SAND No. 2003-0701C

BALANCING SECURITY AND RESEARCH AT BIOMEDICAL AND BIOSCIENCE LABORATORIES

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**

Natalie Barnett
Sandia National Laboratories, P.O. Box 5800, MS 0759, Albuquerque, NM 87185
Phone: (505) 284-6615, email: **nbarnet@sandia.gov**

Jennifer G. Koelm
Sandia National Laboratories, P.O. Box 5800, MS 1373, Albuquerque, NM 87185
Phone: (505) 845-0743, email: **jgkoelm@sandia.gov**

Presented at
"BTR 2003: Unified Science and Technology for
Reducing Biological Threats and Countering Terrorism,"
University of New Mexico, Albuquerque, NM, 19-21 March 2003

ABSTRACT

This paper argues that bioscience research laboratories must take steps to reduce the likelihood that high consequence pathogens and toxins could be illicitly or maliciously diverted from their facilities. Such a "biosecurity" system should be based on the unique nature of biological material and research, an understanding of biological weapons and bioterrorism, and the articulation of specific system objectives. Using this approach, policy makers, bioscientists, and security engineers can 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 microbiological research.

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under contract DE-AC04-94AL85000

INTRODUCTION

The dissemination of *Bacillus anthracis* through the United States postal system during the fall of 2001, which killed five people and injured 22, provoking supposition that someone who works within a U.S. bioscience laboratory may have been the perpetrator, has led to an increased awareness of the biological weapons and bioterrorist threat. Considerably more attention has been paid to state biological weapons programs and non-state actors who have developed and/or used biological weapons. In addition, the general public has acquired an unprecedented fascination with the possibility of misapplying the powers of bioscience to bioterrorism.

In an attempt to improve the United States' ability to respond to a malicious biological attack, the U.S. Government has allocated $1.8 billion in new funding for biological research on agents and toxins that could be used in bioterrorism. At the same time, the U.S. Government imposed new rules that are designed to improve the security and agent accountability of legitimate biomedical and bioscience research laboratories.

It is estimated that approximately 1,500 bioscience research laboratories in the United States will be captured by these new security requirements.[1] Yet the academic and private biological research communities – where perhaps the majority of this new biological research will take place – historically have not been accustomed to operating in a security conscious environment. In fact, security applied to a microbiology laboratory has often been perceived as ineffective, intrusive, expensive, and likely to obstruct and jeopardize vital biomedical and bioscience research.

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 that deter and detect the malicious diversion of that biological material. However, it is critically important to establish an appropriate balance between protection of biological material that could be used in a biological weapon and preservation of an environment that promotes legitimate microbiological research.

How to achieve that balance is no trivial matter, especially because very few microbiologists are knowledgeable about modern security systems and very few security experts have any familiarity with microbiology. Unfortunately, the recent legislation and the accompanying security regulations raise many questions and assuage few concerns. The bioscience research community needs specific tools to help it achieve this critical balance between security and research.

This paper suggests that biosecurity can provide a level of protection without unduly hindering the research provided that the system's objectives are clearly articulated and reflect an understanding of biological material and research as well as probabilities and consequences of biological weapons use. Specifically, these objectives would include a clear rationale for what material deserves protection and what level of protection is appropriate.

To define these objectives in a manner that considers the uniqueness of biological research, one should conduct a biological agent risk assessment and establish specific threat design parameters. The agent-based risk assessment should evaluate and rank pathogens and toxins based on the consequences of their diversion and their attractiveness to an adversary. Threat design constraints should define how an adversary would most likely attempt to steal the material of highest consequence value from the facility. In the absence of these biologically specific evaluations, and the development of security systems that respond to them, laboratory security systems may fail to reduce the likelihood of malicious diversion of pathogens or toxins, be unnecessarily expensive, and hinder legitimate biological research.

