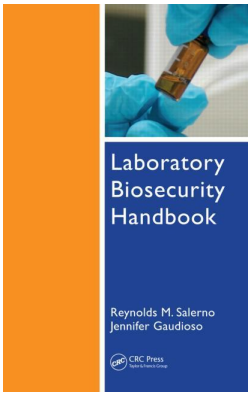

Laboratory Biosecurity Handbook

Reynolds M. Salerno, Jennifer Gaudioso

Components of Biosecurity

Publication details
https://www.routledgehandbooks.com/doi/10.1201/9781420006209.ch3
Reynolds M. Salerno, Jennifer Gaudioso
Published online on: 21 Jun 2007

3 Components of Biosecurity

Physical or engineered security is an important component of a biosecurity system and is often the first thing people think of when they hear the term "security." Sometimes that association has negative connotations, especially when those who understand biology are exposed to security systems that are dominated by traditional physical security that is not designed with any recognition of the unique attributes of biological materials. A comprehensive biosecurity program must include not only physical security but also personnel security, MC&A, transport security, information security, and program management elements (Figure 3.1). These components are the tools in the biosecurity officer's toolkit. The biosecurity officer can select the most appropriate implementation of each element based on his or her facility's unique risks. There are many resources available on the various components of a biosecurity system, especially physical security.[1]

Biosecurity measures should be more stringent for higher-risk scenarios than for lower-risk scenarios. Often, this means that higher-risk agents require more security than lower-risk agents. Low- and very-low-risk agents may require little or no security, whereas moderate-, high-, and extreme-risk agents should receive commensurately higher levels of security. Biosecurity measures should be implemented in a graded manner. A graded protection system is achieved by increasing security incrementally and forming concentric layers of protection around the facility's agents based on the results of the risk assessment. Each layer should have more physical security, personnel security, and MC&A requirements than the previous layer. Information and transportation security requirements will also vary based on the risk assessment, but these controls are not necessarily specific to physical areas within a facility.

This chapter describes each of the critical components of a laboratory biosecurity system. Chapter 4 discusses how to develop and maintain an appropriate biosecurity system using these elements, and Chapter 5 provides specific recommendations for creating biosecurity with combinations of these elements for facilities with different risks.

3.1 PHYSICAL SECURITY

3.1.1 Objective and Principles of Physical Security

Increasing physical security countermeasures is often the most obvious way to reduce the risk that an outside adversary poses and to minimize the threat of those insiders who do not require access to those assets the facility is protecting.

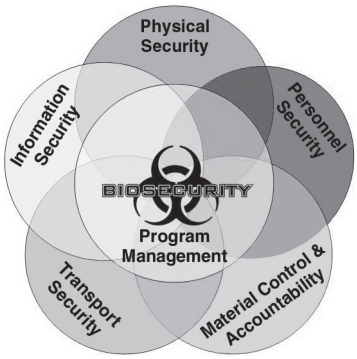

FIGURE 3.1 **(See color figure following page 16.)** Components of biosecurity.

Physical security seeks to reduce the risk of unauthorized access to specific areas or assets. This is accomplished with a mix of several fundamental elements: establishing boundaries, access controls, intrusion detection, and alarm assessment. Access control mechanisms include locks and other barriers to prevent unauthorized individuals from gaining access to restricted items or areas. Intrusion detection systems alert security personnel to attempts to gain access without authorization. Alarms must then be assessed to determine whether they are valid or are false alarms. Valid alarms that have been assessed as either an attempted or successful access to a restricted item or area by an unauthorized individual should be addressed by properly trained response personnel. Response is an important overall element of biosecurity and is addressed in Chapter 4.

3.1.2 Physical Security Elements

3.1.2.1 Perimeters and Other Boundaries

Boundaries must be established to demarcate the areas that are under some sort of access limitation. A fence defines the boundaries of the campus as well as providing a means to control personnel and vehicle access. For facilities that hold only low or moderate malicious use risk agents, signage may provide sufficient property demarcation. Boundaries to restricted areas can include walls, windows, doors, pass-through boxes, pass-through autoclaves, or other equipment access points. Entry and emergency exit doors should be mounted with the hinge pins on the inside of the restricted area, as should any hardware that is associated with securing the doors or windows, such as locks or handles. Exterior ladders should be secured to prevent unauthorized access to roofs and interior courtyards.

The overall layout of the facility and the locations of access control features are important to consider in order to ensure that the normal and emergency paths of employees and visitors do not inadvertently leave gaps in security boundaries. Paths should be analyzed to ensure that routes through applicable checkpoints are enforced without providing alternate, unsecured routes, and that emergency

egress paths do not channel individuals into areas they would not normally have access to. The strength of the perimeter envelope protecting a restricted area will influence how long it takes an outside adversary to gain unauthorized access to the restricted area. The stronger the perimeter is, the longer the "delay" will be between the time of the initial intrusion alarm and the time it takes the outside adversary to gain access to the protected material. The longer the delay, the more opportunity the response force has to respond to an intrusion detection alarm.

3.1.2.2 Access Controls

Access controls provide reasonable assurance that only authorized personnel are allowed to enter a restricted area. The type of access controls selected depends on the level of surety required that only authorized personnel can enter a restricted area. Access can be controlled with a unique item, such as a physical or electronic key. To increase the reliability of the access controls, unique knowledge, such as positive identification by a guard or a personal identification number (PIN), can be required in addition to the unique item. The unique knowledge ensures that the individual who possesses the key is authorized to possess it.

This form of user authentication may also be achieved using biometric devices, which provide a higher level of assurance than a PIN. However, biometric devices are currently limited in utility because some individuals cannot "enroll," i.e., enter a biometric pattern that will subsequently be recognized as their own. This limitation means that any system incorporating biometric devices needs to maintain a separate system of authentication, such as guard identity verification, for those individuals who are unable to enroll in the biometric authentication system.

3.1.2.3 Intrusion Detection

Intrusion detection aims to notify facility staff that an unauthorized individual may have entered or tried to enter a restricted area. At its simplest, intrusion detection is an alert staff member who notices that something is amiss, such as a broken window or an open door that is normally closed. Facilities with only low malicious use risk agents can rely on training their staff to report these types of abnormal situations. Facilities with higher-risk agents can choose between roving guard patrols that are tasked specifically with monitoring the status of restricted-area entry points or electronic intrusion detection systems. Electronic systems have the advantage of providing constant monitoring. Mechanically based systems are inherently less effective than electronic systems but, depending on the facility's level of risk tolerance and local regulations, can be used when electronic systems are too costly or are not available.

