Health Security
Volume 13, Number 3, 2015 © Mary Ann Liebert, Inc.
DOI: 10.1089/hs.2014.0090

Information Security for Compliance with Select Agent Regulations

Nick Lewis, Mark J. Campbell, and Carole R. Baskin

The past decade has seen a significant rise in research on high-consequence human and animal pathogens, many now known as "select agents." While physical security around these agents is tightly regulated, information security standards are still lagging. The understanding of the threats unique to the academic and research environment is still evolving, in part due to poor communication between the various stakeholders. Perhaps as a result, information security guidelines published by select agent regulators lack the critical details and directives needed to achieve even the lowest security level of the Federal Information Security Management Act (FISMA). While only government agencies are currently required to abide by the provisions of FISMA (unless specified as preconditions for obtaining government grants or contracts—still a relatively rare or narrowly scoped occurrence), the same strategies were recently recommended by executive order for others. We propose that information security guidelines for select agent research be updated to promulgate and detail FISMA standards and processes and that the latter be ultimately incorporated into select agent regulations. We also suggest that information security in academic and research institutions would greatly benefit from active efforts to improve communication among the biosecurity, security, and information technology communities, and from a secure venue for exchange of timely information on emerging threats and solutions in the research environment.

There has never been more research done on biological agents and toxins considered severe threats to public, animal, and plant health—so-called select agents[1]—as in the past decade. This is perhaps not surprising, despite tight regulations on possession and transfer of these agents; the US government has spent approximately $60 billion on biodefense in that time frame, with the budget of the National Institute of Allergy and Infectious Diseases (NIAID) having gone from $200 million in 2001 to an annual average of $1.6 billion since 2004.[2]

The list of select agent–registered entities is not made public, but as of January 2015, there were 347 entities participating in either the Centers for Disease Control and Prevention (CDC) of the Department of Health and Human Services' (HHS) Division of Select Agents and Toxins (DSAT) or the Animal and Plant Health Inspection Service (APHIS) of the US Department of Agriculture (USDA) select agent program.[3] In 2004, there were a total of 150 registered entities, and this number has continued to increase annually through 2008 for a total of 242 entities.[4] The current number of registered entities is down from a high of 388 reported in 2009[5] and approximately 374 reported from 2009 through 2011.[6] However, given the current potential for intentional misuse of biological agents,

Nick Lewis, MSc, is Program Manager, Trust & Identity, Internet2, Ann Arbor, Michigan. Mark J. Campbell, PhD, is Biological Safety Officer, Select Agent Responsible Official, Office of Environmental Health & Safety, Saint Louis University, Saint Louis, Missouri. Carole R. Baskin, DVM, is Associate Professor, Institute for Biosecurity, Environmental & Occupational Health, College for Public Health and Social Justice, Saint Louis University, Saint Louis, MO.

returning to pre-2004 numbers of fewer than 150 select agent–registered entities is highly unlikely.

The numbers discussed thus far include only regulated entities in the US engaged in working on select agents. There are also laboratories working with potentially dangerous infectious agents that are not currently on the select agent list and laboratories funded by entities other than the US government. In addition, foreign facilities performing work with the same agents operate under varying degrees of oversight. In fact, the absence of a database accounting for all entities with high-containment laboratories in the US and the resulting lack of central oversight has been lamented on several occasions in various government-issued documents.[4,7-9] With no single agency setting targets or monitoring the expansion of high-containment laboratories, the task of accurately quantifying the combined risks of accidental or intentional release of pathogens and the risk of release of data that could be potentially misused is especially challenging.

The idea of classifying infectious agents according to the risks they present, and the creation of guidelines and regulations to work with these agents, dates back to the 1970s. Prompted by the work undertaken at Fort Detrick, MD, CDC and the National Institutes of Health (NIH) took turns publishing guidelines in rapid succession: *Classification of Etiologic Agents on the Basis of Hazard,*[10] the National Cancer Institute's *Safety Standards for Research Involving Oncogenic Viruses,*[11] and the *NIH Guidelines for Research Involving Recombinant DNA Molecules* in 1976 and since then updated many times, most recently in 2013.[12] Interestingly, unlike the laws and regulations on the possession, use, and transfer of select agents,[1,13-18] these early guidelines were the result of a bottom-up effort by scientists to self-regulate and therefore were born out of a strong consensus among professionals to abide by them. A similar collaborative effort among the CDC, NIH, and the scientific community yielded the first version of the widely and internationally accepted *Biosafety in Microbiological and Biomedical Laboratories (BMBL),* originally published in 1984 and currently in its 5th edition.[19]

Subsequent to a series of troublesome incidents in the 1990s, the Antiterrorism and Effective Death Penalty Act of 1996 was passed into law and implemented in 1997.[13] This act led to the creation of the original Select Agent Rule (42 CFR part 72.6) by HHS.[1] As it became apparent that dangerous biological agents could be acquired and used for illegitimate or nefarious purposes in this country, the law became the first to require that transfers of such agents be preapproved by the CDC, along with a preapproval process of the facilities performing these transfers.[20] Select agents were officially born, and noncompliance with this law resulted in civil and criminal penalties.