CHALLENGES ASSOCIATED WITH PROTECTING PATHOGENS AND TOXINS

There are several unique challenges posed by microorganisms that should differentiate biosecurity from other forms of high security. First, although certain biological agents have the potential to cause serious harm to the health and economy of a population, all have legitimate uses for medical, commercial, and

defensive applications. A biological agent in a vial is not a weapon. Yet, theoretically, any one cell could potentially be amplified and weaponized with commercially available dual-use equipment. 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. Third, biological agents are living, self-replicating 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 carcasses. And the amounts of a biological agent in use or storage within a research setting are typically small, involving microgram- to gram-sized quantities of material. As a result, it is extremely difficult, if not impossible, to use quantity discrepancies to detect diversion of material.

The U.S. Government recognizes these challenges, but believes that protection of certain pathogens and toxins must be improved and regulated. Protection of these organisms and their by-products is one of many complementary strategies the U.S. Government is pursuing to mitigate the biological weapons and bioterrorist threat. The USA Patriot Act and the Bioterrorism Preparedness Act have codified the protection of certain pathogens and toxins into U.S. law.

USA PATRIOT ACT

The Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act)[2] was signed into law on October 26, 2001 (Public Law 107-55). The purpose of this Act was to increase the capabilities of intelligence agencies to detect terrorist activities and to tighten foreign access to potentially dangerous materials and/or knowledge. Sections 817 and 1012 of this Act are important to biological security concerns.

Section 817 of the USA Patriot Act prohibits "restricted persons" from shipping, receiving, transporting, or possessing any organism on the select agent list. There are eight categories of restricted persons, which include foreign nationals from countries that the U.S. Department of State has declared to be state-sponsors of terrorism – currently Cuba, Syria, Libya, Iran, Iraq, North Korea, and Sudan – as well as fugitives from justice and illegal aliens.[3] It is important to note that the USA Patriot Act neither prohibits microbiological research with any particular agent nor specifies who must conduct research on certain agents.

Section 1012 of this Act authorizes the Attorney General to conduct background checks on any person who attempts to secure a license to transport select agent materials. During this background check, the Attorney General may investigate the individual's immigration status, criminal history, and/or international standing. The overall purpose of these provisions is to ensure limited access to pathogens of concern.

BIOTERRORISM PREPAREDNESS ACT

The Public Health Security and Bioterrorism Preparedness and Response Act of 2002[4] was signed into law on June 12, 2002 (Public Law 107-188). This Act was a response to the fall 2001 anthrax attacks, which increased awareness of the nation's vulnerability to bioterrorism. In order to prepare for future attacks, this Act provides statutes that address three main goals: (1) assessing and improving infrastructure integrity, (2) increasing pathogen security, and (3) augmenting public health capabilities.

In addition to addressing the nation's ability to recognize and respond to a biological weapons event, this law requires steps be taken to protect material that could be used in bioterrorism. Title II, Subtitle A, Section 351A calls for the Department of Health and Human Services (HHS) to revise its list of select agents and toxins that pose a severe threat to public health and safety (PL 104-132). Title II, Subtitle B, Section 212 requires the Department of Agriculture (USDA) to develop its own list of regulated plant, animal, and zoonotic pathogens and toxins. The law mandates laboratories that possess any of these biological agents or toxins to improve their security in order to reduce the likelihood that these materials could be diverted for malicious or illicit purposes.

This law also calls for the establishment and enforcement of standards that govern the transfers of listed agents and toxins, the possession and use of listed agents and toxins, and the safeguard and security of

listed agents and toxins. Individuals who possess or use these agents must be registered and their backgrounds must be checked. The law includes language related to exemptions, inspections, disclosure/nondisclosure of certain information, civil money penalties for violating transfer or possession/use rules, notification in the event of an incident, and other issues.