Electronic intrusion detection systems are typically associated with electronic access control systems. If forced entry occurs, or if a door or other monitored entryway is open for an extended period of time, an alarm will be generated. The electronic network can be configured to detect tampering so that, if a communication line is cut or a junction box is tampered with, an alarm will be generated

under these conditions as well. Glass-break sensors will send an alarm if a protected window is broken.

Other types of sensors, including motion detection sensors, will generate an alarm if they are triggered. Motion detection sensors, and any other sensor type not associated with detecting a breach in the boundary of the restricted area but within the area itself, often require additional procedural actions in order to ensure they do not alarm during normal daily activities. These types of sensors, unless used in areas personnel are not usually present, can be configured to a "bypass" mode during normal business hours and activated only upon close of business in the area where they are located. Doors to pass-through autoclaves or equipment/maintenance crawl spaces that are large enough for a human to navigate should also be secured and alarmed as appropriate.

Electronic intrusion detection devices send alarm signals to a central monitoring station where security personnel can monitor the entire security system and dispatch alarm assessment and response personnel to the location of the alarm. The area in which the central monitoring station is located should be a restricted area, and the personnel who have the authority to manage the alarms and intrusion detection configuration should be subject to appropriate personnel security measures.

3.1.2.4 Alarm Assessment

If security officials are notified about an attempt by someone to gain unauthorized access to a restricted area, the incident needs to be evaluated or assessed to determine whether the alarm is false or valid. Equipment malfunctions, accidents, and even animals can be the source of a suspected intrusion, and none of these occurrences warrant an official security incident response. Records should be kept on each actual and each false or nuisance alarm. Each record should contain the date and time of the alarm, the cause of the alarm, or a probable cause if a definite cause cannot be established, and the identity of the recorder or the operator on duty. Analysis of these records can indicate what corrective measures need to be taken to minimize the false-alarm rate.

Alarms, when generated electronically, can be assessed in person or by using remote video assessment. If an alarm is triggered, the location and nature of that alarm should be displayed at a central monitoring station. If video cameras are integrated into the security system, they should be configured to record prior, during, and immediately following the alarm event. In other words, the images should be continuously buffered in the video system memory and, if an alarm occurs, the system can retain those segments of memory that represent the images that the video camera recorded 30 seconds prior to and several minutes after the event. This configuration is considerably more efficient than a video surveillance system in which human operators are responsible for detecting security incidents and other anomalies. Properly configured video assessment systems allow an individual who is monitoring the security system to remotely assess an alarm to determine whether further investigation is necessary.

If an alarm is assessed as valid, someone trained and equipped to apprehend an intruder should respond to the alarm. If an on-site guard force, trained in this type of activity, is dispatched to assess the alarm, it may also serve as the response force. If the assessment is conducted by someone who is not equipped to handle an encounter with an intruder, that individual should summon either on-site security personnel or local law enforcement (LE) to respond. Responses to security incidents will be covered in more depth in Chapter 4.

3.1.3 Integration with Laboratory Biosafety

Controlling access to laboratories can also enhance safety by limiting the number of individuals who may be exposed to the hazards. It may be important to restrict access to a certain laboratory to only those individuals who are professionally qualified to be there. Further, in some cases, it may be necessary to limit access to individuals who have proper immunizations. The use of electronic access controls or procedural requirements to log individuals into restricted areas creates a record of who was in the area when. This information could be beneficial during investigations of laboratory safety or security incidents.

Access controls should be implemented with an awareness of laboratory operations and biosafety practices. Biometric readers can be particularly problematic. Fingerprint readers on storage containers, such as freezers, would require personnel to remove their gloves to open the container. Eye scanners may not work properly in situations where personnel are wearing eye protection, such as safety glasses, goggles, or face shields. Removing personal protective equipment (PPE) to gain access will place a burden on the normal flow of operations and may present a safety hazard. If biometric readers are desired, locating the controls at the entrance to the anteroom of a containment laboratory may be operationally feasible. Alternate access controls, such as keys, access cards, or PINs, should also be considered.

Access controls need to be put into practice in a manner that does not hinder emergency response. A mechanism must be in place that allows for the emergency entry of responders but still ensures the security of the protected materials. The mechanism may be based on procedures or systems. Procedural access for responders in emergency situations should be detailed in emergency response plans and may differ depending on the nature of the emergency. For instance, given the low fire load and with a full fire-suppression system in place, some high-containment laboratories have specifically instructed firefighters not to enter a laboratory to fight a fire. Others require emergency responders to wait for the arrival of a designated facility official to enter buildings or specific areas with MMURs and HMURs. Alternately, facilities can choose to provide authorized access to emergency responders by providing them with keys and access codes prior to an incident. This may be best suited for facilities with LMURs and/or MMURs. A key box system may be used. A key box (e.g., "Knox box") is a small,

wall-mounted safe that holds building keys for emergency responders to retrieve in emergencies. This method may be preferred over providing keys to emergency responders, since the keys might become outdated or misplaced. These boxes can provide a single-point security failure if an adversary were to obtain access to the box. To mitigate this risk, it is recommended that any key box be connected to the alarm system. Facilities with high and extreme malicious use risk agents may even consider screening or preauthorizing a small number of emergency responders (either their own or under a Memorandum of Understanding [MOU] with local responders).

Likewise, staff members must be allowed to quickly and safely exit a laboratory during an emergency. However, life-safety measures should not allow an adversary to gain unauthorized access to biological materials by activating an alarm that implements emergency egress procedures. Many life-safety codes require doors to fail safe (i.e., open) in the event of an emergency. Facilities may need to seek an exception from local building codes because doors that fail-safe represent a security vulnerability. An exception may be feasible because it affects only a small, well-defined population that can be trained on specific emergency exit procedures. An emergency exit device may be an acceptable solution. It consists of a push button, crash-out emergency hardware, or similar device, which allows personnel to override the access controls, locks, and any door interlocks. In the event of a power or electronic control failure, the battery backup should enable the system to fail in the secure (locked) condition. Operating the emergency exit device would break the circuit to the lock and allow egress. In the event of loss of both electric power and battery backup, the system should fail in the safe (unlocked) condition. The security plan should document exactly how the system has been designed to meet both safety and security requirements in the event of an emergency.

3.2 PERSONNEL SECURITY

3.2.1 Objective and Principles of Personnel Security

Personnel security is the principal security measure for addressing the Insider threat. It is fundamentally about ensuring that only trusted individuals are given authorized access to restricted areas.

