laboratory personnel in the development of practices and procedures that fulfill the biosafety and biosecurity program objectives but that do not hinder research or

clinical/diagnostic activities. The success of both of these programs hinges on a laboratory culture that understands and accepts the rationale for biosafety and biosecurity programs and the corresponding management oversight.

In some cases, biosecurity practices may conflict with biosafety practices, requiring personnel and management to devise policies that accommodate both sets of objectives. For example, signage may present a conflict between the two programs. Standard biosafety practice requires that signage be posted on laboratory doors to alert people to the hazards that may be present within the laboratory. The biohazard sign normally includes the name of the agent, specific hazards associated with the use or handling of the agent and contact information for the investigator. These practices may conflict with security objectives. Therefore, biosafety and biosecurity considerations must be balanced and proportional to the identified risks when developing institutional policies.

Designing a biosecurity program that does not jeopardize laboratory operations or interfere with the conduct of research requires a familiarity with microbiology and the materials that require protection. Protecting pathogens and other sensitive biological materials while preserving the free exchange of research materials and information may present significant institutional challenges. Therefore, a combination or tiered approach to protecting biological materials, commensurate with the identified risks, often provides the best resolution to conflicts that may arise. However, in the absence of legal requirements for a biosecurity program, the health and safety of laboratory personnel and the surrounding environment should take precedence over biosecurity concerns.

RISK MANAGEMENT METHODOLOGY

A risk management methodology can be used to identify the need for a biosecurity program. A risk management approach to laboratory biosecurity 1) establishes which, if any, agents require biosecurity measures to prevent loss, theft, diversion, or intentional misuse, and 2) ensures that the protective measures provided, and the costs associated with that protection, are proportional to the risk. The need for a biosecurity program should be based on the possible impact of the theft, loss, diversion, or intentional misuse of the materials, recognizing that different agents and toxins will pose different levels of risk. Resources are not infinite. Biosecurity policies and procedures should not seek to protect against every conceivable risk. The risks need to be identified, prioritized and resources allocated based on that prioritization. Not all institutions will rank the same agent at the same risk level. Risk management methodology takes into consideration available institutional resources and the risk tolerance of the institution.

Developing a Biosecurity Program

Management, researchers and laboratory supervisors must be committed to being responsible stewards of infectious agents and toxins. Development of a biosecurity program should be a collaborative process involving all stakeholders. The stakeholders include but are not be limited to: senior management, scientific staff, human resource officials, information technology staff, and safety, security and engineering officials. The

involvement of organizations and/or personnel responsible for a facility's overall security is critical because many potential biosecurity measures may already be in place as part of an existing safety or security program. This coordinated approach is critical in ensuring that the biosecurity program provides reasonable, timely and cost effective solutions addressing the identified security risks without unduly affecting the scientific or business enterprise or provision of clinical and/or diagnostic services.

The need for a biosecurity program should reflect sound risk management practices based on a site-specific risk assessment. A biosecurity risk assessment should analyze the probability and consequences of loss, theft and potential misuse of pathogens and toxins.[7] Most importantly, the biosecurity risk assessment should be used as the basis for making risk management decisions.

Example Guidance: A Biosecurity Risk Assessment and Management Process

Different models exist regarding biosecurity risk assessment. Most models share common components such as asset identification, threat, vulnerability and mitigation. What follows is one example of how a biosecurity risk assessment may be conducted. In this example, the entire risk assessment and risk management process may be divided into five main steps, each of which can be further subdivided: 1) identify and prioritize biologicals and/or toxins; 2) identify and prioritize the adversary/threat to biologicals and/or toxins; 3) analyze the risk of specific security scenarios; 4) design and develop an overall risk management program; 5) regularly evaluate the institution's risk posture and protection objectives. Example guidance for these five steps is provided below.

Step 1: Identify and Prioritize Biological Materials

- Identify the biological materials that exist at the institution, form of the material, location and quantities, including non-replicating materials (i.e., toxins).
- Evaluate the potential for misuse of these biologic materials.
- Evaluate the consequences of misuse of these biologic materials.
- Prioritize the biologic materials based on the consequences of misuse (i.e., risk of malicious use).

At this point, an institution may find that none of its biologic materials merit the development and implementation of a separate biosecurity program or the existing security at the facility is adequate. In this event, no additional steps would need to be completed.

Step 2: Identify and Prioritize the Threat to Biological Materials

- Identify the types of "Insiders" who may pose a threat to the biologic materials at the institution.
- Identify the types of "Outsiders" (if any) who may pose a threat to the biologic materials at the institution.
- Evaluate the motive, means, and opportunity of these various potential adversaries.

