



# Developing a Risk Assessment and Management Approach to Laboratory Biosecurity

Jennifer Gaudioso, Reynolds M. Salerno, and Natalie Barnett

Sandia National Laboratories, Albuquerque, New Mexico

## Abstract

*A growing awareness in the microbiological research and policy communities centers on the need to increase the protection of dangerous biological agents from theft. However, existing security literature and regulatory requirements do not present a comprehensive approach or clear model for biosecurity, nor do they wholly recognize the operational issues within laboratory environments. The modern laboratory operating environment needs to be defined by both biosafety and biosecurity considerations. In addition to being a component of the operating environment, biosafety can serve as a model for biosecurity. Both of these paradigms should be implemented in a graded manner, with increased protection based on the results of a risk assessment.*

*This article proposes a preliminary framework for assessing biosecurity considerations and provides examples that address specific biological materials. The bio can be divided into several fundamental steps: (1) assessing the materials based on their weaponization potential and potential consequences, (2) assessing the potential adversaries, and (3) analyzing security scenarios. The results of the risk assessment form the foundation for risk management and the design of a biosecurity program. By prioritizing risks, the assessment provides a rational basis for allocating scarce security resources.*

## Introduction

Recent events, such as the 2001 anthrax mailings, Aum Shinrikyo's attempts in the mid-1990s to disseminate anthrax and botulinum toxin, and reported al Qaeda interest in biological weapons, have catalyzed a rising sense of urgency concerning potential biological weapons (BW) terrorism and proliferation. As a result, consensus is growing that those biological agents and toxins that could be used as a terrorist weapon warrant increased control and oversight. However, despite the recent release of the final Select Agent Rule (*Federal Register*, 2005), methodologies for achieving an appropriate level of security for such agents and toxins remain in their infancy.

Protecting dangerous pathogens and toxins from

theft may deter some acts of bioterrorism or the development of proliferation networks, but laboratory biosecurity will not definitively prevent all acts of BW terrorism or proliferation or even all diversions of these agents from a bioscience laboratory because most biological agents can be isolated from a wide variety of natural sources. Moreover, biotechnology has advanced so that some virulent and viable organisms can be constructed synthetically or through genetic engineering (Cello et al., 2002; *ISIS News*, 2001).

Nevertheless, many government policymakers and biological weapons experts have recognized the value of implementing laboratory biosecurity. In 2003, the National Academies of Science's report, *Biotechnology Research in an Age of Terrorism*, implored the scientific and policy communities to pursue, among other things, "harmonized international oversight" for the "protection of biological materials and supervision of personnel who work with those materials" (National Academy of Sciences, 2003). In 2004, Homeland Security Presidential Directive 10, *Biodefense for the 21st Century*, argued that "preventing biological weapons attacks is by far the most cost-effective approach to biodefense" and specifically recognized laboratory biosecurity as one of the most effective methods of achieving "proactive prevention" (White House, 2004). The recent report by the U.S. Weapons of Mass Destruction Commission also recommended "encouraging foreign criminalization of biological weapons development and establishing biosafety and biosecurity regulations" (The Commission, 2005).

While it is now essential and appropriate to establish biosecurity systems, practices, and procedures that deter and detect the malicious diversion of dangerous biological materials, it is critically important to strike an appropriate balance between protection of biological material that could be used in a biological weapon and preservation of an environment that promotes legitimate and life-saving microbiological research, diagnosis, and disease control (Salerno, 2004). The authors argue that achieving this balance between security and science should rely upon the implementation of a comprehensive biosecurity risk assessment and risk management methodology. This article outlines the basis for such a methodology.

## The New Laboratory Operating Environment

In the modern laboratory, some biological agents present a risk for deliberate and malicious use. Therefore, it is prudent that bioscience laboratories assess their biosecurity risk and, if necessary, implement appropriate biosecurity measures. When security resources are limited, laboratory biosecurity systems should aim to protect certain biological agents against theft by those who intend to pursue bioterrorism or biological weapons proliferation. If security resources are readily available, an institution's management may also decide to implement a laboratory biosecurity system that protects any agent against theft that could be used in a relatively low-consequence criminal action—such as a biocrime (Salerno, Gaudioso et al., 2004).