CODES OF FEDERAL REGULATION (CFRs)

Human Select Agents and Toxins

The specific security requirements of PL 107-188 have been stipulated in three Codes of Federal Regulation – 42 CFR Part 73, 7 CFR Part 331, and 9 CFR Part 121 – that were released as final interim rules in December 2002 and went into effect in February 2003.[5] In 42 CFR Part 73, the Centers for Disease Control (CDC) is designated as the HHS agency that will have regulatory oversight responsibility for the revised select agent rule. This CFR identifies those select agents and toxins that pose a threat to human health and safety (Appendix – Table 1) as well as those "overlap" agents that pose a threat to both human and animal health (Appendix – Table 3).

According to the Bioterrorism Preparedness Act, the select agent list that was originally created under 42 CFR Part 72 should be revised using the following criteria: "(I) the effect on human health of exposure to the agent or toxin; (II) the degree of contagiousness of the agent or toxin and the methods by which the agent or toxin is transferred to humans; (III) the availability and effectiveness of pharmacotherapies and immunizations to treat and prevent any illness resulting from infection by the agent or toxin; and (IV) any other criteria, including the needs of children and other vulnerable populations, that the Secretary considers appropriate."[6]

Agricultural Biological Agents and Toxins

7 CFR Part 331 and 9 CFR Part 121 respond to the sub-section of the Bioterrorism Preparedness Act known as the "Agricultural Bioterrorism Act of 2002; Possession, Use and Transfer of Biological Agents and Toxins." The Animal Plant Health and Inspection Service (APHIS) is designated as the USDA agency that will have regulatory oversight responsibility over this new rule. These CFRs contain lists of agents and toxins of concern specifically to animals (Appendix – Table 2), overlap agents that affect both humans and animals (Appendix – Table 3), and those agents and toxins that can harm plants (Appendix – Table 4).

According to the Bioterrorism Preparedness Act, these lists of agricultural agents and toxins should be created according to the following criteria: "(I) the effect of exposure to the agent or toxin on animal or plant health, and on the production and marketability of animal or plant products; (II) the pathogenicity of the agent or the toxicity of the toxin and the methods by which the agent or toxin is transferred to animals or plants; (III) the availability and effectiveness of pharmacotherapies and prophylaxis to treat and prevent any illness caused by the agent or toxin; and (IV) any other criteria that the Secretary considers appropriate to protect animal or plant health, or animal or plant products."[7]

In addition to the agents and toxins listed, the regulations control genetic elements, recombinant nucleic acids, and recombinant organisms of the listed agents or toxins that are viable pathogens or functional toxins. General exemptions include any select agent or toxin that is in its naturally occurring environment, provided it has not been intentionally introduced, cultivated, collected, or otherwise extracted from its natural source. These lists are reviewed by law every two years, or more often as needed, and will subsequently be republished.

These CFRs also contain, as required by the Bioterrorism Preparedness Act, regulations that govern:

- Entity registration of agent possession
- Designation of a Responsible Official
- Security and risk assessments for individuals with access to regulated agents
- Development and implementation of
    - 42 CFR Part 73: Safety, Security and Emergency Response Plans

    - 7 CFR Part 331: Biocontainment and Security Plan
    - 9 CFR Part 121: Biosafety and Security Plan
- Agent transfer rules
- Safety and security training
- Safety and security inspections
- Notification of theft, loss, or release of regulated agents
- Record maintenance of regulated agent inventories, security plans, etc.
- Notification following diagnostic identification of an agent
- Restrictions on experiments that may result in an increase in pathogenicity, drug resistance, or lethality

SECURITY FUNDAMENTALS

There are at least two fundamental truisms about security. First, a security system cannot protect every asset against every conceivable threat. 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. Second, security resources are not infinite. Designing a security system compels facility managers to make important decisions about how limited security resources will be allocated. To make these decisions with confidence, facility managers must be able to enunciate and defend the purpose and application of their security systems.