Systems, such as individual badges, can be put in place to identify authorized individuals and escort those individuals who require access but have not been subjected to the same level of evaluation for personnel reliability as an authorized individual. Some level of "trust" must be established prior to allowing anyone full access to sensitive biological materials. This trust can be established through a background investigation; the depth of this investigation should vary with the level of risk that is associated with the agent that the person has access to. These types of investigations are not available in many places and, even when available, they have limitations. For example, individuals (e.g., citizens of other countries) may not have a well-documented history in the country for their backgrounds to

be well-characterized by an investigation. Facilities need to use the tools available to them in screening their insider population and sometimes must think creatively about how to establish whether an individual is worthy of institutional trust in relation to the most sensitive biological materials. Performing due diligence activities prior to entrusting an individual with sensitive duties is a fundamental aspect of operating a facility in general and implementing biosecurity specifically.

3.2.2 Personnel Security Elements

3.2.2.1 Employees

Personnel screening is one part of the process for determining who at an institution should be given authorized access to restricted areas or higher-risk materials. It is also important to consider who has a need to know or needs to have access, especially because personnel screening can never be completely effective. By ensuring that members of the workforce are suitable for the positions they hold, an institution can mitigate the risk of both accidental and malicious acts. The comprehensiveness of the personnel evaluation should be commensurate with the individual's level of responsibility or position risk. Low-, moderate-, or high-risk designations can be assigned to each employment position, based upon the position's level of responsibility and access to dangerous biological agents. A standard set of personnel screening requirements (e.g., background investigations, personality tests) should be developed for each risk designation group. The screening requirements increase in rigor and intensity with increasing position risk, from low to moderate to high.

Individuals in low-risk positions generally have no contact with dangerous pathogens or toxins or do not need access to restricted areas. In general, these individuals do not have duties for which mistakes, poor judgment, or an abuse of position would cause the institution significant harm. Low-risk positions often make up the majority of positions at bioscience institutions. Little or no personnel screening may be needed for these low-risk positions.

Moderate-risk positions are those with duties that are considerably important to the institution, including those with significant program or delivery-of-service responsibilities. Examples of positions that may be considered moderate-risk include scientists and other lab personnel with direct access to MMURs, shipping and receiving personnel who handle MMURs, laboratory support personnel who require unescorted access to areas containing MMURs (e.g., safety personnel, maintenance personnel, housekeeping personnel, animal husbandry personnel), computer/network support personnel without root administrative access, and unarmed security force personnel.

High-risk positions are those positions with duties that have a broad scope of responsibility and authority. These duties are especially critical to the institution because of the potential consequences that could be incurred if the individual performed actions that were not in the interest of the institution. Examples of positions that may be considered high risk include scientists and other lab personnel

with direct access to HMURs, shipping and receiving personnel who handle HMURs, laboratory support personnel who require unescorted access to areas containing HMURs (e.g., safety personnel, maintenance personnel, housekeeping personnel, animal husbandry personnel), supervisors of those in moderate- or high-risk positions, locksmiths for restricted areas, computer/network personnel with root administrative access, personnel with administrative access to the security control system, and armed security force personnel. Individuals who need to be authorized for access to EMURs may also be considered to hold high-risk positions, or the institution may determine that those individuals should be subject to more intensive or frequent background checks.

The efforts made to ensure an individual is trustworthy should be commensurate with position risk. It is often in the best interest of the institution to prequalify prospective employees for moderate- or high-risk positions prior to extending an offer of employment. Not only will time and money be saved by eliminating additional investment in security screening but some institutions may find it very difficult to release an individual from employment once the person has been hired. A basic check of qualifications and references is generally sufficient for this purpose. Some institutions may also choose to include a criminal check as well. For those institutions that hold HMURs or EMURs, it may be valuable to review as many of the easily verified elements of the full security vetting process as possible in the preemployment qualification check. These could include a verification of not only the individual's professional background but also whether he has a criminal background, financial instability, or drug or alcohol dependence. In some extreme cases, personality evaluations can be conducted. Individuals should be granted authorization to enter restricted areas without an escort only after their personnel screening is successfully completed. Institutions can make positions contingent on an employee's ability to successfully meet the personnel screening requirements.

Traditional personnel screening examines an individual's background to see if any derogatory information is uncovered. Derogatory information is unfavorable information regarding an individual that questions the individual's eligibility or continued eligibility for unescorted access authorization to restricted areas or materials. Such information that is uncovered during the personnel screening process should not necessarily disqualify someone for a position. The information can be evaluated for severity, whether it was a recent or distant event, and the frequency of occurrence. Undesirable behavior that is reported repeatedly and is recent may weigh more heavily in the evaluation, possibly raising the issue to the level of a more serious offense. Examples of information that might be considered derogatory include: association with terrorist or criminal organizations, undesirable patterns of conduct (e.g., alcoholism, drug addiction, financial irresponsibility or major liabilities, dishonesty, lack of employability for negligence, misconduct, or criminal conduct), drug-related offenses (e.g., manufacturing, trafficking, sale, or use), major honesty issues (e.g., extortion, embezzlement, or perjury), violent behavior (e.g., rape, aggravated assault, arson, child abuse, or manslaughter), illegal use of firearms or explosives, disorderly conduct, assault, criminal mischief, harassment, or employment-related misconduct (e.g., insubordination, absenteeism, or rules violations), among others.

Not all institutions will have access to resources that would facilitate personnel screening. In those situations, the institution may want to check with local LE agencies to determine if they can provide assistance. LE may be able to provide criminal histories and possibly information regarding terrorist or extremist affiliations. The institution can also speak directly to personal and work-related associates of the individual being hired into a moderate- or high-risk position. The higher the position risk, the broader the scope of the investigation should be, including the number of years in the past that are examined, the number of individuals who are questioned, the types of issues to be explored, and the frequency of reinvestigation.

The institution should have a documented rationale for how the information gathered during the personnel screening will be evaluated and used. All screening results and evaluations should be treated as sensitive information. A single offense of significant consequence may warrant a decision not to hire an individual or to remove an individual from certain duties. A lesser offense might warrant an interview that provides the individual with an opportunity to explain the circumstances under which the offense occurred, possibly providing the institution with the satisfaction that the individual is suitable for the position despite the recorded offense.

Personnel issues should not end once a person has been hired and authorized for access. In addition to regular reevaluation intervals that depend on position risk, there may be situations that warrant an immediate rescreening. For example, if an individual in a high-risk position is arrested for breaking the law, management may initiate a reevaluation. Institutions can also be proactive in helping to create a positive environment that minimizes the likelihood that personal problems may deteriorate into situations of security concern. The U.S. Secret Service has found that when a malicious act is conducted by an insider, a negative work-related event is the most common cause — the individual often has a work-related grievance and is motivated by revenge.[2] These conditions may be observable by an attentive manager or coworker who is willing to notify management, and an active Employee Assistance Program (EAP) may resolve them without incident. An EAP program is a resource for employees who may have questions or concerns about financial matters, mental health, or substance abuse. EAP programs are another mechanism that institutions can use to help ensure that employees can perform their jobs in a reliable and safe manner.

