

## **Biosecurity: Protecting High Consequence Pathogens and Toxins Against Theft and Diversion**

Reynolds M. Salerno, Ph.D.

Sandia National Laboratories, P.O. Box 5800, MS 1373, Albuquerque, NM 87185  
Phone: (505) 844-8971, email: [rmsaler@sandia.gov](mailto:rmsaler@sandia.gov)

Daniel P. Estes

Sandia National Laboratories, P.O. Box 5800, MS 1373, Albuquerque, NM 87185  
Phone: (505) 844-1401, email: [dpestes@sandia.gov](mailto:dpestes@sandia.gov)

October 2003

## *Introduction*

The tragic events of September 2001 and the subsequent dissemination of *Bacillus anthracis* through the United States postal system underscored the dangers to national and international security posed by terrorist attacks, especially those involving pathogenic microorganisms and toxins. Since the time of these incidents, state-sponsored biological weapons programs and terrorists who have developed and/or used biological weapons have received increased attention and concern. In addition, the general public has acquired an unprecedented fascination with, and fear of, the powers of bioscience and bioterrorism.

Many different strategies are now being applied to combat the proliferation and use of biological weapons. Most strategies – such as increasing the effectiveness and availability of vaccines and antibiotics, improving disease surveillance and detection, building public health capacities, and developing biosensor technologies – are reactionary in nature. They focus on improving the ability to detect and respond to a bioterrorist event after it has occurred. The international community has also begun employing preventive strategies. One of the principal strategies in this category is biosecurity, which is the protection of dangerous pathogens and toxins.<sup>1</sup>

Biosecurity aims to stop proliferation before it starts by protecting dangerous pathogens and toxins – the basic building blocks of a biological weapon (BW) – against theft or malicious diversion from bioscience institutions. By preventing potential bioterrorists or proliferant states from acquiring certain dangerous biological materials, biosecurity provides the first line of defense against both state-based BW proliferation and bioterrorism.

Thousands of bioscience facilities around the world conduct critical research on pathogens and toxins that could be used as biological weapons.<sup>2</sup> Yet the academic and private biological research communities – where the majority of this research takes place – have not been accustomed to operating in a security conscience environment. In fact, security applied to microbiology laboratories has often been perceived as ineffective, intrusive, expensive, and likely to obstruct or jeopardize vital biomedical and bioscience research.<sup>3</sup>

It is evident that the increased biological weapons and bioterrorist threat justifies improving control and oversight over certain biological material that could be used as a terrorist weapon. It is now essential and appropriate to establish biosecurity systems,

---

<sup>1</sup> Biosecurity was officially discussed by technical experts from States Parties to the Biological Weapons Convention at an Experts Group meeting in Geneva, Switzerland in August 2003.

<sup>2</sup> Robert Carlson, “The Pace and Proliferation of Biological Technologies,” *Biosecurity and Bioterrorism: Biodefense Strategy, Science, and Practice*, 1:3 (2003), pp 203-214.

<sup>3</sup> Gigi Kwik, et al., “Biosecurity: Responsible Stewardship of Bioscience in an Age of Catastrophic Terrorism,” *Biosecurity and Bioterrorism: Biodefense Strategy, Science, and Practice*, 1:1 (2003), pp 27-36; John Steinbruner, et al., “Controlling Dangerous Pathogens: A Prototype Protective Oversight System,” CISSM Working Paper, February 5, 2003

(<http://www.puaf.umd.edu/CISSM/Publications/AMCS/finalmonograph.pdf>).

practices, and procedures that deter and detect the malicious diversion of these biological materials. However, 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 lifesaving microbiological research.<sup>4</sup>

Balancing security and research at biomedical and bioscience facilities is no trivial matter, especially because few microbiologists are knowledgeable about modern security systems and few security experts have any familiarity with microbiology. Moreover, the concept of biosecurity remains in its relative infancy. In fact, the international microbiological community has not reached a consensus on a clear definition of biosecurity.

### ***Security Fundamentals***

There are at least two fundamental truisms about security. First, a security system cannot protect every asset against every conceivable threat and, second, security resources are not infinite. A degree of risk will always exist and, therefore, it is important to understand and document what risks the facility management is prepared to accept. These are the risks that the security system cannot protect against, which in turn define what the incident response planning must address. Designing a security system compels institutional managers to make important decisions about how limited security resources should be allocated. To make these decisions with confidence, facility managers must be able to articulate and defend the purpose and scope of their security systems.