Biosafety and biosecurity mitigate different risks, but they share a theoretical approach: They both apply graded protection based on the pathogen or toxin and the environment and manner in which it is used. Biosafety and biosecurity also have some common components, especially physical access controls and program management. In addition, biosafety and biosecurity both include personnel management, material handling and transport protocols, physical security, training, and incident-response planning—although the specifics of these programs will generally differ between biosafety and biosecurity. For example, laboratories want to ensure that staff are qualified to perform their jobs safely (verifying technical backgrounds) and securely (conducting background investigations). And biosafety requires laboratory access to be limited when certain work is in progress, while biosecurity practices limit access to the laboratories that contain certain biological agents.

Resources are always limited, and laboratory managers must determine how to best allocate those resources among many competing demands, such as equipment, supplies, research, maintenance, safety, and security. By providing a means to prioritize risks, the risk-assessment process is the fundamental step in appropriately allocating limited laboratory resources. As the risk increases, protection measures can be strengthened through the number and intensity of controls associated with the item being protected. A graded protection strategy seeks to ensure that the amount of protection and its costs are proportional to the risk. Since some level of risk will always exist, management must decide which risks are unacceptable and must be reduced. Protective measures and incident-response plans should be instituted to reduce risks to an acceptable level.

The U.S. General Accounting Office has endorsed a risk-management approach for mitigating security threats (GAO, 2001; GAO, 2003). In addition, the Select Agent Rule requires security to be based on a risk assessment,

stating that “the security plan must be designed according to a site-specific risk assessment and must provide graded protection in accordance with the risk of the select agent or toxin, given its intended use” (*Federal Register*, 2005).

U.S. laboratories have extensive experience with safety risk assessment, which considers both the likelihood of a laboratory exposure and the hazards the biological materials pose to the individuals within the laboratory. We recommend that a biosecurity risk assessment be based on an evaluation of the likelihood of theft and use of biological material from a laboratory and the hazards such use might pose to the population at large.

## Biological Agent Risk Assessment

Figure 1 provides an overview of the proposed biological agent risk assessment process for determining the appropriate laboratory operating environment. This process can be divided into two fundamental steps: assessing the fundamental risk posed by the agent and examining the factors that may modify that fundamental risk. The biosafety components are already familiar to the bioscience community. The authors believe a parallel process should be adopted for biosecurity. The combined results of the biosafety and biosecurity processes should define the laboratory operating environment. The following sections review the steps outlined in Figure 1. Each section includes a brief discussion of the well-documented biosafety element to provide a context for understanding the comparable biosecurity element.