Management is responsible for ensuring that those they supervise are fit for duty. Proactive monitoring of the state of mind and health of employees will reduce the number of safety- and security-related incidents at the facility. Managers and others who are responsible for laboratory operations should intervene when an individual does not appear to be in a suitable state to work. The greater the safety or security risk, the more important it is that there are those who are empowered to temporarily remove an individual from a work environment when that individual's mental or physical health may impair safe and secure operations. Protocols for such removal or suspension should be documented in the facility's policy and be available to employees so that, should such an action become necessary, the individual will understand the basis for the action.

FIGURE 3.2 **(See color figure following page 16.)** Identification badges.

3.2.2.2 Employee Badges

Institutions require some mechanism for identifying which individuals have been given authorized access to which areas. For all but the smallest of facilities, it is not reasonable to expect employees to remember this information; instead, every individual should wear a badge that indicates his or her access authorization. Preferably, such badges will be designed to be difficult to replicate, will include a photograph of the employee, and will possibly have an electronic access mechanism to allow the badge to also act as a key. Employee badges can also include an institution identifier, individual's name, expiration date (visible and encoded if badge contains electronic access control capability), and color coding that indicates which areas the individual is authorized to access (Figure 3.2).

The badge should be worn above the waist with the photograph in full view. A badge should be worn on the institution's property and be required for access to restricted areas, unless the badge might compromise safety. The institution's badge should not be used for unofficial identification. Any time an individual's appearance changes significantly, a new photograph should be taken and a new badge issued. Employee badges should expire at regular intervals (e.g., 5 years) and be reissued with a new photograph. Replacement badges should also be obtained if the badge is damaged in a manner that obscures the features of the photograph or impairs an individual's ability to gain access to authorized areas or materials.

Badges with electronic access mechanisms can be encoded to allow individuals access only to those restricted areas that they are authorized to enter. The badges should be updated if access authorizations change. Authorization is contingent upon meeting the personnel screening requirements of the position, having a need to know, completing biosafety and biosecurity training, and being current on any applicable immunizations.

3.2.2.3 Visitors

The term *visitor* in this context includes any person, employee or otherwise, who does not have access to a restricted area but who has permission to enter and is therefore provided access with an authorized escort. Visitors may also include individuals from outside organizations who have official business at the

institution being visited; these types of visitors may either be short-term casual visitors or longer-term working visitors.

Personal visitors, including personal friends, relatives, spouses, and children, should only be permitted in unrestricted areas during normal business hours, and such visitors should remain in the company of their hosts. The host's supervisor should be notified in the event that a personal visitor is to be on-site for more than a nominal amount of time. Casual visitors include those who are visiting the facility for business purposes but who are not involved in day-to-day operations during their visit. These individuals may go on tours, receive training, or meet with collaborators. Working visitors may fit into various categories, including any individual who is not employed by the institution but who has official business to conduct on the premises.

If a working visitor is anticipated to be on-site for more than a predetermined amount of time (e.g., 30 days) or if the working visitor requires unescorted access to restricted areas, the visitor should be screened in the same manner as an employee who holds a position of equivalent risk. The screening activities should be conducted as soon as the visitor arrives or in advance of the visitor's arrival in order to avoid the impact of long-term escorting. If a working visitor is able to demonstrate to the institution that the requirements associated with the position have already been met, the host institution may allow unescorted access at its discretion.

Visits to restricted areas should be prearranged, and a visitor should display an appropriate badge. Visits to restricted areas should be limited to official business. Visitor parking should be separated from employee parking and security personnel should be responsible for ensuring that vehicles are parked in appropriate areas. Delivery vehicles should be routed appropriately and met by receiving personnel. Drivers should either be precluded from entering restricted areas or kept under escort. All visitors should have a host at the facility being visited responsible for ensuring that all facility policies and procedures are followed and that the visitor is managed in an organized and professional manner. The host is responsible for ensuring that the visitor has completed all appropriate paperwork and is properly escorted.

The host is also responsible for ensuring that each visitor is issued an appropriate badge. A visitor's badge may or may not include a picture; if the visitor is a working visitor, however, a picture badge similar to those issued to employees but with an indication that it is a visitor's badge is preferable. Visitor badges should expire upon termination of the visit or at a standard interval (such as annually), whichever comes first.

Individuals who have not been given authorized access should be escorted. This includes visitors; support personnel who are required to enter the area for maintenance, repairs, or cleaning but who are not cleared for access; and all other individuals without the appropriate institutional identification and keys that would provide them access to a specific area. Those individuals who have not been fully vetted should also remain under escort in restricted areas until their screening is successfully completed and evaluated. It is important to establish clear escort

policies and procedures, such as appropriate visitor-to-escort ratios, responsibilities of the escort or host, and rules for after-hours visitors.

A visitor to a restricted area should fill out a visitor log or have identifying information logged into the area electronically. The visitor log should include the names of the visitor and the escort, their signatures, the visitor's organization, the purpose of the visit, badge number (if applicable), and the times at which the visitor entered and exited the area. Each restricted area should have an actively maintained a visitor log that is in chronological order for a year or more; the log should then be subsequently archived. Those who are not authorized for routine access, but who have legitimate business in the area, should be escorted by an authorized individual and sign a visitor log.

3.2.3 Integration with Laboratory Biosafety

The basic principles of personnel security have many benefits to laboratory biosafety and are often already in place at institutions with strong biosafety programs. It is prudent practice to verify a person's technical background and training before giving the individual access to a laboratory. Such basic screening gives an institution a degree of confidence that personnel can be trusted to work safely with specific biological agents. Institutions typically have more stringent requirements for experience and training before giving personnel access to enter areas that present a higher biosafety risk. Likewise, escorting visitors in laboratories helps ensure their safety.

Identification badges are often used to indicate authorized access and sometimes to enable entry, but they are not compatible with the operating reality of many containment laboratories. In situations where wearing a badge would result in compromised safety, another mechanism for indicating authorized access can be selected, such as a keypad for PIN entry. Another possible solution is to provide a locker or other secure storage space in the anteroom for keys, badges, and other personal belongings. Keys, access cards, and other such devices also present a potential contamination issue in containment laboratories. Do keys need to be decontaminated before removal from the laboratory?

3.3 MATERIAL CONTROL AND ACCOUNTABILITY

3.3.1 Objective and Principles of MC&A

The objective of MC&A measures is to create an environment that discourages insiders from stealing and using biological agents maliciously. MC&A seeks to adopt practices that establish and reinforce responsible oversight of work with dangerous pathogens and toxins.