Step 3: Analyze the Risk of Specific Security Scenarios

- Develop a list of possible biosecurity scenarios, or undesired events that could occur at the institution (each scenario is a combination of an agent, an adversary, and an action). Consider:
    - access to the agent within your laboratory;
    - how the undesired event could occur;
    - protective measures in place to prevent occurrence;
    - how the existing protection measures could be breached (i.e., vulnerabilities).
- Evaluate the probability of each scenario materializing (i.e., the likelihood) and its associated consequences. Assumptions include:
    - although a wide range of threats are possible, certain threats are more probable than others;
    - all agents/assets are not equally attractive to an adversary;
    - valid and credible threats, existing precautions, and the potential need for select enhanced precautions are considered.
- Prioritize or rank the scenarios by risk for review by management.

Step 4: Develop an Overall Risk Management Program

- Management commits to oversight, implementation, training and maintenance of the biosecurity program.

- Management develops a biosecurity risk statement, documenting which biosecurity scenarios represent an unacceptable risk and must be mitigated versus those risks appropriately handled through existing protection controls.

- Management develops a biosecurity plan to describe how the institution will mitigate those unacceptable risks including:

    - a written security plan, standard operating procedures, and incident response plans;

    - written protocols for employee training on potential hazards, the biosecurity program and incident response plans.

- Management ensures necessary resources to achieve the protection measures documented in the biosecurity plan.

Step 5: Reevaluate the Institution's Risk Posture and Protection Objectives

- Management regularly reevaluates and makes necessary modifications to the:

    - biosecurity risk statement;

    - biosecurity risk assessment process;

    - the institution's biosecurity program/plan;

    - the institution's biosecurity systems.

- Management assures the daily implementation, training and annual re-evaluation of the security program.

ELEMENTS OF A BIOSECURITY PROGRAM

Many facilities may determine that existing safety and security programs provide adequate mitigation for the security concerns identified through biosecurity risk assessment. This section offers examples and suggestions for components of a biosecurity program should the risk assessment reveal that further protections may be warranted. Program components should be site-specific and based upon organizational threat/vulnerability assessment and as determined appropriate by facility management. Elements discussed below should be implemented, as needed, based upon the risk assessment process. They should not be construed as "minimum requirements" or "minimum standards" for a biosecurity program.

Program Management

If a biosecurity plan is implemented, institutional management must support the biosecurity program. Appropriate authority must be delegated for implementation and the necessary resources provided to assure program goals are being met. An organizational structure for the biosecurity program that clearly defines the chain of command, roles, and responsibilities should be distributed to the staff. Program management should ensure that biosecurity plans are created, exercised, and revised as needed. The biosecurity program should be integrated into relevant institutional policies and plans.

Physical Security – Access Control and Monitoring

The physical security elements of a laboratory biosecurity program are intended to prevent the removal of assets for non-official purposes. An evaluation of the physical security measures should include a thorough review of the building and premises, the laboratories and biological material storage areas. Many requirements for a biosecurity plan may already exist in a facility's overall security plan.

Access should be limited to authorized and designated employees based on the need to enter sensitive areas. Methods for limiting access could be as simple as locking doors or having a card key system in place. Evaluations on the levels of access should consider all facets of the laboratory's operations and programs (e.g., laboratory entrance requirements, freezer access, etc.). The need for entry by visitors, laboratory workers, management officials, students, cleaning/maintenance staff and emergency response personnel should be considered.

Personnel Management

Personnel management includes identifying the roles and responsibilities for employees who handle, use, store and transport dangerous pathogens and/or other important assets. The effectiveness of a biosecurity program against identified threats depends, first and foremost, on the integrity of those individuals who have access to pathogens, toxins, sensitive information and/or other assets. Employee screening policies and procedures are used to help evaluate these individuals. Policies should be developed for personnel and visitor identification, visitor management, access procedures, and reporting of security incidents.

Inventory and Accountability

Material accountability procedures should be established to track the inventory, storage, use, transfer and destruction of dangerous biological materials and assets when no longer needed. The objective is to know what agents exist at a facility, where they are located, and who is responsible for them. To achieve this, management should define: 1) the materials (or forms of materials) subject to accountability measures; 2) records to be maintained, update intervals and timelines for record maintenance; 3) operating

procedures associated with inventory maintenance (e.g., how material is identified, where it can be stored, used, etc.); and 4) documentation and reporting requirements.

It is important to emphasize that microbiological agents are capable of replication and are often expanded to accommodate the nature of the work involving their use. Therefore, knowing the exact “working” quantity of organisms at any given time may be impractical. Depending on the risks associated with a pathogen or toxin, management can designate an accountable individual who is knowledgeable about the materials in use and responsible for security of the materials under his or her control.