Following the events of September 2001, Congress passed 3 laws that went beyond regulating the transfer of select agents to restrict who could possess and use these agents, using a process of registration and background checks. They are the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001),[21] the Public Health Security and Bioterrorism Preparedness and Response Act of 2002,[14] and the Agricultural Bioterrorism Protection Act of 2002 and Related Provisions.[15] CDC and APHIS implemented these laws through a series of regulations known as the Select Agent Regulations (SARs).[16-18]

Despite these laws and regulations—or perhaps because of them—the biosecurity community, still highly motivated to self-regulate and optimize communication with the security community, decided to take a closer look at the risk of doing research whose results could be used for both beneficial and harmful purposes, a concept known as dual-use research (DUR). These interactions yielded the Fink Report[22] and ultimately led to the chartering of the National Science Advisory Board for Biosecurity (NSABB), a federal advisory committee housed in the Office of Biotechnology Activities (OBA) in the Office of Science Policy at the NIH. The NSABB, along with the National Academies of Science and a Trans-Federal Taskforce chaired by HHS and USDA, has been involved in making recommendations to improve several aspects of the federal select agent program.[5,9,23] Finally, a series of experiments involving the modification of highly pathogenic avian influenza viruses to be transmissible among certain mammals,[24,25] including possibly humans, resulted in the US issuing policies on dual-use research of concern (DURC) in 2012 and 2014,[26,27] with one proposed in 2013 still as of this writing awaiting final rule.[28] These policies in their current form pertain only to research conducted with a limited list of agents, all of which are also select agents, but they add to the existing restrictions on this type of research by a government entity.

The US is not alone in regulating research with biological agents deemed dangerous or posing a potential threat to national security, and many individual countries have their own set of regulatory requirements. However, list-based regulations are not widespread, and among countries having such regulations, the numbers and identity of the agents on these lists vary considerably (from 22 to 105), as does the nature of the restrictions associated with them.[29] Despite a number of international efforts aimed at creating a more unified approach, this variability may create vulnerabilities in that individuals in the US could find access to material or information restricted by the US federal select agent program from international sources.

Is Research with Select Agents Secure?

We believe that much remains to be done to ensure security of the information and data generated by research with select agents, some of which may be restricted either by select agent regulations or by DURC policies. We also

believe that the risk is currently understated, in part because of the "language barriers" that remain between the biosecurity, information technology (IT), and security communities. This lack of understanding of what achieving information security entails in the biosecurity community is exemplified by the scantiness of the guidance provided, until recently, in regulatory and guidance documents. The laws affecting select agent research and the early versions of the resulting select agent regulations mentioned cybersecurity, commonly understood as measures to protect networks, computers, and data from attack, but they provided no details, and the later versions delivered little more than a couple of paragraphs on information security, which is the protection from unauthorized access, modification, destruction, or other violations.[1,13-18,21] In fact, specific guidelines were not provided until a security plan template was published by the CDC and APHIS in 2007, where the topic was broached in one paragraph.[30] Even such significant documents as the 2008 report to the Congress by the US Government Accountability Office (GAO) on the security of the nation's 5 BSL-4 laboratories[31] and the 2009 *Responsible Research with Biological Select Agents and Toxins*[5] specifically excluded cybersecurity. However, in 2009, the *Report of the Working Group on Strengthening the Biosecurity of the United States* stressed the importance of defining "access" for work with select agents and noted that information systems controls (ISCs) should be a key part of the security plan at select agent–registered institutions.[29] Information systems controls are further defined as including:

- IT infrastructure—firewall protection, antivirus protection, and password protection;
- hardware asset protection—computer room protection, office protection, property pass controls, and secured space for sensitive information;
- personnel security—background checks for IT staff, vendors, and information security managers; and
- data protection—data encryption, remote access protocols, web data sanitation, and security of select agent inventories.