MC&A measures help enhance laboratory biosecurity by establishing exactly what biological *material* is present at a facility, how and where the material is stored and handled, and who is responsible for it. MC&A combines policies,

procedures, and technologies to augment other elements of laboratory biosecurity during the use, storage, and transfer of material. *Control* ensures that material is confined to known, legitimate use, whereas *accountability* ensures oversight by formally associating material with people and information records. Despite the fact that it is not possible to count every microbe in the laboratory environment, it is possible to take prudent measures to ensure that dangerous pathogens and toxins are controlled in a manner that will deter, and possibly detect, theft of these materials. At a minimum, MC&A measures can facilitate forensic analysis if an illicit diversion is detected.

3.3.2 MC&A Elements

3.3.2.1 Material

The first aspect of MC&A is deciding which materials are subject to control and accountability measures. This decision requires identifying the agents, the form of the agents, and whether quantity is a factor. Ideally, material subject to MC&A should be identified through a rigorous risk assessment; there may also be regulatory requirements that define these materials specifically.

The facility risk assessment (as described in Chapter 2) should identify and categorize those materials that require MC&A measures. In addition to MMUR, HMUR, or EMUR agents, consideration should be given to those subcomponents, any special experimental form, or other variant deemed to present a commensurate risk. MMUR, HMUR, or EMUR agents and their controlled subcomponents and variants are herein after referred to collectively as "dangerous biological agents."

The difficulty in defining "material" subject to MC&A is in the details. Dangerous biological agents can be found in many specimens throughout a typical bioscience institute: repository stock cultures, working stocks, clinical specimens, unknown samples, and genomic material, among other categories. These specimens are also found in many forms: liquid solution, lyophilized powder, in an infected host, in animal waste, and as contamination on equipment or other objects. Genomic libraries of dangerous pathogens and identified virulence genes from an organism may also be considered material from an MC&A perspective. It may not be important to include samples of unknown content unless they are suspected of containing dangerous biological agents. Of course, once a sample has been positively identified as a dangerous biological agent, it should be subject to specific MC&A measures that are appropriate to the agent. It must be clear where specific MC&A measures begin and end for specific agents. The manner in which MC&A is implemented may vary for different types and forms of specimens or agents.

MC&A does not apply to equipment, instruments, clothing, and similar laboratory objects that have been, or may have been, contaminated with materials. These items should be decontaminated and, if necessary, disposed of properly in an appropriate area, foregoing the need to include these items in MC&A procedures.

3.3.2.2 Control

Control is implemented to ensure that materials stay where intended and that they are used for a stated purpose by specifically designated and authorized people. Control must encompass all activities involving the material, such as storage, use, transport (see Section 3.4), and disposal. Control should be effective under both normal conditions and anticipated abnormal conditions wherever possible, such as accidents, power failures, or emergencies. Otherwise, covert diversion of material could be attempted under the cover of an abnormal condition (perhaps intentionally caused).

Control can be accomplished in one of two ways. Physical control is a means of preventing unauthorized access, such as locking a freezer or limiting research with the materials to a restricted area. Control can also be accomplished through operational procedures. Physical and procedural control measures aim to (1) assure the integrity of each material item, (2) assure that no item is missing, and (3) minimize the opportunity for misuse during activities that necessarily involve bulk material.

Storing and using dangerous biological agents in restricted areas and limiting access to these materials to authorized personnel help establish control. A locked freezer or vault can offer additional control in laboratory spaces that are shared among more individuals than actually work with a particular material. Automated systems can log events such as laboratory access (in and out) or freezer opening and closing, often providing date, time, and personal identification. Barcode labels or radio-frequency tags are engineered measures that can facilitate inventory taking. Another physical control mechanism is item integrity, which means establishing a complete boundary around an item so that material within the item cannot easily cross that boundary without detection. Item integrity is usually not practical for working stocks, but it may be valuable for higher-risk repository stocks. It can entail the use of an enclosure ("seal") that would reveal any attempt to tamper with the item. Seals require inspection and verification that should occur periodically, or before intended, legitimate use.

There is often a balance between physical and procedural controls. For example, if the required autoclaves, incubators, centrifuges, or other specialized equipment are not located within the same restricted area, procedural controls can be implemented to ensure materials are under the same standard of control throughout their life cycle.

Procedures, designed in advance and explicitly considering their laboratory biosecurity implications, are central to the effective control of pathogens and toxins. MC&A procedures can typically be integrated with current standard laboratory procedures. MC&A elements may be appropriate to include in many procedures, such as working with the material, inactivating and disposing of the material, conducting inventory checks, labeling sample containers, removing material from storage, and returning it to storage. In addition to procedures for routine activities, unexpected conditions should be anticipated wherever possible. What is the course of action if a sample is discovered missing?

Control is greatly facilitated if material is aggregated into *items*, i.e., discrete, identifiable, and countable units. Material in solution in a test tube or sealed in an ampoule can be aggregated as an item, for example. Similarly, material in an animal carcass might be considered an item, but it would be better if the carcass itself were confined in a sealed box; the box would then become the item. It may not be necessary to define items at the most detailed level possible. An item could be a cabinet or freezer, or even a restricted-access laboratory, provided that control measures can assure item integrity. If it can be done, such higher-level aggregation would obviate any need to count vials.

Regardless of how it is defined, each item should correspond one-to-one with an associated information record for accountability purposes. Although the associated quantity of material within the item can sometimes be specified, it is essentially irrelevant for replicating organisms; any amount is significant. Instead, the number of containers or accountable *items* is the relevant quantity to track for replicating organisms. The quantity of toxins and other nonreplicating materials is meaningful, however. Because the risk for nonreplicating dangerous biological agents is quantity-dependent, the institution can only accurately characterize its risk if it is aware of the total quantity of material at their facility. This implies the necessity of some basic level of MC&A measures for nonreplicating materials, with the sophistication of the controls and accountability increasing with the quantity of material.

3.3.2.3 Accountability

Accountability is the means of ensuring that someone is responsible for the dangerous biological agents stored and/or used within a defined area. Assigning qualified, authorized individuals to oversee the control of protected agents, keeping accurate and timely records, reporting, and auditing are all aspects of accountability.

Each dangerous pathogen and toxin should have a designated "accountable" individual who is knowledgeable about the assigned pathogen or toxin in storage and in use. An accountable individual may be assigned on an agent-by-agent basis, on a per-laboratory basis, or using any other convenient distinction. The critical characteristic of this individual's accountability function is the responsibility of having an ongoing awareness of an agent's status within the laboratory. The accountable individual is responsible for providing information about how, when, where, and why assigned pathogens and toxins have been used, transported, or destroyed, and for maintaining current accountability (inventory) records. Accountable individuals are responsible for overseeing the work associated with their assigned pathogens or toxins. Any anomalies noted by the accountable individual should be reported to the appropriate officials promptly. The head of the facility should be responsible for ensuring that an appropriate accountable individual has been assigned to each dangerous pathogen or toxin located in the facility.

