



Biosecurity: Challenges and Applied Solutions for Our Future Needs

Conference Abstracts

April 22-23, 2003 at the Hilton Alexandria Mark Center Hotel, Alexandria, Virginia

A conference hosted by the American Biological Safety Association, Canadian Centers for Applied Biosafety, and Science Applications International Corporation, in partnership with the American Industrial Hygiene Association.

Biosecurity, Bioterrorism and Plant Pests

James Lackey

United States Department of Agriculture
Riverdale, Maryland

Plant Protection and Quarantine (PPQ), the United States Department of Agriculture has traditionally regulated the importation into the United States, or interstate movement, of plant pests under a permit system, which allowed for research or similar purposes in contained facilities. This system was designed to prevent the dissemination of these pests, including pathogens, arthropods, parasitic, and other weeds, nematodes, and others, into the environment of the United States where they could cause economic and other losses. Depending on the nature of the organisms and the scope of the work, these facilities may require laboratory, growth chamber, or greenhouse components. Many are designed specifically for this kind of work and can be expensive. The permits are issued under regulations of the Plant Protection Act (PPA). The regulations, and the Act, do not provide a detailed set of standards for containment, biosafety, or biosecurity. They only provide for inspections and a determination of ade-

quacy of the facility to prevent plant pest dissemination. Since these are plant pests, and thus economic pests, they have little, if any, human health concerns. Therefore, many of the safeguards to protect workers in containment facilities for medical pathogens are not needed. On the other hand, host plants in the containment facility are often infected or infested with these organisms, and the potential for spores or other disseminules within the interior of the facility exists, with possible escape to the outside.

The Agricultural Bioterrorism Protection Act (ABPA) adds an additional strong set of new requirements to this permit system for a small subset of the previously regulated pests. Currently there are 10 pathogens listed under PPQ regulations for ABPA; *Liberobacter africanus*, *Liberobacter asiaticus* (Huanglongbing = Greening disease, citrus), *Peronosclerospora philippinensis* (Philippine downy mildew, corn), *Phakopsora pachyrhizi* (soybean rust, soybean), plum pox potyvirus (plum pox, stone fruits), *Ralstonia solanacearum* R3 B2 (bacterial wilt brown rot, potato), *Sclerophthora rayssiae* var. *zeae* (brown stripe downy mildew, corn), *Ancytrium endobioticum* (potato wart or potato canker, potato), *Xanthomonas oryzae* pv. *oryzicola* (bacterial leaf streak, rice), *Xylella fastidiosa* (citrus variegated chlorosis, citrus). Under the ABPA, these pathogens will be subject not only to stringent containment requirements for the physical facility, procedures, and personnel, but they will also be subject to a defined set of requirements to protect against the use of such agents in domestic or international terrorism or for any other criminal purpose. These requirements include personnel background checks, restricted access and other secu-

city systems, training and skills review, recordkeeping and inventory control, incident response procedures, and others. There is also a provision for exemptions for certain diagnostic laboratories and specific exemptions for good cause.

Department of Defense (DoD) Policy on Safeguarding Biological Select Agents

Christina Bromwell
Department of Defense
Washington, DC

The Deputy Secretary of Defense approved the interim policy for safeguarding biological select agents and toxins furnished by or in the custody or possession of the DoD at the beginning of February. The policy was effective immediately.

It requires compliance with the registration requirements of title 42, Code of Federal Regulations, Part 73 and directs the development of minimum standards to ensure that biological select agents and toxins are properly safeguarded against loss, theft, diversion and unauthorized access or use.

The policy is applicable to all DoD Components that furnish, have custody or have possession of biological select agents or toxins justified by a prophylactic, protective, bona fide research or other peaceful purpose to support biological defense programs, medical research, clinical diagnostic testing, or teaching. The policy also applies to DoD contracts for which performance depends on access to DoD biological select agents or toxins.

The Army Approach to Biological Surety

John Humpton
Department of Defense
Washington, DC

The presentation will review the Army's approach to developing a biological surety program. It will identify the factors leading to the decision to establish the program, the process that was used to develop the program, and the elements of the pro-

gram. The presentation will address the relationship of the Army's program to other efforts at the Department of Defense and national levels.