Security systems should be based on the assets or materials that require protection. Institutional administrators must be cognizant of what materials they possess, the nature and locations of those materials, and who has access to them. Those materials that could cause a national or international security incident if diverted and misused must receive greater protection than other assets. In addition, managers and administrators must evaluate how an adversary would attempt to divert, steal, destroy, or release those assets. Defining which assets are critical to protect and which methods would be employed to harm those assets establishes the security system's objectives and scope.

In addition to appreciating the nature of the assets that require protection, security systems must uniquely apply to the operations of the specific environment. System designers must understand the characteristics and purposes of all the other critical operating systems that will have to interact with the security system. In a biological research environment, one of the most important operational considerations is *biosafety*. Biosafety aims to reduce or eliminate exposure of laboratory workers or other persons

---

<sup>4</sup> Reynolds M. Salerno, et al., "Balancing Security and Research at Biomedical and Bioscience Laboratories," *BTR 2003: Unified Science and Technology for Reducing Biological Threats and Countering Terrorism—Proceedings* (Albuquerque, NM: March 2003). Another paper that addresses biosecurity is Chris Royse and Barbara Johnson, "Security Considerations for Microbiological and Biomedical Facilities," in J. Richmond, ed. *Anthology of Biosafety: V. BSL-4 Laboratories* (Mundelein, IL: ABSA, 2002).

and the outside environment to potentially hazardous agents involved in microbiological or biomedical research. Biosafety is achieved by implementing various degrees of laboratory “containment,” or safe methods of managing infectious materials in a laboratory setting.<sup>5</sup>

Biosafety and biosecurity systems should be complementary, even though biosafety and biosecurity have different objectives and strategies. The objective of biosecurity is to protect dangerous pathogens and toxins, and critical related information, against theft or diversion by those who intend to pursue bioterrorism or biological weapons proliferation. Simply stated, biosafety aims to protect people from dangerous pathogens, while biosecurity aims to protect pathogens from dangerous people. Both methodologies are now critical to the operation of a modern bioscience institution.

Similar in many ways to the practice of biosafety, biosecurity depends on the implementation of comprehensive policies and procedures that affect the facility’s operations only to the extent that is required. Ideally, security measures taken should not hinder a researcher’s ability to perform experiments in a timely manner, delay or prevent authorized access to materials, or impede communication between associates and peers. To the extent possible, the security system should be transparent to those who are required to use it. In other words, the emphasis of biosecurity should be on creating and sustaining a “security culture” at the bioscience facility – a culture where individuals understand the rationale and support the need for systems to protect dangerous pathogens and toxins from theft and diversion.

### ***Challenges Associated with Protecting Pathogens and Toxins***

There are several unique challenges posed by microorganisms that differentiate biosecurity from other forms of high security.<sup>6</sup> First, although certain biological agents have the potential to cause serious harm to the health and economy of a population if misused, all have legitimate uses for medical, commercial, and defensive application. The possession of any one of these inherent “dual use” materials does not necessarily signal an intention to use that material as a weapon. This characteristic is fundamentally different from other materials used in weapons of mass destruction, such as certain chemical materials, which have no peaceful uses.

Second, biological agents are widespread. They exist in nature and are globally distributed in research laboratories, collection centers, and clinical facilities. By contrast, special nuclear materials are much less widely available and, thus, are much more difficult for terrorists to acquire than biological agents.

---

<sup>5</sup> National Institutes of Health and Centers for Disease Control and Prevention, *Biosafety in Microbiological and Biomedical Laboratories*, fourth edition, May 1999 (<http://bmbi.od.nih.gov/contents.htm>); World Health Organization, *Laboratory Biosafety Manual*, second edition (revised), 2003 ([http://www.who.int/csr/resources/publications/biosafety/who\\_cds\\_csr\\_lyo\\_20034/en/](http://www.who.int/csr/resources/publications/biosafety/who_cds_csr_lyo_20034/en/)).

<sup>6</sup> National Research Council of the National Academies, *Biotechnology Research in an Age of Terrorism: Confronting the Dual Use Dilemma* (Washington, DC: October 2003) <http://www.nap.edu/books/0309089778/html/>.