Most records exist for the institution to retain historical knowledge about MC&A-subject material. Exactly how such knowledge is recorded may vary considerably according to the particular circumstances. The objective is to describe

both the existence and use of material accurately in a timely manner, and completely, so that an accountable person can answer questions that could arise later. Laboratory notebooks, inventories as manual ledgers or electronic files and databases, and shipping/receiving receipts are all examples of material records that contribute to accountability. To serve these functions, the information records should unambiguously indicate the specific material and the associated accountable person.

Decisions must be made about several aspects of record keeping:

- *When* must information be recorded?
- *What* information must be kept?
- *How long* must information be kept?
- *Where* should information records be kept?
- What *security* is required for these records?

There is a variety of information that is important to document. First, the attributes of the material must be captured to characterize the material, i.e., to describe what it is. This category includes the agent strain information and possibly its origin, date of acquisition, source history, quantity, and various measured data. A description of the item is necessary to identify which item it is. When multiple items exist, it is especially important to specify the container, identifying information from the label, and its location. It may also be useful to document the status of the material (i.e., active working samples in use, only stored seed stocks exist, material destroyed or transferred to another accountable person or institution) and the associated dates for any relevant change in status. The records should provide the name and contact information of the accountable person for each material. The inventory should include all biological materials that are subject to MC&A measures at the facility. The inventory should cover all repository stocks as well as any unique moderate-, high-, or extreme-risk isolates. The facility inventory should include information about the location of each of the dangerous pathogens and toxins and its associated accountable individual. For higher-risk agents, a certain subset of working samples may also be subject to formal inventory controls.

A physical inventory is used to reconcile these records (the "book inventory") with the materials that are actually at the institution. A physical inventory is accomplished by identifying and listing all subject materials item-by-item in a particular area, such as a laboratory or a workstation within a laboratory. The physical inventory is assembled by a thorough search and review of all locations where the subject materials may exist. A physical inventory should be conducted periodically, with the frequency depending on the agents involved; the higher the risk, the more frequently physical inventories should be conducted. Whenever a physical inventory is conducted, the results should be compared with the current book inventory, and any discrepancies should be identified. If a discrepancy indicates the possibility of theft, or if the discrepancy remains otherwise unexplained, it should be reported immediately to the accountable individual and, if appropriate, local and national authorities. Conducting a physical inventory

includes identifying items, counting items, and occasionally conducting tests to verify contents. When large numbers of items are involved, especially for lower-risk materials, selective (statistical) sampling for identification or diagnosis may be employed.

MC&A information might prove useful to an adversary, so it should be treated as sensitive information and should be subject to information security practices. MC&A information is often intermingled with information recorded for scientific purposes, so care should be taken to prevent sensitive MC&A information from inadvertently being released to the public. A detailed inventory should be kept in a secure, limited-access database.

3.3.3 Integration with Laboratory Biosafety

Measures may already be implemented in various institutions that appear to be (and may in fact be called) MC&A. From a laboratory biosafety perspective, it is important to know what materials are present at an institution, which ones are in active use, which ones are just held in storage, who uses the material, and who is responsible for it. These are the same principles that underlie MC&A for laboratory biosecurity. However, when MC&A measures are already in place at a facility, they should be reviewed explicitly from a laboratory biosecurity perspective and updated as appropriate. New procedures specific to biosecurity should be developed where gaps are identified.

The CDC and NIH *Biosafety in Microbiological and Biomedical Laboratories* (*BMBL*) and the WHO's *Laboratory Biosafety Manual* both require a biohazard sign for laboratories at BSL2 or higher. This sign is intended to provide notification of potential biohazards, such as the specific biological agents, present in the room. The biohazard signs normally include the name of the agent, specific hazards, and contact information of the investigator. Identifying the agent, its location, and the name of those individuals responsible for that agent may conflict with the objectives of biosecurity. Depending on the location of the sign, it can identify the location of biological agents to those who do not have a legitimate need to know that information. The locations of biohazard signs for laboratories with MMURs or higher must be carefully planned to avoid compromising security while providing the necessary level of safety. The first consideration is to assess who has access to the laboratory door where the sign typically would be placed. Is the laboratory in a restricted corridor that can only be accessed by authorized individuals? Does the laboratory have an anteroom? If so, a simple biohazard sign can be placed on the door to enter the restricted access anteroom, and biohazard sign that lists the specific biological agents can be placed on the inner door. A less desirable but still plausible solution may be to post a simple biohazard sign on the laboratory door and place specific information on the biological agents and other hazards in a designated location right inside the laboratory entrance. Personnel with access to the laboratory must then be trained on the location of this information.

3.4 TRANSPORT SECURITY

3.4.1 Objective and Principles of Transport Security

Transport security is a mechanism to implement MC&A to reduce the risks of insider and outsider theft while material is being transported between restricted areas. This transport can be within a facility, between facilities within a country, or internationally.

Scientists, health agencies, and diagnostic laboratories rely on the timely exchange of biological materials for a variety of reasons. During the process of transportation, materials move outside of established restricted areas and may be more vulnerable to theft or tampering. Accountability of the material, documentation, and oversight during the transport process are measures that improve biosecurity. Transport security can reduce the likelihood of (1) inappropriate handling and movement of material by scientists or technical staff, (2) the possibility of loss or misplacement of material during transfer, and (3) the possibility of theft of material for malicious purposes, which may indicate vulnerabilities for terrorist activities as well.

3.4.2 Transport Security Elements

Internal transport is the movement of dangerous pathogens and toxins between restricted areas at a facility. External transport refers to the process of moving dangerous pathogens or toxins between facilities (Figure 3.3).