Bioterrorism: Impact and Implications for Biosafety

Maureen Best
Health Canada
Ottawa, Ontario, Canada

The biosafety community has traditionally been involved in laboratory safety issues regarding the safe handling of biological agents. We are now seeing biosafety practitioners handling bioterrorism issues including biosecurity and emergency response to suspicious packages. With growing concern about the possible use of biological agents from laboratories as agents for bioterrorism, the regulatory environment is changing to prevent such misuse of pathogens. We are also seeing greater movement towards international harmonization of biosafety requirements to secure movement of pathogens between facilities.

In response to questions regarding the adequacy of security at laboratories who work with, store or transport pathogens and toxins, biosecurity guidelines have been developed to prevent unauthorized entry to laboratory areas and to prevent the unauthorized removal of biological agents from laboratories. Traditional emergency response plans for biosafety practitioners have been augmented to include plans specifically for bioterrorism incidents. In the area of decontamination, we have adapted our standard decontamination plans and procedures to non-laboratory areas including office buildings and mail rooms.

The scope of work carried out in clinical laboratories is changing to include diagnostics for bioterrorism agents, which in turn has led to a steady increase in the demand for and construction of containment facilities. National and international laboratory response networks to efficiently and effectively manage bioterrorism incidents are being developed. Biosafety specialists assigned to arrange shipments of biological specimens and bioterrorism samples to laboratories have encountered significant

difficulties. The urgency of these shipments necessitates a 24/7 transportation capacity. Changes to ensure the security of such shipments are also being considered by national and international transportation regulatory authorities.

Laboratories are being asked to collaborate with the first responder community to respond to and analyse anthrax hoax letters and suspicious packages for the presence of biological pathogens of concern. In direct response for rapid diagnosis in the field by the first responder community, we are also seeing the movement of the laboratory to the field. Traditional laboratory techniques are being applied to rapid field devices.

Adaptation to the bioterrorism crisis has provided an opportunity for biosafety specialists to enhance their knowledge, to improve biosafety standards and procedures, and to build more effective working relationships.

Biosecurity in the 21st Century: Governing Bioscience

Gigi Kwik

Center for Civilian Biodefense Strategies

Johns Hopkins University

Baltimore, Maryland

The growing power of bioscience increases the destructive potential of a biological attack, making it imperative to prevent the misapplication of research gains towards weapons use. However, research efforts that lower barriers towards bioweapons development are pervasive, constantly evolving, and are usually of beneficent value to human health or biodefense. Rapid and strategic bioscience advancement (including that which inadvertently lowers barriers towards bioweapons development) may be the only viable defense strategy. How can we increase biodefense and constrain malignant applications of bioresearch? Over time, we must build a network of "checks and balances": regulations, incentives, cultural expectations, and practices that encourage and enable progress in scientific understanding so that scientific knowledge can address human needs while simultaneously assuring responsible stewardship of bioscience so it is not used for malevolent purposes.

With its strengths and wisdom, the scientific community must confront the problem of bioterrorism. The Johns Hopkins Center for Civilian Biodefense Strategies aims to describe measures that can be undertaken by scientists to lower societal risk from more potent bioweapons, without constricting research needed for biodefense and human health. Our recommendations are based on research into the governance of complex, evolving technologies (e.g., Internet) and interviews with working scientists whose research is clearly beneficent, but could clearly be misapplied towards bioweapons ends.

Impact of Biosecurity on Biomedical Research at Duke University

Debra L. Hunt

Duke University

Durham, North Carolina

The concept of "biosecurity" is a new one in the world of academic freedom in university research laboratories. To researchers who are accustomed to sharing organisms and results with other researchers, compliance with such issues as 24-hour monitoring of select agent labs, background checks and fingerprinting, locked freezers and doors, and notification of a government entity prior to destruction of select agents is, to some, an unnecessary burden. Researchers must now consider the type of information that can be published and strike a "balance between the openness of scientific communication, which is essential for the advancement of the biomedical research effort aimed at biodefense, and secrecy for protecting national security information" (Ron Atlas, American Society for Microbiology [ASM]).

As with any major change in procedural and/or facility requirements, the new rules have spawned both negative and positive impacts. At Duke University, those researchers who have worked with toxins or organisms for many years that are now considered "select" for biosecurity reasons, find some of the new requirements a bit onerous, such as keeping an inventory of the number of vials of viable organisms, changes in the process of ordering and receiving select materials, or installation of expensive security measures such as monitors or security alarm systems.