Security systems should be based on the asset or material that requires protection. What assets exist at the particular facility that could cause an incident of national security magnitude? What would be the consequences if those assets were diverted from the facility and used maliciously? What makes those assets attractive to an adversary? How would an adversary attempt to steal that material? These types of questions must be addressed and answered in order to articulate a security system's objectives. To achieve balance between security and research in the biological research world, the security system's objectives must reflect an understanding of biological material and research, as well as probabilities and consequences of biological weapons use.

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 and the outside environment to potentially hazardous agents involved in microbiological or biomedical facility research. Biosafety is achieved by implementing various degrees of laboratory "containment," or safe methods of managing infectious materials in a laboratory setting. We believe that biosafety and biosecurity initiatives should be complementary, but we appreciate that the objectives and strategies of biosafety and biosecurity are different and should not be confused. The objective of *biosecurity* is to protect high-consequence microbial agents and toxins, and critical related information, against theft or diversion by those who intend to pursue bioterrorism or biological weapons proliferation.

The measures taken to increase the security of a biological research environment should not obstruct the other critical operating systems within a laboratory and, ideally, the security measures should not hinder the ability to perform experiments in a timely manner or to communicate openly and directly with research associates and peers. To the extent possible, the security system should be transparent to those who are required to use it. The security system should be based primarily on specific policies and procedures – not necessarily security technologies and equipment – that create and sustain a "security culture." The users of the system must be persuaded that security provides a valuable function; without this operational support, no security system will be effective.

AGENT ASSESSMENT AND ASSETS TO PROTECT

The purpose of the security system must be clear to the organization's management and staff. The first question that should be answered to achieve this clarity is "what must the security system protect?" By law, the agents and toxins listed in Tables 1, 2, 3, and 4 must all be protected. 42 CFR Part 73, 9 CFR Part 121, and 7 CFR Part 331 explain that these 82 agents are "those agents that have the potential to pose a severe threat to public health and safety, animal health, plant health, or animal or plant products." They have been chosen because of the high infectious-disease consequences that they would cause to human, animal, and/or plant health.

We believe that the primary assets protected by a high security system should have national security implications. The loss of a primary asset would potentially have consequences so severe that national security could be affected. The secondary assets are those that would assist an adversary in gaining access to or diverting a primary asset. Additional assets at a facility should also be categorized on that same scale. In this manner, the security system should be designed to have graded levels, with the highest risk assets receiving the highest level of protection, and security increasing gradually as one moves physically closer to the assets.

We contend that not all of the CFR-listed agents are equally likely to be diverted for purposes of bioterrorism and, thus, do not have equal national security implications. We believe that the list of 82 agents in the CFRs should be evaluated from a weaponization perspective, so that there could be a gradation of agents ordered from those that require the most security to those that require little or no security. We define those agents that should require the highest level of protection as High Consequence Pathogens and Toxins (HCPTs), and we believe that few of the CFR-listed agents are genuinely HCPTs.

We define HCPTs as 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.

Thus, we argue that biological agents should be evaluated based on both the consequences of their diversion and their attractiveness to an adversary. In other words, determining which pathogens and toxins are HCPTs requires an assessment of their infectious disease risk and the risk that the organisms or toxins could be used as weapons. These are the types of criteria that we believe should be used in identifying the HCPTs that the security system should protect:[8]

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

- Risk that agent would be used as a weapon
  - Availability (*Bacillus anthracis* can be isolated from nature and can be found in at least hundreds of laboratories around the world; *Variola major* can not be isolated from nature and is officially located in only two laboratories in the world)
  - Ease of amplification (rate of growth, nature of growth media, level of technical equipment and expertise required, etc.)
  - Ease of processing (how easily can the organism be processed in a way to facilitate dispersal, such as aerosolization and inhalation?)
  - Environmental hardiness (viability in a broad range of temperatures, hydration levels, light levels, etc.)
  - Availability of countermeasures/immunity (availability of pharmacotherapies or prophylaxis)
  - Ability to be camouflaged as an endemic or common disease.