Third, biological agents are living, self-reproducing organisms, the volumes of which continually change throughout legitimate research activities. They can be found in a number of locations within a facility, including freezers, incubators, and infected animals and their waste. Quantification of actual amounts of materials is further encumbered because the amounts of a biological agent required for effective use or as a basis for growth are typically small, involving microgram- to gram-sized quantities.

Fourth, because microorganisms do not emit detectable or recognizable amounts of energy, they cannot be identified with current standoff detection systems. Despite these challenges, protecting certain pathogens and toxins is an essential component of both national and international biological weapons nonproliferation strategies.

In order to design an appropriate security system, which considers all of these unique challenges associated with protecting pathogens, the system designers should employ a biosecurity methodology that aims to establish clear objectives for the biosecurity system. In other words, the system designers should employ a risk management approach that establishes which assets should be protected against which threats.<sup>7</sup> To accomplish this task, the system designers and institutional managers should identify and prioritize the facility's assets, identify the adversaries who would likely attempt to divert or steal those assets, develop scenarios of undesirable events involving those assets and threats, and conduct a security risk assessment incorporating these scenarios.

### ***Asset Identification and Prioritization***

The purpose of the security system must be clear to the organization's management and staff. A fundamental step in achieving this clarity is defining and prioritizing the assets that the security system is designed to protect. Assets should be divided into separate categories based on their consequences of loss (e.g. low, medium, and high). In this manner, the security system can be designed to have graded levels, with the highest consequence assets receiving the highest level of protection, and lower consequence assets receiving appropriately lower levels of protection.

#### **Primary Assets**

High consequence or primary assets are those materials whose loss could result in an event that would have national or international security consequences. The primary assets that a most biosecurity systems should aim to protect are generally limited to dangerous pathogens and toxins. However, not all pathogens are equally likely to be diverted for purposes of biological weapons proliferation and, thus, not all pathogens should receive the same level of security. Agents should be evaluated based on their

---

<sup>7</sup> The US General Accounting Office has endorsed a risk management approach for addressing mitigating security threats. See US GAO, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, DC: October 2001). Also see US GAO, *Combating Bioterrorism: Actions Needed to Improve Security at Plum Island Animal Disease Center*, GAO-03-847 (Washington, DC: September 2003).

attractiveness to an adversary. In other words, how easy would it be to deploy the agent as a weapon, and how significant would the consequences be of using that agent as a weapon?

Those agents that are in a form that would be easiest for an adversary to deploy and perpetrate a high consequence event are the most attractive to an adversary and, thus, are primary assets that require the highest level of security. There are many characteristics of some agents that make them less attractive to adversaries. For instance, if an agent required processing to improve dissemination or virility, were environmentally fragile, required technical equipment or materials to amplify, caused easily recognizable and treatable infectious disease, or was readily defeated by high degrees of local immunity, it would be less attractive to adversaries than other high consequence assets.

Those agents that require the highest level of protection are defined as High Consequence Pathogens and Toxins (HCPTs) – those microorganisms and their by-products that are capable, *through their use as a weapon*, of severely affecting national or international public health, safety, economy, and security. HCPTs are those agents that have the properties and attributes that would make them effective weapons material. They are the agents most likely to be targeted for diversion from a legitimate biological research laboratory for the purposes of bioterrorism or biological weapons proliferation.<sup>8</sup>

Determining which pathogens and toxins are HCPTs, and therefore primary assets, requires an assessment of their infectious disease risk and the risk that the organisms or toxins could be used as, or developed into, a weapon. The important characteristics to consider in this assessment are<sup>9</sup>:

- Infectious disease risk
  - Infectivity (ability to invade a host organism)
  - Pathogenicity (ability to cause disease in a host organism)
  - Lethality (ability to cause death in a host organism)
  - Transmissibility (ability to spread disease from host to host)

---

<sup>8</sup> Three US Codes of Federal Regulations (42 CFR 72, 9 CFR 121, and 7 CFR 331) have defined the “select agents” that must be secured at bioscience facilities in the United States. In the opinion of the authors, all of these select agents are not necessarily HCPTs, and all do not require the same level of protection against theft or diversion. For the US regulations, as well as additional articles and documents on biosecurity, see [www.biosecurity.sandia.gov](http://www.biosecurity.sandia.gov).