Very few, however, have elected to either destroy the agents or transfer to other registered labs.

The negative impact on our safety office has been primarily a matter of time and effort involved in identification of select agent labs and helping the researchers become compliant. Many of the requirements are practical safety measures, such as development of emergency/fire response plans, exposure follow-ups, and required agent-specific safety training.

New research grants in bioterrorism preparedness, however, have provided additional opportunities for more researchers to become involved in select agent work. In fact, Duke researchers are clamoring for the NIH biodefense grants, including participation in the Southeast Regional Center of Excellence in Biodefense and Emerging Infections (SERCEB), and a grant submission for a \$16 million Regional Biocontainment Laboratory for collaborative research with other institutions to develop therapeutics, vaccines, and diagnostics for select agents. The positive impact on research will include not only the development of new technologies for better diagnostics and treatments for bioterrorism agents, but also provide an opportunity to piggyback work with emerging infections for the benefit of public health in general.

The Duke Biological Safety Office has benefited as well, having justified a new laboratory safety position to assist with safety concerns in the new laboratories at the facility. Closer collaboration with Duke researchers in the Select Agent process has helped to enhance the safety office reputation, and is providing unique and exciting opportunities. For example, the Director of the SERCEB and, hopefully, the RBL, will require certification in the Safety of Biocontainment (provided by Biological Safety) for all researchers working in these facilities.

Biosecurity: An Academic/Research Community Paradigm Shift

Cecil Smith

Ohio State University

Columbus, Ohio

Ohio State University is a land grant institution established in 1870. The University consists of a

large urban campus and multiple regional campuses. There are approximately 57,000 students, 32,000 employees and an estimated 20,000 contractors/visitors to the campuses on a daily basis. The Columbus Campus also operates three hospitals that serve local, state, regional and national healthcare needs. Research activities generate approximately \$425 million annually. All of our campus environments are open to the public with very few restricted access spaces in the academic, administrative, research and healthcare buildings. Many buildings support academic and research activities in adjacent spaces. Daily operational management decisions are decentralized to Deans, Department Chairpersons and ultimately principal investigators. The institutional culture promotes academic/research freedom with minimal censorship or control of research information.

Implementation of the Public Health Security and Bioterrorism Preparedness Act of 2002 forced the university to identify key responsibilities for biosecurity. Two principal issues came into immediate focus: 1) defining the difference between biosafety and biosecurity; and 2) utilizing existing institutional administrative infrastructure to develop and implement an action plan. The Office of Research and the Office of Environmental Health and Safety became the principal stakeholders for assuring compliance and facilitating the overall process.

It quickly became apparent that the climate fostering academic/research freedom was in direct conflict with regulatory mandates relating to select agents. Senior management and the research community needed a paradigm shift. Biosecurity implications include:

1. Changes in the research risk management process relating to new research and existing research.
 2. Development of an institutional "BioSecurity Matrix" consistent with regulatory mandates and institutional risk management policies.
 3. Understanding the key elements of: risk/threat assessment, material accountability, physical security, data security, personnel security, agent transfer, emergency response/preparedness and risk communication.
 4. Educating management and the research community.
-

Management of Select Agent Responsible Official Duties at the CDC Atlanta Campus

Robbin S. Weyant

Centers for Disease Control and Prevention
Atlanta, Georgia

The Centers for Disease Control and Prevention (CDC) houses an extensive array of laboratories working with Select Agents (SAs), providing a variety of services including diagnostic and environmental testing, methods development and validation, epidemiologic support, and basic research on the biology and pathogenesis of SA diseases. CDC laboratories provide SA diagnostic reagents and control materials to collaborating institutions in the U.S. Laboratory Response Network, NIH Grantees, and other registered entities. Since 2001 CDC laboratories have been involved in over 200 SA transfers per year. Implementation of SA regulations, including the December 13, 2002 HHS and USDA Select Agent Interim Final Rules, at CDC is accomplished through a collaborative effort between the CDC Office of Health and Safety (OHS), National Center for Infectious Diseases (NCID), and Office of Security and Emergency Preparedness (OSEP). The Responsible Official and Alternate Responsible Official for the CDC Atlanta facilities reside in the OHS. OHS conducts a program for laboratory safety including training, workplace hazard analysis, incident response, and risk assessment. OHS information on laboratory safety can be accessed on the OHS web site (<http://www.cdc.gov/od/ohs>). The RO and aRO work with senior management from NCID and OSEP, along with principal investigators to develop policies for monitoring and securing SA inventory, and controlling access to SA materials. These policies and procedures have been incorporated into a CDC Select Agent User's Guide that is distributed to principal investigators. Screening of workers for compliance with the Department of Justice security assessments is accomplished collaboratively by NCID, OHS and OSEP, with security of personal information given high priority. Specific administrative approaches to the CDC SA management program will be presented and discussed.