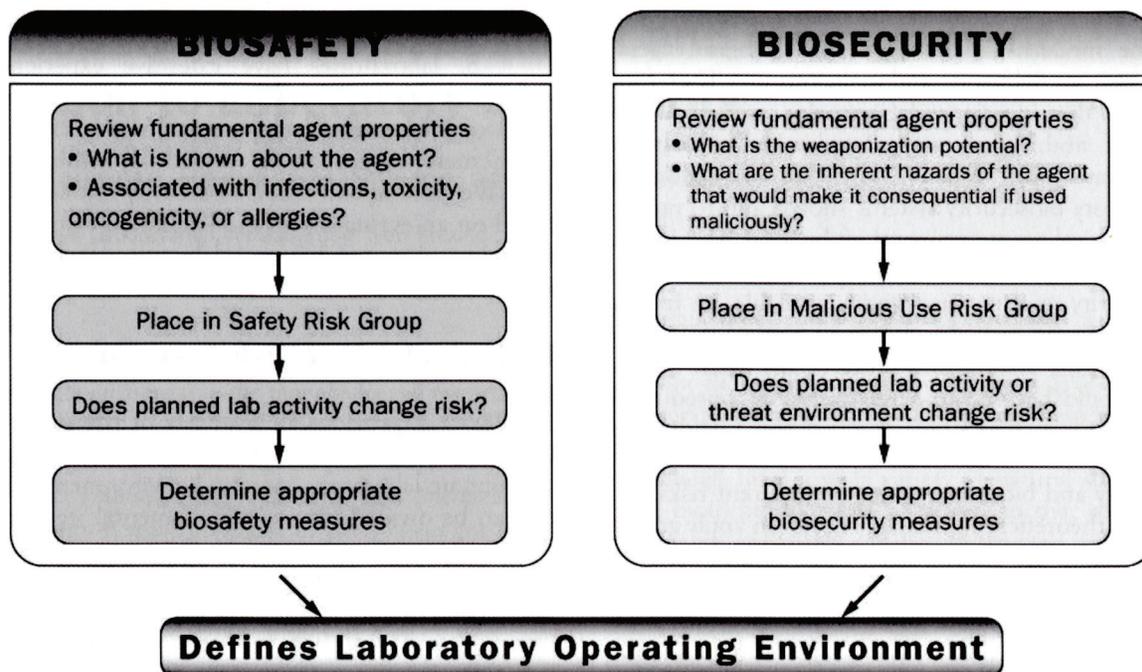
### Fundamental Agent Properties

In a biosafety risk assessment, the first step is to review what is known about the agent, including whether the agent is associated with laboratory-acquired infections, toxicity, oncogenicity, or allergies. This review enables the agent to be assigned to a safety risk group. The third edition of the World Health Organization's *Laboratory Biosafety Manual* describes biosafety risk groups as the starting point to determine appropriate biosafety measures: “One of the most helpful tools available for performing a microbiological risk assessment is the listing of risk groups for microbiological agents. However, simple reference to the risk grouping for a particular agent is insufficient in the conduct of a risk assessment...the assignment of a biosafety level takes into consideration the organism (pathogenic agent) used, the facilities available, and the equipment practices and procedures required to conduct work safely in the laboratory” (WHO, 2004).

A biosecurity risk assessment should start with an analogous review of the agent's potential for malicious use. The fundamental biochemical properties of the agent should be reviewed to consider whether the agent could be effectively used as a weapon. An analysis of an agent's “weaponization potential” should include factors such as

**Figure 1**

Biosafety and Biosecurity jointly define the laboratory operating environment.



the availability of a suitable strain, ease of production (an appropriate quantity in an appropriate form), modes of dissemination, environmental stability of the agent (both in the laboratory and after dissemination), and the availability and level of knowledge required to use the agent as a weapon (Gaudioso, 2004). In addition, the potential hazards of the agent and the effects that it would have on the population at large should be considered. This hazard analysis should evaluate various characteristics of the agent, including infectivity, incubation period, pathogenicity, virulence, lethality, transmissibility, and availability of preventive measures and/or postexposure treatments. An agent's hazard characteristics influence the consequences of malicious use of that agent, such as the numbers of people, animals, or plants killed or sickened, as well as economic and social impacts.

### Malicious-use Risk Groups

This article suggests that five malicious-use risk groups replace the two de-facto levels (protected or not) established by the Select Agent Rule. These are:

1. **Nonpathogenic:** The inherent hazards of the agent would result in no or insignificant consequences if used maliciously.
2. **Low Malicious-use Risk (LMUR):** Pathogens and toxins that are difficult to deploy maliciously, and/or the inherent hazards of the agent would result in low consequences if used maliciously.
3. **Moderate Malicious-use Risk (MMUR):** These pathogens and toxins are relatively difficult to deploy as a

weapon and the inherent hazards of the agent could have localized consequences, causing low to moderate casualties or low to moderate economic impacts, if used maliciously.

4. **High Malicious-use Risk (HMUR):** These pathogens and toxins are not particularly difficult to deploy as a weapon and the inherent hazards of the agent could have national or international consequences, causing moderate to high casualties or moderate to high economic impacts, if used maliciously.

5. **Extreme Malicious-use Risk (EMUR):** These pathogens and toxins would normally be classified as HMUR, except for the fact that they are not found in nature. Since legitimate facilities are the sole source for these materials, higher security measures are worth consideration. Thus, a separate risk group is important for the risk analysis. This could include either eradicated or genetically engineered agents if they were suspected of representing a high-risk pathogen or toxin.