<sup>9</sup> US Congress, Office of Technology Assessment, *Technologies Underlying Weapons of Mass Destruction. OTA-BP-ISC-115*, Washington, DC: US Government Printing Office, December 1993; US General Accounting Office, *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks*, Washington, DC: September 1999; William C. Patrick III, “Biological Warfare: An Overview,” in *Proliferation*, Kathleen Bailey (Ed.), Livermore: Lawrence Livermore National Laboratory, . 1994; Raymond A. Zilinskas and W. Seth Carus (National Defense University), *Possible Terrorist Use of Modern Biotechnology Techniques*, April 2002, Unpublished.

- Weaponization risk
  - Availability (number of facilities that house the pathogen or toxin)
  - Ease of amplification (rate of growth, nature of growth media, level of technical equipment and expertise required, etc.)
  - Ease of processing (including ease of aerosolization and increased inhalation characteristics)
  - Environmental hardiness (viability in a broad range of temperatures, hydration levels, light sensitivity, etc.)
  - Lack of availability of countermeasures/immunity (pharmacotherapies or prophylaxis)
  - Ability to be camouflaged as an endemic or common disease

### Secondary Assets

Medium consequence or secondary assets are those materials whose loss could result in an event of somewhat lesser magnitude than the loss of a primary asset, or whose loss could assist an adversary in achieving an event of national or international consequence. Secondary assets could be pathogens and toxins that are not as dangerous as those identified as primary assets, information related to the security system, newly discovered attributes of dangerous pathogens or toxins, or techniques that could be exploited by a terrorist.

Examples of secondary assets in a biological research environment include:

- Pathogens or toxins whose loss would be significant, but something less than the consequences associated with losing an HCPT
- Information related to HCPTs
  - Agent databases containing information on which agents are stored at the facility, where they are stored, and who has access to them
  - Non-public critical information related to the maintenance or manipulation of HCPTs
  - HCPTs shipping and receiving information
  - Information regarding new techniques or discoveries that may aid a terrorist in developing a more effective biological weapon
- Human resources records that reflect personal information of those individuals who work with or otherwise have access to HCPTs, security systems, or computer systems
- Information related to the security system that protects the dangerous pathogens and toxins (e.g. facility blueprints)
- Mission critical systems (e.g. the control centers that manage the security systems, the computer network, and containment-related environmental controls)

### Tertiary Assets

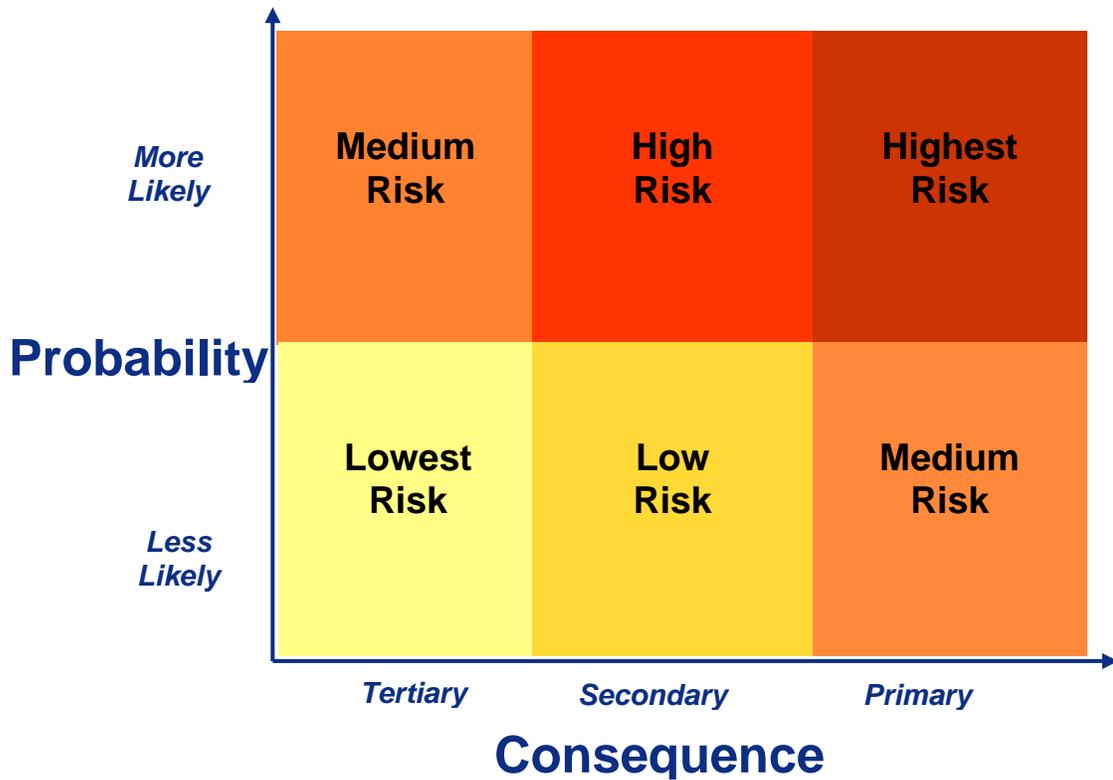
Low consequence or tertiary assets are those materials whose loss could result in an event of somewhat lesser magnitude than the loss of a secondary asset, or whose loss could assist an adversary in gaining access to a secondary asset. Tertiary assets could be pathogens and toxins or types of information that are not as dangerous as those identified as secondary assets. Tertiary assets are often associated with the operations of a facility. Any operational asset that could be destroyed and cause a medium or high level consequence should be redundantly installed. Other operating systems, such as electrical power, air handling equipment, and laboratory equipment, are often designated as tertiary assets at a bioscience facility.