While HCPTs should be the primary assets of concern, the secondary assets in a biological research environment should include the following:

- Information related to HCPTs
    - Agent databases: what agents, where located, who responsible
    - Non-public critical information related to HCPTs that could be beneficial for conducting bioterrorism
    - Non-public procedures related to HCPTs (e.g. shipping and receiving)
- Human resources records that reflect personal information of those individuals who work with or otherwise have access to material, security, or computer systems
- Information related to the security system that protects the HCPTs (e.g. facility drawings and blueprints)
- Mission critical systems (e.g. the control centers that manage the security systems, the computer network, and containment-related environmental controls).

THREAT ASSESSMENT AND DESIGN PARAMETERS

Once it is clear what the security system should protect, a threat assessment should then establish the design parameters for the system. Specifically, management must decide against whom the security system should protect the target agents. Many mistakenly assume that a threat assessment should be a description of all possible malevolent actions that could happen to a facility, or a prediction of who will attack the facility. Instead, this exercise should determine a baseline threat by describing how an adversary would likely attempt to divert the primary assets or gain access to the secondary assets.

The threat assessment defines the characteristics, motivations, and capabilities of the adversaries who are likely to attempt to steal the target agents. For instance, what would the adversary know about the facility? How would the adversary attack the facility? What tools or skills would the adversary have? How might the adversary be deterred? What risks would the adversary be willing to incur to perpetrate the theft?

By setting the baseline design parameters, the threat assessment establishes which possible but unlikely scenarios the security system should not be required to protect against. These are the risks that the facility accepts, and develops incident response plans to address. Thus, the threat assessment is the critical "resource allocation" step because it helps ensure that funds are only being expended to address the high-consequence and high-probability events.

In general, a threat assessment for the biological research community would conclude that a terrorist commando assault on a university or even a government laboratory is unlikely. With the exception of *Variola major*, the agents could be more easily acquired somewhere else. Moreover, an overt attack using force would signal authorities to take preemptive medical and/or agricultural countermeasures that could significantly mitigate the consequences of the bioterrorist attack. A terrorist organization interested in killing people or embarrassing the government would not likely target a bioscience research laboratory; there are many other better targets to achieve those goals.

Outsiders acting in an overtly hostile manner would not likely try to steal regulated agents for the purposes of committing bioterrorism. Their purpose would likely be to protest animal experimentation or research on genetically modified organisms (GMOs). However, an overt attack on a facility by an animal rights group could result in an inadvertent release of pathogens into the environment, and should be protected against for that reason.

Outsiders who would attempt to steal regulated agents for the purpose of bioterrorism would likely commit their crime covertly. They would avoid detection at all costs and would likely abort their diversion attempt if they thought they would be caught. These covert outsiders would include visiting scientists, students, and short-term contractors.

For a biological research facility, the most likely adversary is someone with approved access. An insider who is willing to divert a regulated agent may be a disgruntled employee, financially desperate, personally threatened, psychologically unstable, or motivated by any number of other reasons. Insiders are the most difficult threat to protect against. They are familiar with the protocols of the institution, including security procedures and technologies.

Insiders and covert outsiders do not comprise the traditional threat group that high security systems are designed to protect against. Security standards for the protection of special nuclear materials and critical federal infrastructure focus almost exclusively on the overt outsider threat groups. For this reason, we strongly recommend that the biological research community develop, publish, and employ unique biosecurity standards.

Unfortunately, the Codes of Federal Regulation for protecting biological agents and toxins provide little guidance on developing threat assessments and baseline design parameters. The CFRs indicate that a "security plan must be based on a systematic approach in which threats are defined, vulnerabilities are examined, and risks associated with those vulnerabilities are mitigated with a security systems approach." This language allows for multiple interpretations of appropriate threat constraints and, therefore, may result in a wide variation of protection levels for similar agents.

