Letter from the Biosecurity Task Force

The ABSA Biosecurity Task Force has developed this information paper for our membership to facilitate an understanding of issues related to biosecurity. Legislation has recently been passed that affects organizations and individuals that possess, as well as ship, pathogenic materials and toxins of biological origin, not limited to Select Agents. This will undoubtedly prompt organizations to reexamine their current methods and programs for safeguarding biological threat materials. The first paper ("White Paper") summarizes key points related to understanding biosecurity, while the second paper (by Doug Moore) provides one organization's approach (a work in progress) to developing and implementing a biosecurity plan for its Biosafety Level 3 (BSL-3) facilities. The Task Force will be developing other products to further assist the membership to meet the challenges in safeguarding materials, as well as,to provide recommendations for potential solutions and protective measures.

Barbara Johnson
Chair, Biosecurity Task Force

◆ ◆ ◆ ◆ ◆

ABSA Biosecurity Task Force White Paper: Understanding Biosecurity

ABSA Biosecurity Task Force Members:
Barbara Johnson, Science Applications International Corporation (Chair)
Sandra Fry, Agriculture Canada
Douglas Moore, USDA, Plum Island Animal Disease Research Center
Kenneth Obriot, Wyeth, Security
Chris Royce, SAIC-Threat Reduction Support Center
Stefan Wagener, Health Canada

Introduction

Over the past decade questions have arisen regarding the adequacy of security at biomedical institutes and facilities that work with, store, or transport pathogens and toxins. As an extremist demonstrated he could procure pathogens "for private use" by phone, and since it is possible that an individual with access to a biological research facility may be the perpetrator of the recent anthrax letter attacks, legislation has been passed to increase security at facilities working with, storing, or transporting pathogens and toxins. While information has been published and presented on the topic of biological security over the past years, no comprehensive federal or international guideline has been developed on this topic.

Statement of the Problem

Decades ago the U.S. Government defined and established security and personnel reliability programs in DOE and DOD nuclear and chemical facilities. The material being protected (i.e., processed

nuclear material, warheads, chemical weapons) was bulky in size and would have to be stolen in substantial volume to be of use to a terrorist. The programs were sensitive to national security, often conducted at facilities that were closed to the general public, and relied heavily on the "guards, gates, guns, and two-man rule" approach to security and personnel reliability. This paradigm does not optimally meet the needs of security in biological facilities and may actually give a false sense of protection, while causing significant damage to academia, medical centers, federal programs, and the U.S. biomedical and biotechnology industries. This does not mean there is no need for biosecurity; rather, it means that a security approach must (1) understand the unique aspects of biological work and material, (2) identify the assets and vulnerabilities associated with biological programs, and (3) develop measures that address and solve the problem.

Why Biological Materials Pose Unique Challenges

Several aspects intrinsic to work with biological materials have been identified as key drivers for biosecurity to be implemented differently compared to other security programs. First, biological pathogens can replicate, making the theft of even minute quantities significant. This small amount could easily be obtained from any number of individuals with approved access to working cultures or stocks, infected animals or bedding, laboratory freezers or refrigerators, or from a central storage repository. Access control and mechanisms for monitoring access may deter the average unauthorized individual from entering an area and obtaining pathogens, but do not address the threat of an authorized individual obtaining pathogens for illicit use. It is vital that individuals working with, or with access to, pathogens are responsible, reliable, well trained, and trustworthy.

The second aspect is that there are no devices that detect biological pathogens or toxins being taken from a facility, and any "tag and detection" technology can be defeated if the material taken has not been tagged. While random searches of briefcases may deter some individuals, the minute amounts carried out in a well-hidden vial may never be noticed. Again, individual integrity is of paramount importance.

Finally, pathogens (including "high consequence pathogens") and toxins can be found in clinical laboratories, hospitals, research universities, private industry, and numerous state and federal facilities. Many of these facilities by nature are accessible to the public, have a changing workforce, rely on collaborative effort, and have varying budget constraints. Any biosecurity guideline or program should be developed to meet functional requirements and should allow the institutes to develop a strategy for implementing the requirement.

Approach to Developing a Biosecurity Program

Several components that form the cornerstones in the development of a biosecurity program include the concept of security management, security plan development, security risk analysis, and assessment of proactive and reactive measures. Security management is a systematic process to developing a rational and cost-effective biosecurity program strategy that will protect critical facility and programmatic assets. Security plan development would optimally be a coordinated effort among major stakeholders (i.e., security, biosafety, scientific director, local law enforcement, others). The risk analysis process develops assessments of assets, threats, vulnerabilities, and risk that will then be reviewed in the context of countermeasure applicability. Countermeasures are plans, actions, technologies, or other measures that are taken to prevent, lessen, or respond to a threat. Countermeasures are broadly based on personnel, technical and operational considerations, and solutions. The biosecurity

program should at a minimum address physical protection, personnel suitability/reliability, pathogen accountability (onsite and through the transportation process), and biosecurity incident response.

Proactive Measures to Implement a Biosecurity Program

Measures should fulfill identified functional requirements with consideration to mission objectives, goals, and other operating constraints. Institutes, their biosecurity requirements, and approaches to meeting those requirements may vary. Some applied requirements identified by a broad range of facilities may include general aspects of managed access that encompass visitor control, location of biological materials within a facility and access to biological materials, and material accountability. Approaches should include the development of written and documented security procedures and should optimally provide funding for a designated site security administrator (and trained security staff) to ensure compliance and consistency in implementation. Since one commonality across facilities is that personnel are key assets, a combined approach to (1) adhere to hiring practices that select for honest, well-balanced employees, (2) establish a personnel reliability/suitability program, (3) institute an effective Employee Assistance Program, and (4) raise the level of security awareness among employees may be among the most important factors in developing an effective biosecurity program.

Conclusion

As a discipline, biosecurity has been evolving at institutes and across various agencies and industries in an independent manner. It would be beneficial to develop a national guideline or set of recommendations for biosecurity in facilities working with, storing, and transporting pathogens. A proponent organization that develops these guidelines will have to intimately understand the intricacies and unique aspects of pathogens and work with pathogens. While various Government agencies are developing their own regulations, a unified approach would be of national and international benefit. The Task Force is in the process of developing a supplemental pamphlet to provide more applied information regarding how to identify requirements and implement a biosecurity program.

◆ ◆ ◆ ◆ ◆

A Summary: USDA's Security Policies and Procedures for Biosafety Level 3 Facilities

Douglas M. Moore
Plum Island Animal Disease Center

The USDA's Agricultural Research Service (ARS) and the Animal and Plant Health Inspection Service (APHIS) operate high-level biocontainment laboratory facilities that work with crop, animal, zoonotic, and human pathogens. These are Biosafety Level 3 (BSL-3) or USDA's enhanced BSL-3 biocontainment laboratories (referred to as BSL-3 Agriculture or BSL-3AG). If released into the environment, some pathogens could pose a risk to plant and animal production within the United States. Also, if mishandled certain pathogens could also be a threat to human health. USDA facilities working with these pathogens have biosafety programs designed to the specific needs of each laboratory. In the past, these biosafety programs varied from facility to facility due to the different organisms being