3.4.2.1 Internal Transport

The usual internal transport process is straightforward. Typically, an individual in the originating laboratory removes a sample from storage, walks it across the facility, and hands the sample to an individual in the receiving location. The receiving laboratory either uses the sample or places it in storage. Such movement may occur as laboratories exchange materials under study; internal transport also

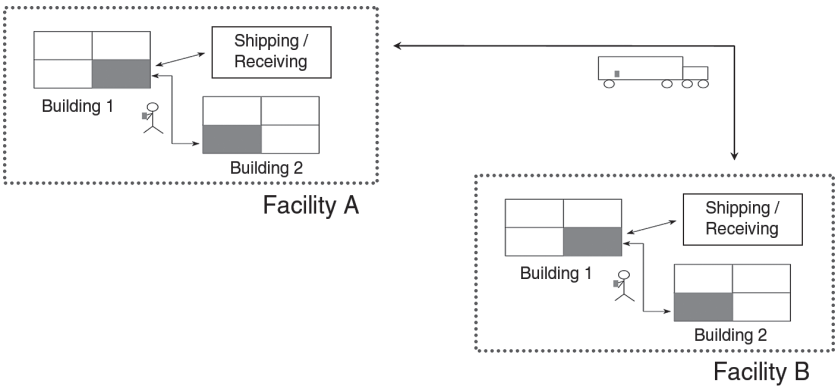

FIGURE 3.3 Transport.

includes materials added or removed from the inventory as a result of shipping and receiving processes, or materials sent to disposal areas (e.g., autoclave and incinerator rooms). Either laboratory or shipping personnel may be responsible for preparing packages in accordance with all appropriate regulations.

Because materials may be vulnerable to theft while outside restricted areas, facilities need to demonstrate prudent and sufficient stewardship of these materials during transport, with more stringent measures in place for the transport of higher-risk materials. A key problem for internal transport is determining at which point a diagnostic sample should be subject to internal or intrafacility transport security procedures. Are the measures implemented upon arrival of a specimen at the facility if it is suspected of containing a dangerous biological agent, or are they initiated after the sample is determined through confirmatory testing to be an agent that requires transport security?

The same basic principles of MC&A are applicable to internal transport security. Everyone who has physical access to dangerous biological agents in transport should be subject to the same personnel security requirements as those required for other individuals with access to the materials in the laboratory. Facilities should recognize that laboratory personnel are not necessarily the only ones with unescorted access to dangerous pathogens and toxins during transport. Transport protocols can be analyzed to determine who may have access to such materials, such as dedicated delivery people. Analysis of transport processes may identify areas that are used for temporary storage, such as shipping and receiving offices or loading docks. Controls should be implemented in these areas at a level equivalent to the restricted areas where the material is stored or used.

Transport of materials should also be integrated into the MC&A protocols. The accountable individual for the material preapproves the transport. For higher-risk materials, a facility may decide that transport must be preapproved by a designated institutional responsible official or biosafety officer (BSO). Prior to approving the transport, the individual ensures that a new accountable individual is identified at the recipient laboratory or verifies that appropriate shipping or destruction documentation is maintained.

Chain of custody refers to the process employed to document who has control of a sample and when. The chain-of-custody process documents that an accountable individual has control over the integrity of the packaged material, and that secure receipt of the material has occurred at the appropriate facility location. Chain-of-custody documentation accompanies the material during transport and includes the name and quantity of material being moved, the shipping and consignee contact information (or laboratory contact information as applicable), and time and date signatures of every individual who assumes control of the material *en route* (e.g., those who initiate delivery, package, or relinquish custody). The chain-of-custody process also documents any situation in which an individual assumes custody on behalf of another individual. If an authorized individual is not able to ensure custody of the package, then the package can be controlled in a restricted area or within an access-controlled cage or freezer. Chain of custody can be achieved via many mechanisms, including paper, where each individual

signs a physical document, or personal digital assistant (PDA) scanners. Chain of custody does not guarantee that a sample will not be stolen. However, it does raise the threshold by introducing a degree of accountability in the transfer process.

3.4.2.2 External Transport

This process likely includes internal transport steps (e.g., to a shipping area or from a receiving area) in addition to relinquishing custody to a commercial carrier or courier. A facility cannot guarantee or oversee the security of material outside of the facility, but consideration of external security issues can limit the possibility of incidents. As warranted by the risk, additional procedural steps can be taken by shipping and receiving facilities to exercise due diligence during all three stages of external transport: preshipment, *en route*, and receipt.

The facility can require laboratorians to obtain preshipment authorization. The authority to approve shipment may change depending on the risk of the material being transported. For lower-risk agents, the accountable individual could be empowered to make shipping decisions, whereas approval from a designated facility representative could be required prior to shipping a higher-risk material. As an element of the preapproval process, the sending laboratory should have knowledge of the professional capabilities of the receiving laboratory. The originating laboratory can notify the receiving laboratory of any shipping-related information (e.g., tracking number, time of shipment, expected time of receipt).

Security while the package is *en route* begins with the selection of a reputable carrier. For higher-risk materials, carriers with transportation security plans can be selected. The opportunity for theft is greatly reduced by limiting exposure time to the commercial transport system. Rapid shipments via air reduce exposure time. Air services may also have well-controlled staging and bulk break areas restricted to authorized employees. Stealing dangerous pathogens or toxins from a commercial overnight carrier would be more difficult than other possible forms of transportation. The packaging should not attract any special attention; labels on the outside packaging should have only the minimum identifying information required by the commercial carrier.

Some air freight service providers provide a *constant surveillance* service. This service can extend the time until delivery and increase the cost of transportation. Because of the additional transportation time, constant surveillance is *not* recommended. Although many commercial carriers provide tracking services, it should be recognized that these services are not in real time, nor do they guarantee custody over a package at all times. However, tracking does provide information regarding the relative position of the package in the transport system and can facilitate creating a document trail for facilities. Facilities can designate individuals who are responsible for package tracking and monitoring during the external transport.

The receiving facility can provide notification to the sending facility that the material has been successfully received. Both laboratories can be prepared to independently and immediately notify the shipping company if any shipment

does not arrive as expected. There should also be procedures for reporting missing shipments of higher-risk agents to appropriate authorities.

Procedures should also be established so that an accountable institutional official is notified in advance that a shipment of dangerous biological materials will be received at the facility. That institutional official can ensure that only authorized individuals receive custody of that particular package when it arrives at the facility, and that it is rapidly delivered to the appropriate restricted area within the facility. Procedures should also be created to accommodate those circumstances when a package of dangerous biological materials arrives at a facility without prior notification or without clear indication of the intended recipient.

3.4.3 Integration with Laboratory Biosafety

Transport security mechanisms must coexist with a large body of safety regulations; must allow for the efficient transportation of all materials, especially frozen materials; and must remain cost effective so as not to unduly hinder the research and diagnostic work that is essential for advancing public and agricultural health.

Limited access to dangerous pathogens and toxins during transport can be complementary to transport safety issues. Restricted access means fewer people to train and less exposure risk in the advent of a spill.

Under safety regulations, the maximum amount of dangerous animal or human pathogens or toxins that may be transferred is 50 ml liquid/50 mg solid by passenger airplanes, and 4 liters liquid/4 kilograms solid by cargo airplanes. Quantity limitations also provide some security benefits. The opportunity for theft is also reduced by limiting the amount of time that the biological agents are outside of restricted areas.