ACHIEVING BIOSECURITY

The agent-based risk assessment and the definition of threat parameters together establish the objectives that the security system must meet: the assets that must be protected and the threats that the assets must be protected against. To achieve an appropriate balance between security and research for the biological community, the security system's objectives must be clearly articulated and reflect an understanding of biological material and research, as well as probabilities and consequences of biological weapons use.

After the assets and threats have been defined, biosecurity experts should conduct a vulnerability assessment that identifies those vulnerabilities of the facility that would allow the defined threats to divert the defined assets. The security system should be designed to mitigate only those identified vulnerabilities. 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 not adequately protect the buildings against a car bomb, but may adequately deter a visiting scientist from stealing a regulated agent or toxin.

A system that protects regulated agents against the most likely threats should include many different components. It should not rely on physical security measures or security technologies alone. In addition to physical security components, a comprehensive biosecurity system would implement a personnel reliability program, an information technology security program, and a material control and accountancy program (including security during transfers). Moreover, a comprehensive biosecurity system should establish a security program management infrastructure that would oversee such critical elements as a security training regimen and an internal and external security evaluation and audit process.

The features of the biosecurity system that address the insider threat should include a personnel reliability program, information technology security program, material control and accountancy, controlled access to containment areas where regulated agents are stored or used, chain of custody procedures for the movement of regulated agents beyond the access-controlled areas, and an alarm assessment and response capability. To protect against the outsider threat, the biosecurity system should include visitor screening and escort procedures, an information technology security program, material control and accountancy, intrusion detection and access controls at the likely avenues of approach into the access-controlled areas, and an alarm assessment and response capability.

In summary, an appropriate balance between security and research for a bioscience laboratory can be achieved by following a systematic process designed to establish a protection system that is unique to the biological research environment. Not employing such a process may result in a security system that wastes

valuable resources and fails to adequately protect the designated biological agents and toxins. In order to achieve an efficient and effective biosecurity system, an organization should:

- Establish clear security system objectives
  - Identify assets for protection (agent-based risk assessment)
  - Define threat parameters to protect against (threat assessment)
- Conduct a vulnerability assessment
  - Identifies only those vulnerabilities that would allow the defined threats to divert the defined assets
- Design the system to mitigate the vulnerabilities
- Write a security plan incorporating
  - Program management
  - Personnel reliability
  - Physical security
  - Information security
  - Material control and accountancy (including transfer security)
  - Incident response plan
  - Training
  - Auditing
- Implement the security system and procedures
- Create and sustain a security culture
- Maintain, review, and exercise the security system and plans

CONCLUSION

The anthrax attacks of the fall of 2001, the USA Patriot Act of 2001, the Bioterrorism Preparedness Act of 2002, and new Codes of Federal Regulation have dramatically affected bioscience research in the United States. Scholars have criticized this traditional regulatory response to the biological weapons threat as imposing a "nuclear weapons" perspective on the biological research community. In particular, it has been asserted that this "command and control" approach does not appreciate that "the institutional behavior to be influenced is complex, diffuse, and rapidly changing – all traits that characterize the diverse bioscience community."[9] Some scholars have even suggested that controlling access to dangerous pathogens "is highly dysfunctional in terms of scientific reality and will almost certainly intensify the underlying peril."[10]

We agree that applying standards for protecting special nuclear materials to the biosciences would provide little if any benefit to the increasing threat of bioterrorism and biological weapons proliferation. It would result in a tremendous expenditure of resources; it would not effectively protect the agents of concern; and, most importantly, it could fundamentally jeopardize critical biomedical and bioscience research. In fact, the application of any security standards that do not appreciate the unique nature of biological research could cause these detrimental results.

We also agree that protecting regulated agents alone cannot prevent bioterrorism or biological weapons proliferation. The U.S. biotechnology industry represents only a small fraction of the world's bioscience expertise and possesses only a small portion of the world's biological material; a potential bioterrorist could steal a pathogen from a less secure laboratory overseas or simply isolate an organism from nature. Finally, a biosecurity system cannot protect against the creation of novel, more virulent strains of pathogens, or the misapplication of the powers of bioscience to biological weapons development and use.