The authors foresee that the overwhelming majority of biological agents would be evaluated as a minimal malicious-use risk (nonpathogenic or LMUR). It is likely that most of the current Select Agents would be evaluated as MMUR. We would expect very few agents to be categorized as HMUR or EMUR since few agents are both easy to use and have the potential to cause high consequences. A security risk assessment may result in higher security than that currently mandated by Federal regulations for those very few agents that represent a high malicious-use risk, and lower levels of security for those agents that

would be considered less attractive to adversaries who are interested in pursuing bioterrorism or BW proliferation.

### Examples of Agent Security Risk Group Assessments

Perhaps the best way to understand why different biological agents warrant different degrees of security is to analyze a few examples. Qualitative, and not comprehensive, risk assessments for selected agents are described below. Not all agents present an equal risk for BW terrorism or proliferation and, thus, not all agents are equally attractive to those individuals who would choose to steal biological agents from a legitimate bioscience facility. The process for malicious-use risk assessment is demonstrated by analyzing the relative ease or difficulty of deploying the agent as a weapon and the public and/or agricultural health and economic impacts of using the agent as a weapon. This type of analysis helps to justify a graded, agent-based approach to laboratory biosecurity.

#### *Mycobacterium leprae*

##### Hazards associated with possible malicious use:

*M. leprae* is the causative agent for leprosy (WHO, 2005). It is a Gram-positive, rod-shaped bacterium that does not form spores. This agent is not highly virulent, and most people who are exposed to it do not develop leprosy. For those individuals who contract the disease, the majority of patients recover without specific treatment; the remaining patients can be cured through a multidrug treatment regimen. *M. leprae* has an incubation period of 2 to 20 years. The person-to-person transmission mechanisms are not fully understood, but *M. leprae* is not highly contagious.

**Weaponization potential:** Production of any quantity of *M. leprae* would be a significant challenge since this agent has never been successfully grown in artificial media or human tissue cultures. *M. leprae* is a very slow-growing organism with a generation time of up to 30 days. *M. leprae* does not form spores so it is not expected to be environmentally hardy.

Based on our analysis, we would consider *M. leprae* to present a low hazard and have a low weaponization potential. We recommend categorizing *M. leprae* as a LMUR.

#### *Coccidioides immitis*

##### Hazards associated with possible malicious use:

*C. immitis* is a fungus that is pathogenic to humans and animals. Infection may cause coccidioidomycosis (also known as Valley Fever or Desert Fever). Coccidioidomycosis is not contagious and there is a high natural immunity in areas where it is endemic. Infection is usually asymptomatic; 30% - 40% of the infected become ill (Deresinski, 2003). Most cases resolve without any treatment. Since only 5 to 10 out of every 1,000 persons infected might develop a life-threatening infection, Deresin-

ski, a *Coccidioides* researcher, concludes "that this fungus is not an outstanding candidate as a weapon of war or of bioterrorism" (Deresinski, 2003). *C. immitis* is not included on the CDC Category A, B, or C lists of potential biological threats, but it is a Select Agent.

**Weaponization potential:** To work with this agent requires technological knowledge. Biosafety Level 3 is recommended for all activities with cultures and for processing soil likely to contain infectious *C. immitis* (Health Canada, 2000). Coccidioidomycosis is the tenth most common laboratory infection. The disease is endemic to arid and semiarid areas of the Western Hemisphere. Because of its wide distribution, the fungus is easy to procure but testing must be done to identify a virulent strain. It is straightforward to grow colonies and induce spore formation (Dixon, 2001). *C. immitis* is not known to have been weaponized by a State program.

Based on our analysis, we would consider *C. immitis* to present a minor to moderate hazard and to have a moderate potential as a weapon. We recommend categorizing *C. immitis* as a MMUR.

#### *Bacillus anthracis*

##### Hazards associated with possible malicious use:

*B. anthracis* are Gram-positive, rod-shaped bacteria that form spores. Aerosolized *B. anthracis* causes pulmonary anthrax, which has a high fatality rate (> 60%) (Dixon, 1999). Diagnosis during the early stages of infection is difficult; anthrax initially presents as a nonspecific, flu-like illness. Pre-event vaccination and early postevent antibiotic treatment can prevent infection. A relatively high lethal dose (LD<sub>50</sub> = 2,500 - 55,000 spores) is required to cause infection (Inglesby, 1999), and anthrax is not transmissible from person to person. *B. anthracis* is listed as a CDC Category A agent.