3.5 INFORMATION SECURITY

3.5.1 Objective and Principles of Information Security

Information security is a set of tools and practices used to protect sensitive information. Protecting sensitive information from release is a security measure because release of this information could aid an individual's efforts to steal protected biological agents by indicating how to circumvent the laboratory biosecurity system.

This section is devoted to protecting information that may be considered sensitive, particularly sensitive security-related information. However, other forms of sensitive information, such as personnel and financial records, may also warrant these types of protections, including legitimate restriction from public access. Information, such as experimental data and proprietary information which may be considered a valuable asset, should be held redundantly by the institution, thereby reducing the consequences of loss to a negligible amount and minimizing the risk of theft or sabotage.

3.5.2 Information Security Elements

3.5.2.1 Sensitive Information

The first step in providing information security is identifying information that is sensitive. In this context, sensitive information could help an adversary circumvent the security system to acquire protected biological agents. This type of information not only should be protected from public disclosure but also should be limited to specific authorized individuals. Sensitive security information may be connected to any of the elements of laboratory biosecurity. All physical security information warrants some level of protection. Information regarding physical security plans, user-level access, or other details of the physical security system is sensitive. Similarly, facility plans, including blueprints and other details, may be considered sensitive and need to be protected. Other sensitive physical security information includes physical security system manuals, passwords, and other system-specific details. Laboratory notebooks with MC&A records; material inventories, whether electronic or paper; transportation documentation and similar records may also be sensitive.

In addition to representing an employee confidentiality concern, sensitive personal information can be a biosecurity concern. Background investigation and personality test results could be used in an inappropriate manner to coerce or embarrass a person with access to dangerous pathogens or toxins. Additionally, personnel access authorizations could lead an adversary to target a particular individual for collusion or to monitor that person in the hopes of learning some specific security procedures that may be in place.

A process should be established for review and approval of all potentially sensitive information prior to public release. By implementing such a process, sensitive information can be identified and protected from inadvertent disclosure. Sometimes information can be modified in a way that it is no longer sensitive. Aggregate summaries of inventory information, for instance, may not be sensitive. Generalities regarding risk or security may also be acceptable for public consumption. The review and approval process can be designed to help identify how information can be modified to make it appropriate to release publicly.

Once sensitive information is identified, appropriate security measures can be designed and implemented. These measures encompass handling, storing, transmitting, and destroying such information. The same fundamental principle of limiting access to authorized individuals is central to information security. In addition to personnel screening, authorization requires determining who has a need to know. The owner or originator of the sensitive information should determine who else needs access to that information to execute professional responsibilities. In addition to this need to know, those persons should be authorized to have access to that sensitive information. In most cases, authorization should be dependent upon successfully completing an appropriate amount of personnel screening to determine that the person can be trusted with that sensitive information.

Marking information that has been determined to be sensitive information helps indicate that it requires appropriate protection. The manner in which information is marked depends on the form of the information. For instance, documents may have a cover page identifying them as sensitive information. The top and bottom of each page in a file can be labeled as sensitive. Labels for removable electronic media need to be clearly visible and applied in a way that they do not interfere with the drive mechanisms. Removable electronic media include CDs, DVDs, pen drives, floppy disks, digital tape cassettes, removable hard drives, and any other device on which data can be stored, and that is normally removable from the system by the user or operator.

Sensitive information, both in hard copy and electronic form, should be physically protected and stored within a facility's restricted areas. Institutions need to consider when they will allow sensitive information to be stored and handled outside of their restricted areas. It may be permissible for employees to work at home or on travel if there is a reasonable expectation of privacy and the employee takes measures equivalent to protecting valuable personal property.

Most sensitive information will need to be shared or exchanged between authorized individuals at some point. Facilities will need to determine and institute the appropriate security protocols for transmitting or sharing sensitive information. Sufficiently secure information transfer mechanisms may include in-person discussions, use of telephone landlines (noncellular phones), fax, reputable mail services, restricted access computer networks, or encrypted and authenticated e-mail.

Destruction of sensitive information also needs to be considered. Comprehensive destruction may be warranted. For paper documents, this includes shredding or burning. A hard-drive wiping program provides a similar level of destruction for electronically stored sensitive information. Electronic storage devices can be destroyed through physical damage to the point of inoperability via shredding, degaussing, melting, or other such methods before disposal.

3.5.2.2 Electronic Information

Sensitive information may be found in many electronic formats on stand-alone computers and computer networks throughout the facility. It may be appropriate to store information that is critical to security (e.g., physical security systems, dangerous pathogen inventories) on stand-alone computers or isolated networks within restricted areas to limit the risk of compromise. All elements of the network (routers, servers, Web servers, Web applications, domains, firewalls, wireless local area networks, and remote access) need to be assessed from a security perspective. Strong passwords, desktop management of upgrades and patches, and virus protection are all important aspects of desktop security measures for any computer with sensitive information or with access to a network that contains sensitive information.

Any individual with root administrative access to the administrative or security network needs to be aware of information sensitivity levels and cognizant of any actions taken in the handling and protection of that information. Additional training and policy controls should be implemented for individuals with root access to these systems. Individuals with root access should be screened to the highest level associated with the information or controls that root access provides to them.

3.5.3 Integration with Laboratory Biosafety

MC&A-relevant information is *not* the same as laboratory research results or the scientific content of publications. Classification or limiting the public release of research findings, methods, and techniques is an entirely separate issue. The laboratory biosecurity considerations here are limited specifically to avoiding the release of information about (1) where particular dangerous biological material is and how one might obtain it for malicious use, and (2) what specific laboratory biosecurity measures are in place at specific facilities to protect dangerous biological material. Publications should be reviewed to prevent unnecessary release of such MC&A-relevant information.

Having a clear process for determining what information can be shared with whom can be a significant benefit to laboratory biosafety and the institution as a whole. A well-defined review and approval process can help ensure that the institution does not unduly restrict information from public dissemination. In some cases, without such a process, employees can self-censor information because they do not know what is acceptable to release from a legal and institutional perspective.

References

1. Garcia, M.L., 2001, *The Design and Evaluation of Physical Protection Systems,* Butterworth-Heinemann, Boston, MA; Gregg, M. and Kim, D., 2005, *Inside Network Security Assessment: Guarding Your IT Infrastructure,* Sams Publishing, Indianapolis, IN.
2. U.S. Secret Service and CERT Coordination Center/SEI, May 2005, *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, Washington, D.C., p. 22 [by Michelle Keeney, J.D., Ph.D., Eileen Kowalski at the National Threat Assessment Center, and Dawn Cappelli, Andrew Moore, Timothy Shimeall, Stephanie Rogers at the Software Engineering Institute].