### ***Threat Identification and Security Risk Assessment***

After defining what assets the security system should protect, the institution's management should establish threat scenarios (who, what, when, where, how), and evaluate them based on the relative likelihood of that threat materializing and the associated consequences. This threat identification and security risk assessment process should not be a description of all possible malevolent actions that could befall a facility. Instead, this exercise should evaluate the relative risk of reasonable threat scenarios. Then, the institution's management should decide which of those risks to protect against and which warrant incident response plans.

The threat identification step should define the characteristics, motivations, and capabilities of the adversaries who may attempt to steal or disperse the target assets. What kind of adversary would target this facility? What would the adversary know about the facility? What tools or skills would the adversary have? How might the adversary attack the facility? The objective of this review should be a list of scenarios of undesirable events based on the defined assets and the defined adversaries. For instance, which adversaries would attempt to steal biological agents, which would attempt to steal information, and which would attempt to destroy or deface the facility?

The security risk assessment step should evaluate all of these developed scenarios according to their probability and consequences. The highest risk scenarios are those judged to be more likely than others and with consequences that could result in a national or international security incident. The relative risk of each additional scenario declines as either the probability or the consequences of the event decreases. The following chart depicts the risk prioritization process, which should aim to position each scenario into at least one of the risk levels.



After all of the developed scenarios have been assigned relative risk levels, the institution’s management must decide which risks the security system must protect against. In addition, the risk assessment helps management define which possible but unlikely scenarios the security system should not be required to protect against; these are the risks that the management accepts, and develops incident response plans to address.

This final step in the security risk assessment reflects the management’s level of risk tolerance and/or risk aversion. The more risk tolerant the management is, the fewer resources it will need to invest in security. And conversely, the more risk averse the management is, the more resources it will have to invest in security. Thus, the risk assessment is the critical “resource allocation” step because it helps ensure that funds are expended primarily to prevent the high-consequence and high-probability events.

In general, the security risk assessment of a bioscience facility would reveal that adversaries would not likely conduct an overt external assault to steal agents. First, these agents are not unique materials; they can be isolated in nature and exist in laboratories throughout the world. Second, an overt attack using force would signal authorities to respond with medical and/or agricultural countermeasures that could mitigate the consequences of a bioterrorist attack.

Bioscience facilities should concern themselves with defending against an insider who has approved access. An insider who is willing to divert a primary asset may be a disgruntled employee, or one who is financially desperate, personally threatened, psychologically unstable, or motivated by any number of other reasons. Insiders are

familiar with the protocols of the institution, and have knowledge of, and access to, the asset.

Bioscience facilities should also concern themselves with outsiders who would attempt to steal a biological agent covertly. This type of adversary would likely avoid detection and abort their diversion attempt if they thought they would be caught. These covert outsiders could include visiting scientists, students, and short-term maintenance workers.