Information Security

Policies should be established for handling sensitive information associated with the biosecurity program. For the purpose of these policies "sensitive information" is that which is related to the security of pathogens and toxins, or other critical infrastructure information. Examples of sensitive information may include facility security plans, access control codes, agent inventories and storage locations. Discussion of information security in this section does not pertain to information which has been designated “classified” by the United States pursuant to Executive Order 12958, as amended, and is governed by United States law or to research-related information which is typically unregulated or unrestricted through the peer review and approval processes.

The objective of an information security program is to protect information from unauthorized release and ensure that the appropriate level of confidentiality is preserved. Facilities should develop policies that govern the identification, marking and handling of sensitive information. The information security program should be tailored to meet the needs of the business environment, support the mission of the organization, and mitigate the identified threats. It is critical that access to sensitive information be controlled. Policies for properly identifying and securing sensitive information including electronic files and removable electronic media (e.g., CDs, computer drives, etc.) should be developed.

Transport of Biological Agents

Material transport policies should include accountability measures for the movement of materials within an institution (e.g., between laboratories, during shipping and receiving activities, etc.) and outside of the facility (e.g., between institutions or locations). Transport policies should address the need for appropriate documentation and material accountability and control procedures for pathogens in transit between locations. Transport security measures should be instituted to ensure that appropriate authorizations have been received and that adequate communication between facilities has occurred before, during, and after transport of pathogens or other potentially hazardous biological materials. Personnel should be adequately trained and familiar with regulatory and institutional procedures for proper containment, packaging, labeling, documentation and transport of biological materials.

Accident, Injury and Incident Response Plans

Laboratory security policies should consider situations that may require emergency responders or public safety personnel to enter the facility in response to an accident, injury or other safety issue or security threat. The preservation of human life, the safety and health of laboratory employees and the surrounding community must take precedence in an emergency over biosecurity concerns. Facilities are encouraged to coordinate with medical, fire, police and other emergency officials when preparing emergency and security breach response plans. Standard Operation Procedures (SOPs) should be developed that minimize the potential exposure of responding personnel to potentially hazardous biological materials. Laboratory emergency response plans should be integrated with relevant facility-wide or site specific security plans. These plans should also consider such adverse events as bomb threats, natural disasters and severe weather, power outages, and other facility emergencies that may introduce security threats.

Reporting and Communication

Communication is an important aspect of a biosecurity program. A “chain-of-notification” should be established in advance of an actual event. This communication chain should include laboratory and program officials, institution management, and any relevant regulatory or public authorities. The roles and responsibilities of all involved officials and programs should be clearly defined. Policies should address the reporting and investigation of potential security breaches (e.g., missing biological agents, unusual or threatening phone calls, unauthorized personnel in restricted areas, etc.).

Training and Practice Drills

Biosecurity training is essential for the successful implementation of a biosecurity program. Program management should establish training programs that inform and educate individuals regarding their responsibilities within the laboratory and the institution. Practice drills should address a variety of scenarios such as loss or theft of materials, emergency response to accidents and injuries, incident reporting and identification of and response to security breaches. These scenarios may be incorporated into existing emergency response drills such as fire drills or building evacuation drills associated with bomb threats. Incorporating biosecurity measures into existing procedures and response plans often provides efficient use of resources, saves time and can minimize confusion in an emergency situation.

Security Updates and Reevaluations

The biosecurity risk assessment and program should be reviewed and updated routinely and following any biosecurity-related incident. Reevaluation is a necessary and on-going process in the dynamic environments of today’s biomedical and research laboratories. Biosecurity program managers should develop and conduct biosecurity program audits

and implement corrective actions as needed. Audit results and corrective actions should be documented. Records should be maintained by the appropriate program officials.

Select Agents

If an entity possesses, uses or transfer select agents, it must comply with all requirements of the National Select Agent Program. See Appendix F for additional guidance on the CDC and USDA Select Agent Programs (42 CFR part 73; 7 CFR 331 and 9 CFR 121).

REFERENCES

1. Richmond JY, Nesby-O'Dell, SL. Laboratory security and emergency response guidance for laboratories working with select agents. MMWR Recomm Rep. 2002;51:(RR-19):1-6.
2. Laboratory biosafety manual. 3rd ed. Geneva: World Health Organization; 2004.
3. American Biological Safety Association. ABSA biosecurity task force white paper: understanding biosecurity. Illinois: The Association; 2003.
4. Possession, use and transfer of select agents and toxins, 42 C.F.R. Part 73 (2005).
5. Possession, use and transfer of biological agents and toxins, 7 C.F.R. Part 331 (2005).
6. Possession, use and transfer of biological agents and toxins, 9 C.F.R. Part 121 (2005).
7. Casadevall A, Pirofski L. The weapon potential of a microbe. Bethesda, The National Institutes of Health; 2005.