Nevertheless, we believe that it is necessary to take steps to reduce the likelihood that high consequence pathogens and toxins could be stolen from a legitimate bioscience research laboratory. 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 to establish systems that deter and detect the malicious diversion of that biological material. We also believe that, as long as these steps are designed specifically for biological materials and research, a biosecurity system can be implemented that is relatively transparent to the research community, uses resources efficiently, and does not unnecessarily hinder bioscience research.

The current regulatory approach could be significantly improved if the long list of regulated agents were evaluated based on weaponization characteristics as well as public and agricultural health criteria. Known pathogens and toxins should be categorized such that those agents most likely to be targeted for diversion, and with the worst consequences if used as a weapon, would receive the highest level of protection. In addition, it is critical that experts in biological weapons, security systems, microbiology, and public and agricultural health collaborate in developing bioscience-specific threat assessments. How biosecurity objectives are crafted will determine whether the resulting systems are effective or destructive.

APPENDIX – TABLE 1
Human Select Agents and Toxins (42 CFR Part 73.4)

Abrin (more than 100 mg)	Toxin
Cercopithecine herpesvirus 1 (Herpes B virus)	Virus
Coccidioides posadasii	Fungi
Conotoxins (more than 100 mg)	Toxin
Crimean-Congo haemorrhagic fever virus	Virus
Diacetoxyscirpenol (more than 1,000 mg)	Toxin
Ebola viruses	Virus
Lassa fever virus	Virus
Marburg virus	Virus
Monkeypox virus	Virus
Ricin (more than 100 mg)	Toxin
Rickettsia prowazekii	Bacteria
Rickettsia rickettsii	Bacteria
Saxitoxin (more than 100 mg)	Toxin
Shiga-like ribosome inactivating proteins (more than 100 mg)	Toxin
South American haemorrhagic fever viruses (Junin (non-vaccine strain (Candid #1)), Machupo, Sabia, Flexal, Guanarito)	Virus
Tetrodotoxin (more than 100 mg)	Toxin
Tick-borne encephalitis complex (flavi) viruses (Central European Tick-borne encephalitis, Far Eastern Tick-borne encephalitis, [Russian Spring and Summer encephalitis, Kyasanur Forest disease, Omsk Hemorrhagic Fever])	Virus
Variola major virus (Smallpox virus)	Virus
Variola minor virus (Alastrim)	Virus
Yersinia pestis	Bacteria

APPENDIX – TABLE 2
Animal Biological Agents and Toxins (9 CFR Part 121.3)

African horse sickness virus	Virus
African swine fever virus	Virus
Akabane virus	Virus
Avian influenza virus (highly pathogenic)	Virus
Bluetongue virus (exotic)	Virus
Bovine spongiform encephalopathy agent	Prion
Camel pox virus	Virus
Classical swine fever virus	Virus
Cowdria ruminantium (Heartwater)	Bacteria
Foot-and-mouth disease virus	Virus
Goat pox virus	Virus
Japanese encephalitis virus	Virus
Lumpy skin disease virus	Virus
Malignant catarrhal fever virus (exotic)	Virus
Menangle virus	Virus
Mycoplasma capricolum/*M*. F38/*M*. *mycoides capri* (contagious caprine pleuropneumonia)	Bacteria
Mycoplasma mycoides mycoides (contagious bovine pleuropneumonia)	Bacteria
Newcastle disease virus (VVND)	Virus
Peste des petits ruminants virus	Virus
Rinderpest virus	Virus
Sheep pox virus	Virus
Swine vesicular disease virus	Virus
Vesicular stomatitis virus (exotic)	Virus

APPENDIX – TABLE 3
Human and Animal Overlap Agents and Toxins (zoonotic) (9 CFR Part 121.3 / 42 CFR Part 73.5)