Biosecurity Implementation at a Biologically Secure Facility

Douglas M. Moore

Plum Island Animal Disease Center
Greenport, New York

The Plum Island Animal Disease Center has operated a biocontainment facility on Plum Island, New York for nearly 50 years. The Center performs laboratory and animal-based studies on communicable livestock diseases which do not occur in the United States on an Island-based facility as required by Federal Law and USDA policy. The facility operates as an enhanced BSL-3 facility, known as BSL-3AG, designed to protect both staff and the environment from exposure to infectious agents. Facility design and operation criteria, strict biosafety procedures, and personnel security qualifications have been the core of a biosafety/biosecurity program throughout this period. In the last few years, increased attention has been focused on the security of USDA BSL-3 facilities handling both animal and plant pathogens. Following the terrorist attacks in September 2001, the USDA determined that a uniform policy was needed for all of its BSL-3 laboratories to ensure the security of pathogenic materials and the protection of the facilities themselves. In December 2001, the Department issued biosecurity requirements for its BSL-3 facilities and Departmental Manual 9610-001, "USDA Security Policies and Procedures for Biosafety Level-3 Facilities" (the P&P), defines these requirements. The P&P is a document that provides background, definitions, responsibilities, regulatory basis and specific elements which establish a facility's Biosecurity Plan. The specific elements are: 1) Inventory Control Procedures; 2) Physical Security Systems; 3) Cybersecurity Systems; 4) Personnel Suitability Determinations; and 5) Biosecurity Incident Response Plans. While much of the P&P was part of Plum Island's existing biosecurity program, the new P&P placed additional requirements into the program. This has resulted in both operational and cultural changes at the facility with significant impacts on physical security systems, pathogenic material controls, and personnel access to biocontainment areas of the facility. The experiences of USDA in assessing and imple-

menting its biosecurity needs may provide beneficial information to other organizations and institutions developing biosecurity programs.

Biosurety, U.S. Army Medical Research Institute of Infectious Diseases

Kathleen W. Carr

U.S. Army Medical Research Institute of
Infectious Diseases
Fort Detrick, Maryland

Biosurety is a program intended to provide assurance that high consequence pathogens and toxins are safeguarded from diversion, theft or unauthorized access. In the Department of Defense (DoD), this program was created in December 2001 and is still in its development stages. The four pillars of the DoD's program are agent accountability, personnel reliability, physical security and safety operations. The focus of this presentation is to highlight the implementation of the biosurety program at the United States Army Medical Research Institute of Infectious Diseases. While many facets of a biosurety program existed prior to its formal inception, the program must appropriately balance requirements with the ability to conduct biodefense research.

Keep it Sane; Keep it Simple: Compliance with Bioterrorism Legislation Need Not Stifle Biomedical Research

Deborah E. Wilson

National Institutes of Health
Bethesda, Maryland

(Not presented.)

The USA Patriot Act of 2001 and the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 have provisions which will dramatically affect the conduct of biomedical research in this country. Institutions are being asked to control research materials as never before. In addition of further regulating Select Agents as defined in Title 42 CFR 72.6, the PATRIOT Act will allow

prosecution of individuals knowingly possessing any biological agent, toxin, or delivery system of a type or in a quantity not justified by peaceful purposes such as prophylaxis, disease prevention or bona fide research. Biomedical research institutions are being required not only to control Select Agents more closely but to delve into the backgrounds of research personnel in order to comply with the "restricted persons" provisions of the PATRIOT Act. Information regarding personnel and the agents with which they work must be centrally reported and maintained in a national database for law enforcement use and forensic purposes. In a country where academic freedom has ruled supreme, these changes are uncomfortable at many levels.