The *Report of the Defense Science Board Task Force on Department of Defense Biological Safety and Security Program* (2009) noted that cyber-threats were not addressed adequately and that, among other issues, the so-called isolation of computer systems was not complete.[32] Then, in 2010, Executive Order 13546 mandated the establishment of appropriate practices for physical security and cybersecurity for facilities that possessed Tier 1 agents—that is, agents that are perceived as representing the highest risks of misuse.[33] Later the same year, the Federal Experts Security Advisory Panel, which was created as a result of Executive Order 13546, recommended that select agent regulations be amended to include (1) standards for cybersecurity designed to improve the isolation of computer systems storing select agent–related information, (2) further restriction of access to these data by individuals with select agent clearance to the absolute minimum required to perform their duties, and (3) effective prevention of various cyber-threats.[34]

Finally, since 2012, several "guidance" documents have been released that discuss, in relative detail, infrastructure requirements and implementation of information security in select agent–registered facilities: *Security Guidance for Select Agent or Toxin Facilities* in July 2013 by CDC, DSAT, and APHIS select agent program[35] and the *Information Systems Security Control Guidance* published by the same group in 2012 and updated in 2014[36] (henceforth collectively referred to as the Guidance). Despite these developments, it is important to note that the IT security requirements for select agent work are still much less rigorous than the physical security requirements. Furthermore, IT security requirements need to be applied to all data or systems used in select agent work to ensure that a physical security incident will not lead to an information security incident and vice versa.

Currently, select agent regulatory entities believe they have developed appropriate IT security guidelines independently of the work in other government agencies or at the National Institute of Standards and Technology (NIST). However, most research organizations have found that putting in place sufficient information security controls for maintenance of an effective biosecurity infrastructure is very challenging, leading to many vulnerabilities. These challenges are not unique to select agents, of course, but the consequences are especially significant with select agent research. For instance, the sprawl of high-containment laboratories, while past its peak, has led to a parallel increase in the number of individuals with select agent clearance. As of January 2015, there were approximately 11,000 such individuals;[3] this number is up from 8,335 in 2004.[4] The more people with access to select agents or to sensitive information connected to select agent research, the higher will be the risk of malicious external influences, manipulation, or threats targeting these individuals and resulting in access to this information.

During a 2013 meeting on personnel security programs organized by the American Association for the Advancement of Science (AAAS) and others,[37] these risks were discussed at length and included stealthy strategies such as "inquiring about research at conferences or trade fairs; sending or recruiting students at US universities; romantic or sexual advances; exploiting foreign assistance or cooperation; and targeting certain ethnicities or nationalities."[37(p6)] Employees may never realize that they are providing meaningful information, so it is questionable whether continuous monitoring of personnel would detect such breaches of information security. Notably, a security risk assessment (SRA) approval clearance is required for any individual with physical access to select agents, but individuals who are not SRA approved may still have access to certain types of data or information, such as security plans,

relevant to select agent work in their facilities, and this may create vulnerabilities. This is all the more a concern in the age of heavily funded "big data" science,[38] which increases the probability of these data and related select agent–restricted information being inadvertently or intentionally circulated, or the potential for restricted agents to be created de novo without the mandated oversight.[39] While not all data obtained through select agent research falls within the scope of select agent regulations, which are primarily concerned with information enabling access to the select agents themselves, the 2 are often comingled to the extent that prior to publication, information system security should be concerned with both, particularly in the context of the new DURC policies. In fact, the NSABB considered advocating that access to new genetic sequence information about select agents be specifically restricted, although it ultimately did not make the recommendation because it was deemed "not feasible, likely to be ineffective, and/or would unduly hinder scientific research."[40]

Key-cards or access codes create other vulnerabilities. The 2007 security plan template by CDC and APHIS[30] was most concerned with the establishment of procedures when such items are lost or forgotten, when employees leave, or to prevent inadvertent or neglectful sharing of credentials or physical access. This focus was a reflection of the directives given in the select agent regulations.[16-18] The 2013 *Security Guidance for Select Agent or Toxin Facilities* (CDC/APHIS) reemphasizes these points but goes further by suggesting that key-cards be integrated with an intrusion detection system (IDS).[35] The document does not specify whether the intrusion detection system in question would be solely for building security or would include an IDS for IT systems as well (also known as intrusion prevention systems or IPS, which often also include an intrusion detection system). In an earlier version of this document, it imprecisely mentions, "An IDS for an IT system is sometimes referred to as an intrusion prevention system (IPS) where they use anti-virus software to inhibit the action of malware"[35] and where an intrusion prevention system has additional functionality over an intrusion detection system to block attacks. The 2013 Guidance distinguishes between the 2 types of IDS,[35] but it does not comment further on the need for synergy between the 2 systems relative to monitoring activity suggestive of tampering with coding of key-cards or password administration.

This would seem rather critical to address, as a 2014 survey of high-containment laboratories revealed that the vast majority of those doing select agent research (85%) used passcodes for access as opposed to physical keys,[41] and past inspections of select agent entities by the Office of Inspector General (OIG) noted multiple weaknesses in physical access controls and information technology controls.[43,44] Furthermore, the use of passwords in information security has been fraught with challenges, and people often outright reject the advice given to use a secure passcode or password.[45] The Guidance requires a 1-factor authentication (ie, username and strong password) for cybersecurity, but physical security requires multiple barriers and factors to protect physical access, which altogether are more rigorous than using a password. The Federal Information Security Management Act, which mandates information security in the federal government, requires 2-factor authentication to be used for identification and authentication for organizational users when applied at a so-called moderate level, thereby aligning physical and cybersecurity requirements with multiple independent barriers for access.