**Weaponization potential:** *B. anthracis* has been weaponized by many former national programs, including by the United States, Great Britain, the Soviet Union, and Iraq, and it has been used for bioterrorism. Most work with *B. anthracis* can be done safely at Biosafety Level 2. *B. anthracis* is endemic to much of the world, but many strains are weakly virulent, so strain-typing is required. This agent grows readily on all common laboratory media and easily forms spores, which are exceptionally stable in storage and in the environment. Opinions differ as to the ease of aerosolizing the spores. However, the 2001 anthrax letters and a recent Canadian study of an agricultural spraying of a related agent (Levin, 2003) seem to indicate that creating suitable *Bacillus* aerosols may not be so difficult.

Based on our analysis, we would consider *B. anthracis* to present a moderate to high hazard and to have a relatively high weaponization potential. We recommend categorizing *B. anthracis* as a HMUR.

### *Variola major virus*

**Hazards associated with possible malicious use:** The infectious dose for *Variola major* to cause smallpox is unknown but believed to be only a few virions. A vaccine is available that offers high protection when administered up to 24 hours postexposure (Henderson, 1999). Treatment is mostly limited to supportive care. The antiviral cidofovir has been demonstrated to be efficacious against monkeypox and smallpox in animal models and is currently available as an investigational new drug (IND). Since the eradication of smallpox in 1980, relatively few people have been vaccinated against it, providing almost universal susceptibility to the disease in the general public. In the past, epidemics have resulted in an overall 30% fatality rate, although the death rate in infants and children is usually higher. The case fatality rate may be higher in naïve populations; smallpox epidemics among the American Indians resulted in a greater than 50% fatality rate (Henderson, 1999). Smallpox is typically contagious as a respiratory droplet, which requires intimate face-to-face exposure (approximately 3-6 feet), but there have been rare reports of airborne contagion as droplet nuclei (e.g., a hospital outbreak in Germany in 1970).

The carrier is normally not infectious until the pox rash appears, with the first appearance in the throat preceding the rash on the face and hands by up to 24 hours. A prodromal period of 2-4 days of intense fever, malaise, and prostration precedes the rash. During the prodrome, a carrier would not be infectious nor is it likely that he or she would be able to walk around and infect others during the subsequent infectious period when he or she is covered with smallpox. There is a distinct possibility of genetically engineering *Variola* virus to be more virulent. Genetic engineering that results in increased virulence has been demonstrated for other orthopox viruses (Jackson, 2001) and the Soviets are suspected of having worked to increase the virulence of *Variola major* virus (Jane's, 2002).

**Weaponization potential:** *Variola major* was developed and stockpiled for use as a weapon by the Soviet Union, although they have claimed to have destroyed all such agent. *Variola major* is very stable in aerosols (Harper, 1961), displaying significant viability for several hours over a wide range of temperatures and relative humidities. The viral particles remain viable for up to 2 days after release before becoming fully inactivated by the environment. *Variola* virus has been eradicated from nature and legally exists in only two official repositories; therefore, obtaining the virus should be difficult.

Based on our analysis, we would consider *Variola major* to present a high hazard and to have a moderate weaponization potential. The analysis would place *Variola major* in the HMUR category, except that it has been eradicated from nature. Thus, we recommend categorizing *Variola major* as an EMUR.

These qualitative assessments illustrate that not all agents are equally likely to be targeted for diversion by adversaries. The choice of agents for our analysis also demonstrates that, even for Select Agents, there is considerable variation in weaponization potential and associated hazards.

### **Potential Risk Modifiers**

Risk groups provide a baseline for safety and security measures, but other issues should also be incorporated into the risk assessment. The security risk assessment should incorporate the form of the material (e.g., aerosol preparation), the manner of storage (e.g., whether the material is prepared for long-term storage), and the quantities of nonreplicating materials (e.g., toxins)—in other words, those factors that may lower the threshold of development for someone intent on malicious use. Consideration should also be given to those activities that may result in materials that, if used as a weapon, would cause more significant consequences than a similar agent isolated from nature. This may occur when an experiment produces an agent that is more environmentally stable or more virulent than the wild-type agent.