Bacillus anthracis	Bacteria
Botulinum neurotoxins (more than 0.5 mg)	Toxin
Botulinum neurotoxin producing species of *Clostridium*	Bacteria
Brucella abortus	Bacteria
Brucella melitensis	Bacteria
Brucella suis	Bacteria
Burkholderia mallei (formerly *Pseudomonas mallei*)	Bacteria
Burkholderia pseudomallei (formerly *Pseudomonas pseudomallei*)	Bacteria
Clostridium perfringens epsilon toxin (more than 100 mg)	Toxin
Coccidioides immitis	Fungi
Coxiella burnetii	Bacteria
Eastern equine encephalitis virus	Virus
Francisella tularensis	Bacteria
Hendra virus	Virus
Nipah virus	Virus
Rift Valley fever virus (non-vaccine strain (MP-12))	Virus
Shigatoxin (more than 100 mg)	Toxin
Staphylococcal enterotoxins (more than 5 mg)	Toxin
T-2 toxin (more than 1,000 mg)	Toxin
Venezuelan equine encephalitis virus (non-vaccine strain (TC-83))	Virus

APPENDIX – TABLE 4
Plant Biological Agents and Toxins (7 CFR Part 331.3)

Liberobacter africanus	Bacteria
Liberobacter asiaticus	Bacteria
Peronosclerospora philippinensis	Fungi
Phakopsora pachyrhizi	Fungi
Plum pox potyvirus	Virus
Ralstonia solanacearum, race 3, biovar 2	Bacteria
Sclerophthora rayssiae var. *zeae*	Fungi
Synchytrium endobioticum	Fungi
Xanthomonas oryzae pv. *oryzicola*	Bacteria
Xylella fastidiosa (citrus variegated chlorosis strain)	Bacteria

[1] Federal Register, Rules and Regulations, Vol. 240, No. 67, 42 CFR Part 73, December 13, 2002 (Department of Health and Human Services, Office of the Inspector General), p. 76895; Federal Register, Rules and Regulations, Vol. 67, No. 240, 7 CFR Part 331, 9 CFR Part 121, December 13, 2002 (Department of Agriculture, Animal and Plant Health Inspection Service), p. 76921.

[2] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Public Law 107-55, 107th Congress.

[3] The USA Patriot Act defines "restricted persons" as the following: (1) individuals under indictment for a crime punishable by imprisonment for a term exceeding one year; (2) individuals who have been convicted in any court of a crime punishable by imprisonment for a term exceeding one year; (3) fugitives from justice; (4) unlawful users of a controlled substance; (5) individuals who have been adjudicated as mentally defective or have been committed to a mental institution; (6) illegal aliens; (7) foreign nationals (other than permanent resident aliens) who are citizens of a country that the Secretary of State has determined has repeatedly provided support for acts of international terrorism; and (8) individuals who have been discharged from the Armed Services of the United States under dishonorable conditions.

[4] Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Public Law 107-188, 107th Congress.

[5] Federal Register, Rules and Regulations, Vol. 240, No. 67, 42 CFR Part 73, December 13, 2002 (Department of Health and Human Services, Office of the Inspector General); Federal Register, Rules and Regulations, Vol. 67, No. 240, 7 CFR Part 331, 9 CFR Part 121, December 13, 2002 (Department of Agriculture, Animal and Plant Health Inspection Service).

[6] ''Public Health Security and Bioterrorism Preparedness and Response Act of 2002,'' SEC. 351A, ENHANCED CONTROL OF DANGEROUS BIOLOGICAL AGENTS AND TOXINS.

[7] ''Public Health Security and Bioterrorism Preparedness and Response Act of 2002,'' Subtitle: ''Agricultural Bioterrorism Protection Act of 2002,'' SEC. 212, REGULATION OF CERTAIN BIOLOGICAL AGENTS AND TOXINS.

[8] 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*, 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.

[9] 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.

[10] 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).