Still the question remains, how can academia, states, local and federal governments and industry, alike conform to the requirements and still conduct the types of research needed to combat bioterrorism in this country? The interests appear competing. How will the Government insure that the needed organisms, toxins, or possibly genetic elements are made available for legitimate research purposes while exerting the mandated controls? What additional funding constraints, if any, will be implemented at the federal level?

The National Institutes of Health has developed a simple and sane approach for the control of these regulated agents in the biomedical research arena.

Some of the basic program elements include: employee notification of requirements and restrictions; establishing an "authorization process" for use of Select Agents; protection of the researcher; inventory controls; and staff "clearances" to work with restricted agents.

Five-Year Implementation of a Biosecurity Plan in a Private Research Facility

Melina Kinsey

Midwest Research Institute
Kansas City, Missouri

In 1997, Midwest Research Institute (MRI), a private, not-for-profit center for applied research and technology development, developed a biosecurity plan following the enactment of Title 42 CFR Part

72, Additional Requirements for Facilities Transferring or Receiving Select Agents. The biosecurity plan, called the Biotechnology Employee Reliability Program, began as a procedure for screening employees who work with select agents in Biosafety Level 2 and Level 3 laboratories at MRI's Kansas City headquarters. The plan set forth criteria to evaluate individuals based on a list of disqualifying factors and considerations. Since 1999, the plan has expanded to other aspects of the MRI biosafety program such as training, physical security, material accountability, and emergency response. The plan has also been implemented at MRI's laboratory facilities in Palm Bay, Florida, and Rockville, Maryland, and will require only minor revisions to comply with the new select agent regulations enacted in 2003. A model for a working biosecurity plan will be presented. The presentation will include the impact of the plan on biosafety, security, human resources, and the institutional biosafety committee. We will also present the pros and cons of the plan, the impact on government and independent client research contracts, and responses to the MRI plan from agencies such as the CDC and USDA.

Biosafety and Biosecurity: Lessons Learned at the Canadian Science Centre for Human and Animal Health

Kevin Smith

Canadian Science Centre for Human and Animal Health
Winnipeg, Manitoba, Canada

Presented from the perspective of the Canadian Science Centre for Human and Animal Health (CSCHAH) and its related security aspects. Issues to be covered: initial development and cost; security philosophy; security design and objectives; the integrated approach to security; discussions on the three most important aspects of security (physical, personnel; and risk assessments); other issues; and what the future holds. The discussion will focus on these topics as they relate to the biosecurity issues within CSCHAH. There will be a 20-minute Power Point presentation with a brief Q&A period to follow.

Integrating Security and Biosafety: Developing a Biosecurity Program at the Canadian Food Inspection Agency

Sandra Fry

Canadian Food Inspection Agency
Nepean, Ontario, Canada

The Canadian Food Inspection Agency (CFIA) has 21 laboratories across Canada that is responsible for food safety, animal health, and plant protection. These laboratories range in design and function from high hazard chemistry laboratories, greenhouses and standard micro labs to a network of Level 3 biocontainment laboratories and animal handling areas. The challenge of implementing a biosecurity program in these settings involves the diversity and location of sites, multiple occupants and custodianship, standard setting vs. standard utilization and the integration of existing security and scientific programs. These issues will be outlined with a discussion of the solutions that are being brought forward and implemented.

This presentation will outline the Agency's proactive strategy to integrate existing physical security systems with our enhanced awareness of microbial, toxin and chemical security. Key aspects of the approach include central coordination, the conducting of "enhanced" Threat Risk Assessments, and pathogen inventory planning across multiple sites. The USDA policy and procedures for biosecurity will be outlined, as will the ABSA Biosecurity White Paper, which is being used as the basis for this program. An overview of roles and responsibilities for the new area of Biosecurity within a large government organization will also be discussed.

New Challenges in a New Environment

Janet Nicholson

Centers for Disease Control and Prevention
Atlanta, Georgia

The Centers for Disease Control and Prevention's (CDC) National Center for Infectious Diseases' (NCID) mission is to prevent infectious diseases through: 1) surveillance and response; 2) applied research; 3) infrastructure and training; and

4) prevention and control measures. For the laboratory this means rapid detection of outbreaks, improved diagnostic testing methods for new, re-emerging, and drug-resistant pathogens, better understanding the risk factors for infection and disease, understanding the relationships between infectious agents and some chronic diseases, providing diagnostic and reference reagents for public health laboratories, and training the next generation of laboratorians.