Moreover, security-risk assessments must explicitly identify the individuals or types of individuals in the laboratory's environment who could pose a threat to the dangerous biological materials held by the laboratory. Local law enforcement agencies may assist in the identification of potential adversaries who could perpetrate the theft of a biological agent. These individuals may be grouped into two general categories: insiders and outsiders. Insiders are those individuals with authorized access to the facility, and outsiders are those without authorized access. It is important for the facility's security risk assessment to consider the possible motive, means, and opportunity of those insiders and outsiders who may attempt to illicitly acquire dangerous biological materials.

It should be assumed that the adversary's motive is to steal a particular pathogen or toxin so that he or she can subsequently misuse it to cause or threaten harm. The reasons why an individual would want to misuse a pathogen or toxin vary widely, from ideological to emotional. An individual's motivation could also influence how he or she would choose to misuse a biological agent and the intended results.

The means of an adversary is determined by his or her technical skills and knowledge of the facility's operations. Insiders are not assumed to have the tools to overcome security systems through physical means, but their knowledge of the facility and its operating systems may still give them the means to acquire the material covertly. The insider may also be highly skilled scientifically.

An adversary's opportunity to conduct a malicious act is related to his or her access and proximity to the pathogen or toxins that are intended to be stolen. Outsiders

ers may or may not be part of the threat environment; in general, outsiders do not need to incur the risk of stealing pathogens from even a modestly protected institution when they could easily procure that material elsewhere. By contrast, insiders will always be an element of the threat environment. Some insiders have technical expertise, operational knowledge, access to the materials, and ability to act covertly—all of which reduce the risk to the individual and increase the likelihood of success.

In summary, a laboratory biosecurity risk assessment should evaluate both the technical characteristics of the facility's materials and the motive, means, and opportunity of its potential adversaries. These technical and adversary evaluations should be combined into a series of scenarios, which can be prioritized by risk. The scenarios should be developed based on the results of the first two steps of the biosecurity risk assessment: the agent evaluation and the adversary evaluation. Each scenario is a combination of an agent, an adversary, and an action. The institution's security risk is a function of the probability of each scenario materializing and its associated consequences. The biosecurity risk assessment should rank various security scenarios so that management can choose which risks are unacceptable and prioritize the institution's investment in protection measures and operational restrictions.

In general, the highest risk scenario will likely be covert theft and planned use of a HMUR by an insider; if an insider has the motive, he or she will have the greatest means and opportunity to conduct the act. An overt assault by a terrorist group is expected to be a much lower risk for most facilities since most biological agents are widely available, and terrorists may be expected to balance the value of the facility's assets against the risk of being apprehended while attempting an overt illegal action. Such an attack would also alert the authorities to initiate medical countermeasures, thereby mitigating the potential consequences of a subsequent bioterrorism attack.

### **Risk Mitigation Measures**

After identifying and prioritizing risks, management must decide which scenarios to protect against comprehensively (highest risks) and which to protect against through incident-response planning. Management may also decide that some scenarios need no protection. This risk decision should precede design and implementation of protection measures. The following section outlines a "toolkit" of biosecurity components that can be used to realize the risk decision.

A graded implementation of the components of biosecurity can be used to establish an effective and efficient biosecurity program. These components include physical security, personnel security, information security, material control and accountability, material transport security, and biosecurity program management. Appropriate

biosecurity measures can range from simple, good laboratory and business practices to stringent security measures.

The physical security system can include measures aimed at limiting access to only authorized personnel, detecting unauthorized access, and responding to incidents. Physical security measures may be as basic as locking the doors in unattended laboratories, or controlling access for only authorized personnel by controlled keys. When higher security is warranted (e.g., insider theft of a HMUR agent), electronic access control systems that track when specific individuals enter laboratories can be employed. The access control system can require a unique object (e.g., proximity card) or, for a higher degree of assurance, a unique object and unique identifier (e.g., PIN number) and/or unique characteristic (e.g., biometric). Electronic access control systems generally have alarms that should be monitored and assessed. Response personnel may need to be available to address intrusion alarms. To mitigate the most extreme risks, two- or three-level electronic access controls may be imposed and a full-time, on-site guard force may need to monitor the grounds and respond to alarms.