Insiders and covert outsiders do not comprise the traditional threat group that high security systems have been designed to protect against. For this reason, it is necessary for the bioscience community, in collaboration with security experts who are knowledgeable about microbiology, to develop, publish, and employ uniquely tailored biosecurity standards that can guide facility managers who are responsible for implementing biosecurity systems.

### *Achieving Biosecurity*

These evaluations – asset identification and prioritization; threat identification; and security risk assessment – determine the objectives of the biosecurity system. The analyses provide the information necessary for the institution’s management to define the assets and threat scenarios that must be protected against, and those that the incident response planning must address. In this manner, the institution’s management sets the design parameters and performance objectives of the biosecurity system.

With these objectives as their parameters, biosecurity experts should conduct a vulnerability assessment that identifies those vulnerabilities of the facility that would allow a high risk scenario to occur. The security system should be designed to mitigate only those identified vulnerabilities that are associated with the risks the institution has decided to mitigate.

It is important to recognize that a security system can effectively protect the defined assets against the defined threats without mitigating every conceivable facility vulnerability. For instance, a facility’s security system may be unable to protect a building from a large-scale physical assault, but may prevent a visiting scientist from stealing a primary or secondary asset. The institution’s management can address the risk of a large-scale assault – a risk that management has decided to accept – through incident response planning.

An effective biosecurity system includes many different components and should not rely on physical security and technologies alone. In fact, the most important aspects of a biosecurity system are procedural and cultural – elements that do not require large expenditures of resources. For example, a biosecurity system should physically consolidate, to the extent possible, all dangerous pathogens and toxins. Access to those biological materials should then be controlled by a combination of door locks or access controls and limiting the number of authorized personnel.

The personnel who receive permission to access these areas should provide evidence that they have a legitimate need to handle, use, or transport dangerous pathogens or toxins, and that they have completed specific biosafety and biosecurity training. In addition, these personnel should be subject to a level of background screening that demonstrates their honesty and reliability. Procedures should also be established for escorting visitors and support personnel who only need occasional access to areas where dangerous pathogens and toxins are located.

A biosecurity system should establish control and accountability of dangerous pathogens and toxins by documenting exactly what materials exist at the facility, where in the facility they are located, who has access to them, and who is responsible for them. Material control and accountability procedures should avoid trying to apply quantitative material-balance inventory accounting principles, which are impossible to achieve in a biological environment.

Because dangerous pathogens and toxins are often transferred between facilities and shared among researchers, it is important for a biosecurity system to implement procedures to document, account for, and control both internal and external transfers of that particular material. Ideally, the procedures would demonstrate continuous custody of dangerous pathogens and toxins during both internal and external transfers.

All of the components of the biosecurity system should be documented in a biosecurity plan, which should be regularly reviewed and revised. In addition, an incident response plan should be written as well as regularly reviewed and revised. These core texts of the biosecurity system, as well as the many biosecurity policies and procedures, indicate that there is also a genuine need for information control and oversight. Biosecurity systems should include procedures for handling, using, and storing certain sensitive information related to the dangerous pathogens and toxins and the various methods for accessing and protecting them.

Perhaps most importantly, a biosecurity system should include a security program management infrastructure that develops and maintains the biosecurity plan and incident response plan, and conducts regular security training for the institution's staff. Creating and sustaining a biosecurity culture is the responsibility of the security program management staff.

### ***Conclusion***

Although biosecurity cannot prevent biological weapons proliferation or bioterrorism, it is appropriate to take steps that reduce the likelihood that high consequence pathogens and toxins could be stolen from a bioscience research laboratory. The increased biological weapons and bioterrorist threat justifies improving control and oversight over those biological materials that could be used to cause a devastating or highly disruptive event. However, a balance between security and research must be achieved in order to protect critical assets as well as allow vital bioscience to advance.

Achieving this balance requires a comprehensive knowledge of the assets, threats, risks, and vulnerabilities associated with bioscience research. The security system, policies, and procedures should be designed specifically to address these unique bioscience characteristics. To achieve this goal, biosecurity objectives must be clearly defined and articulated to the research community. Simply applying the security standards that currently protect other high value or high consequence assets could result in inadequate protection of certain biological agents, inefficient use of limited resources, and the potential jeopardy of biomedical research.