Bioterrorism detection and response capabilities rely on: 1) rapid and accurate diagnostics for human, animal, and environmental specimens; 2) collecting and characterizing strains of organisms that may be used for bioterrorism; 3) developing assays to identify unique characteristics of agents (antimicrobial resistance) e.g., 4) understanding the routes of infection and pathogenesis of the pathogens; and 5) knowing the efficiency and efficacy of decontamination methods. CDC's laboratories are actively engaged in work to address these needs.

The security of the CDC main campus in Atlanta has continually been assessed for at least the last eight years, and measures have been put in place to ensure a level of security commensurate to the threat. Laboratories have always been considered areas that need limited access, and a cardkey system has been in place for over 20 years. Enhancements in security over the years have included: 1) an increased guard force, including armed guards; 2) a ring concept that is controlled by multiple cardkey access to the most sensitive areas; 3) criminal background checks for all CDC personnel and contractors; 4) installation of cameras in strategic locations; 5) fences and gates to control access to the campuses; and 6) criteria for inventory information and restricting access to inventories. A year ago HHS required CDC to enact additional security requirements, including the addition of cameras to monitor freezers, refrigerators, etc., where select agents are stored and requiring security clearances for persons working with Variola. The requirements of the Select Agent Rule have not added significantly to the security enhancements already in place.

The impact of increased security on the laboratory activities has made access to many laboratory areas difficult for unauthorized persons, ensured that personnel allowed in these areas have approvals

to be there, and made everyone more aware of security issues. Challenges remain in further refining inventory, access, and personnel issues.

Threat and Security Planning for Biological Laboratories

Edwin S. Taylor
Camber Corporation
Frederick, Maryland

Security planning can be accomplished by compliance with a specified standard promulgated by a responsible agency, by the development of a independent Design Basis Threat (DBT) to plan against, or by the combination of the two methods. Effective security planning requires attention to the threat to be protected against and the vulnerabilities of the operation to those threats. The threat is defined as what the security measures are directed against, while the vulnerabilities are the areas of the operation which can be exploited by the threat actor. Threat development is a complicated and difficult process, prone to great error, both in commission and omission. If it is seen basically as a guess, then the reasons for likely error become obvious. Focus on the threat actor, as is commonly done, results in the greatest margin for error, while focusing more on methods employed results in the least. Threat assessment concerning biological laboratories is far from a mature process and therefore prone to such errors. Security planning based solely on compliance with federal standards then, has a large potential for catastrophic failure. This presentation will discuss the preparation of threat and vulnerability analyses as applied to biological research laboratories, and the integration of those analyses into effective security operations, tailored to the specific needs and requirements.

Bio-Security Access Control Basics

Richard Kibby
Science Applications International Corporation
McLean, Virginia

This presentation, "Bio-Security Access Control Basics" will provide an introduction to Access Con-

trol (AC) techniques, tactics, and procedures. Various levels of AC and the objectives of implementing AC at these levels will be discussed. An AC program has several elements that need to be considered. Those elements are; perimeter barriers, protective lighting, camera systems, intrusion detection devices, and entry control equipment. The equipment coupled with security procedures constitutes an Access Control Program. Each of these elements will be reviewed to demonstrate how they contribute, either as a single element or in unison, to secure a resource and control access. The objective of this presentation is to provide information regarding how a viable system that controls entry to an area, or protects a resource, must be employed to successfully limit unauthorized persons from gaining access to an area or materials.

This presentation will cover physical security protection for two vulnerabilities. The first is protecting sensitive materials from unauthorized persons. The second vulnerability is a new concern that has developed since 9/11 and the events of actual incidents. That concern is insider threats. Security systems, personal reliability programs, and access control are the means necessary to protect sensitive materials in today's threats. Physical security measures alone will not guarantee the protection of sensitive materials. Technology is used to keep unauthorized persons from having access. An additional subject that requires consideration is the insider threat and establishing a personal reliability program to better ensure those with access remain reliable. Without some program to monitor the reliability of those with access, there is still some degree of risk that must be considered by decision makers. Access control and security technology only provide a part of the answer. This lecture will center around AC and security equipment.