Personnel security measures help to ensure that the staff who need to handle, use, and store dangerous materials can be trusted not to conduct a malicious act. The sophistication of background investigations can vary depending upon the risk posed by the assets to which the individuals will have access. For low risks, a basic suitability check, such as verifying the accuracy of the individual's resume and calling several references, may be all that is appropriate. Or the results of the risk assessment may suggest that the employer should conduct more detailed background investigations. Elements of background checks can include criminal database checks, terrorist database checks, credit history checks, drug screening, and interviews with the individual's neighbors and colleagues. Employers may also choose to vary the frequency with which these background checks are periodically updated. Other important personnel security measures include photo identification badges and visitor escorting policies.

Material control and accountability (MC&A) establishes points of responsibility for dangerous materials and creates procedures that track the storage and use of those agents. These measures can also be instituted in a graded manner. Each material should have an associated accountable individual who is aware of the use of the material and is accountable for the stocks. Laboratory notebooks can be used to document the stocks, as well as the use and transfer of the agents. For higher risks, the facility may wish to account for and inventory materials in facility-wide databases. Under the most extreme risks, two authorized individuals may be required for access to repository stocks.

Transport security endeavors to provide a measure of

security to biological agents outside of access-controlled areas. Good laboratory practice dictates that a laboratory principal investigator (PI) or another accountable individual is aware of all material transfers and that these are documented in laboratory notebooks or other records. For higher risks, facilities may require that material transport be preapproved and under a continuous chain of custody. Timely shipping methods, such as overnight express, may be selected. The facility may have the recipient provide notification of successful receipt and establish procedures for missing packages. In some cases, material transfer or end-use agreements may be appropriate.

Information security establishes prudent policies for handling sensitive information associated with the biosecurity program. Policies regarding security information, network security, passwords, and e-mail use should be established. Information about the security of these agents should be protected according to the risk that loss of the information presents.

Program management oversees the development and implementation of an effective biosecurity program. A biosecurity plan should guide day-to-day security operations, and incident response plans should describe what specific actions will be taken in the event of a security event at the facility. Depending on the risks at the facility, a Biosecurity Officer or other designated facility representative should oversee the implementation of the biosecurity plan and ensure that the facility is prepared to respond to security incidents. This individual would also provide biosecurity training to those personnel who require it, and perform internal reviews and exercises to evaluate the effectiveness of the biosecurity system.

Any biosecurity program should not unduly hinder the normal operations of the bioscience facility. While biosecurity measures may introduce some level of inconvenience into the existing work environment, they must yield benefits in security and personnel safety.

## Conclusions

This article suggests a mechanism for applying a risk-assessment approach to biosecurity. Over time, the microbiological community may view such biosecurity programs, developed according to an agent-based risk assessment, as providing reasonable control recommendations that are proportional to the security risk. Widely accepted biosecurity risk assessment methodologies would help facilitate international collaborations by creating more uniform standards. Since funding to increase security often comes at the expense of research, risk management should be applied in the most efficient manner possible. Agent-based risk assessment would help to appropriately allocate scarce security resources and ensure that laboratory biosecurity systems achieve genuine national security objectives. Most importantly, this approach would facili-

tate safe and secure biomedical and bioscience research on those agents and toxins deemed most dangerous to human, animal, and plant health. This concept of malicious-use risk groups should be developed and vetted through a collaboration of experts in biological weapons, public and agricultural health, microbiology, and security.

## Author's Note

This work was created under U.S. Government contract by employees of Sandia National Laboratories as part of their official duties. The U.S. Government retains non-exclusive rights to use the work.

## References

- Cello, J., Paul, A. V., & Wimmer, E. (2002). Chemical synthesis of poliovirus cDNA: generation of infectious virus in the absence of natural template. *Science*, *297*, 1016-1018.
- Commission, The. (2005). *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*. Report to the President of the United States, March 31, 2005.
- Deresinski, S. (2003). *Coccidioides immitis* as a potential bioweapon. *Seminars in Respiratory Infections*, *18*, 216-219.
- Dixon, T. C., Meselson, M., Guillemin, J., Hanna, P. C. (1999). Anthrax. *The New England Journal of Medicine*, *34*, 815-829.
- Dixon, D. M. (2001). *Coccidioides immitis* as a select agent of bioterrorism. *Journal of Applied Microbiology*, *91*, 602-605.
- Federal Register*. (2005). Rules and Regulations, Vol. 70, No. 52, 42 CFR Part 73, March 18, 2005 (Department of Health and Human Services, Office of the Inspector General), p. 13294; *Federal Register*, Rules and Regulations, Vol. 70, No. 52, 7 CFR Part 331, 9 CFR Part 121, March 18, 2005 (Department of Agriculture, Animal and Plant Health Inspection Service), p. 13242.
- GAO. (2001, October). *Homeland security: A risk management approach can guide preparedness efforts*. Washington, DC: GAO-02-208T.
- GAO. (2003, September). *Combating bioterrorism: Actions needed to improve security at Plum Island Animal Disease Center*. Washington, DC: GAO-03-847.
- Gaudioso, J., & Salerno, R. M. (2004). Biosecurity and research: Minimizing adverse impacts. *Science*, *304*, 687.

Harper, G. J. (1961). Airborne micro-organisms: Survival test with four viruses. *Journal of Hygiene*, 59, 479-486.

Health Canada. (2000). Population and public health branch, material and safety data sheet, Office of Laboratory Security. Available at [www.hc-sc.gc.ca/pphb-dgspsp/msds-ftss/msds40e.html](http://www.hc-sc.gc.ca/pphb-dgspsp/msds-ftss/msds40e.html)

Henderson, D. A., et al. (1999). Smallpox as a biological weapon. *Journal of the American Medical Association*, 281, 2129-2137.

Ingelsby, T. V., et al. (1999). Anthrax as a biological weapon. *Journal of the American Medical Association*, 281, 1735-1745.

ISIS News. (2001, October) Institute of Science and Society and Department of Biological Sciences, Open University, United Kingdom (UK). No. 11/12. Available at [www.isis.org.uk/isisnews/isisnews11-12.php](http://www.isis.org.uk/isisnews/isisnews11-12.php)

Jackson, R. J., Ramsay, A. J., Christensen, C. D., Beaton, S., Hall, D. F., & Ramshaw. I. A. (2001). Expression of mouse interleukin-4 by a recombinant ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox. *Journal of Virology*, 75, 1205-1210.

Jane's Chem-Bio Web. (2002, December 13). News, genetically modified smallpox. Available at [www.janes.com](http://www.janes.com)

Levin, D. B., & Valadares de Amorim, G. (2003). Potential for aerosol dissemination of biological weapons: Lessons from biological control of insects. *Biosecurity and Bioterrorism*, 1, 37-42.

National Academy of Sciences. (2003). *Biotechnology research in an age of terrorism: Confronting the dual use dilemma*. Washington, DC: Author.

Salerno, R. M., & Estes, D. (2004). Biosecurity: Protecting high consequences pathogens and toxins against theft and diversion. In R. F. Pilch & R. A. Zilinskas (Eds.), *Encyclopedia of bioterrorism defense*, 57-62. New York: J Wiley & Sons.

Salerno, R. M., Gaudioso, J., Frerichs, R. L., & Estes, D. (2004) A BW risk assessment based on historical and technical perspectives. *The Nonproliferation Review*, 11(3), 24-55.

White House. (2004). *Biodefense for the 21st century*. Washington, DC: Author.

World Health Organization. (2004). *Laboratory biosafety manual* (3rd ed.). Geneva: WHO.

World Health Organization. (2005). Elimination of leprosy as a public health problem. Available at [www.who.int/lep/](http://www.who.int/lep/). Accessed August 10, 2005.

## NIOSH Guide

NIOSH has an excellent new guide available for the prevention of occupational exposures to West Nile virus.

[www.cdc.gov/niosh.docs/2006-115/#d](http://www.cdc.gov/niosh.docs/2006-115/#d)