The first steps to protection are assessing the threat, vulnerabilities, and the risk to materials at your facility. The results of these combined assessments will determine the level of AC that you should employ. Typically, single element programs provide a minimum of security for low risk areas. For this level, discussion will cover access control levels that might have lights or cameras, access re-

quirement signs, or a sign-in sheet or badges to assure the authorized people have access into the area. The presentation will continue with materials that are more critical. The AC systems become more complex and employ multiple elements to ensure the security and access by authorized persons. These systems will employ more positive identification techniques such as proximity cards with key pads for positive identification using PIN numbers. These systems work in conjunction with other electronic security systems that operate during non-duty hours to record who entered the facility and at what times. These include cameras and other devices that record the time doors and containers were opened etc. For critical or dangerous materials, the discussion will cover some combination of elements that maximize access control and combine technology to have positive identification, entry and exit time recording, CCTV video recording and possibly container lock-out systems during non-working hours. Theoretically, the most stringent access control system would employ an outer perimeter system such as the entryway to a lab with lights, cameras, and a security system that would allow only certain people in the facility after work hours. The next element of AC would be sensors and other devices that would turn on recording systems for security cameras and/or warn security persons that someone has entered the facility. And finally, the immediate area that contains the material, such as a room or locker, would have electronic devices that would provide positive identification and intrusion detection of a person attempting access.

It is the intent of this lecture to provide the listener with a basic understanding of what an access control system is, what the major elements in access control are, and finally give some examples of combining access control elements to increase the security of sensitive materials. The listener should also understand that these elements are not applied randomly. A systematic process of understanding the threat, vulnerabilities, and risks to the material are important factors that determine what level of access control should be employed.

Better Safe than Sorry: The Importance of Conducting Background Checks in Today's World

Ken Obriot
Wyeth Pharmaceuticals
Richmond, Virginia

The importance of conducting proper background checks can not be underestimated nor ignored. In today's environment of litigation and with the lurking threat of terrorism it is now more important than ever that businesses conduct proper background screening of their prospective employees.

It is far too easy to do a less than adequate background check and find out later that you hired someone who is either not up to performing the job or is actually jeopardizing your business and the safety of your employees. Could these problems have been avoided by conducting a thorough background investigation?

We are finding more and more that background screening is being mandated by federal, state, and local governments. Businesses that are affected include: home health care providers, nursing homes, childcare providers, security guards, to name a few. Soon those agencies dealing with select agents and toxins will need to meet federal requirements and conduct screening on all employees having access to these agents.

The key to a good background investigation is verification. Check the sources look for discrepancies and when in doubt check further. Don't rush the process spend the time now or pay for your mistakes later.

In this program we will guide you through the process of how to conduct a proper background check and look at some of the resources that are available to you to verify information.

We will also look at a few examples of bad hires, how they can hurt you and pitfalls to avoid. We will also discuss setting up a system of verification that requires additional checks based upon levels of sensitivity for employee groups.

Agent Accountability and Inventory Control Procedures

Michelle D. McKinney
Science Applications International Corporation
McLean, Virginia

Numerous regulations and guidelines exist to establish a baseline of security that will be followed by all registered facilities that possess, use and transfer select agents and toxins. How to achieve the appropriate level of security at different facilities with different types of laboratories that work with different select agents and toxins will be unique for each facility. Agent accountability is one of the biosecurity policies and procedures that must be addressed in addition to evaluations of program specific items such as existing threats, vulnerabilities and risk that must be performed. The different challenges for securing and accounting for samples in repositories, working stocks and experimental use will be discussed, as well as investigating and reporting discrepancies. The pros and cons of administrative versus technology driven methods for accountability will be examined. Finally, once you have the appropriate record keeping system in place you must have reliable and trustworthy employees who will not only follow the system, but help enforce its implementation. Even the best of customized record keeping and accountability programs will fail if your employees do not comply with it.

Abstracts not provided:

"The New Select Agent Regulation" by Stephen Morse, Centers for Disease Control and Prevention, Atlanta, Georgia

"Biosecurity, Biosafety, Biosurety—Perceptions, Reality and the Future" by John Parker, Antibody Systems, Inc., Hurst, Texas

"The Role of Department of Justice (DOJ) in Facility Biosecurity" by David M. Hardy, Federal Bureau of Investigation, Washington, DC