While implementing the 2013 Guidance, some institutions started identifying some of the areas where needed security controls were previously omitted, in part due to lack of involvement of information security teams and to unintentional oversights by responsible parties. Increasing attention was devoted to trying to ensure that the framework had controls to detect, manage, respond to, and remediate threats—all critical to ensuring an entity was effectively managing its risk. These challenges are, of course, not unique to select agent research.

Funding for select agent research has increased dramatically since 2001,[2,26] causing a surge in the number of needed inspections from 2004 to 2008 due to the addition of 92 facilities and 947 high-containment laboratories. During that time, the DSAT budget has actually decreased by approximately $2 million, and only 3 inspectors have been added.[4] The impact of the DSAT's shrinking budget and personnel resources on the quality of oversight has not been formally studied, nor has the adequacy of the budget of the APHIS select agent program, but several reports by the OIG (HHS and USDA) during the same time period suggested that significant issues existed regarding compliance with select agent regulations and the inspections themselves.[45,46] At the institutional level, the 2009 *Responsible Research with Biological Select Agents and Toxins*[5] recognized the significant financial burden of security compliance for individual select agent entities and recommended that federal agencies funding select agent research establish dedicated funding for select agent compliance beyond standard indirect costs.[5] While an in-depth discussion of the financial burden associated with the select agent program at the agency and entity levels is beyond the scope of this article, lack of adequate funding may lead to, among other possible weaknesses, insufficient implementation and oversight of key information technology controls for the safeguarding of select agent physical security as well as of data restricted under DURC policies.

At a broader level, another key vulnerability relevant to information security is the limitations inherent in list-based regulations. While it is known that select agents pose serious threats to public health if misused, it is not known, nor can we fully predict, what may be the potential uses and risks of all biological and nonbiological agents and scientific technologies in existence or yet to be discovered, many by pure chance. It is also impossible to know all information

security threats an entity might face and all the methods to attack the information systems at a facility. In fact, most incidents of dual use have not so far involved the current list of select agents or the list of agents in the "United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern,"[20,26] so it is possible that we may ultimately need to expand the scope of our "concern" and our understanding of what measures are necessary to ensure information security in the context of biological and technological research.

Information Security and Biosecurity

Federal Information Security Management Act

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.[47] Information security is integral to biosecurity, since a failure in any of the above could compromise the biosecurity of an agent and put society in danger. Therefore, information security needs to be integrated into all research processes, and good judgment must be used to identify what needs to be secured and what constitutes sufficient security for a specific line of research; securing "everything" in an entity to the highest level would be an inefficient use of financial and organization resources and be apt to ultimately increase vulnerabilities.

In 2002, FISMA was passed, mandating use of a risk-based approach to information security across the federal government.[48] In 2008, the federal government also started including FISMA requirements in some contracts and grants by HHS, NIH, the Department of Defense (DoD), and others to promote FISMA compliance outside the federal government, but this requirement has applied thus far only to information "collected, stored, processed, transmitted or used on behalf of HHS or any of its component organizations,"[49] and not to data that grantees retain intellectual property rights over, including select agent–restricted information or DURC policy–restricted data.[49] The sponsoring agency may specify the level of FISMA security required or may ask grantees or contractors to perform a security categorization to determine the appropriate level.

FISMA provides the parameters for securely configuring a system. For example, while the Guidance mentions firewalls and segmenting an entity's network to restrict access between areas that contain information on biological select agents and toxins and those that do not, it does not specify how to configure or manage the firewall securely.[36] Should all access be blocked, with only a few exceptions after review? FISMA has details on what data should be logged and reviewed for managing a firewall in its "Audit and Accountability" security control section, and it contains details on secure configuration of a firewall in its "System and Communication Protection" section, where it specifies limiting external connections, which connections should be denied by default and only allowed as approved, and many other specific details on the information security controls necessary to protect a system. Additionally, NIST publishes guidance documents to aid in the implementation of FISMA standards, and the security control catalog included in NIST800-53 has an extensive list of security controls that provide supplementary direction on what security controls should be implemented.[50]

However, grades on FISMA compliance scores based on OIG reviews suggest that federal agencies themselves are still struggling to implement this legislation.[51] This could be because of insufficient funding, or difficulties with making major changes to large organizations, or for many other reasons. Part of the challenge is that the federal government is bound by many different information security laws and regulations and still does not uniformly use FISMA, although it is increasingly moving in this direction.[52] The select agent program is not the only program, nor are CDC and USDA the only agencies, with unique information security requirements: For instance, DoD used the Information Assurance Certification and Accreditation Process[53] before switching to FISMA in 2014, and it also updated safeguards for unclassified controlled technical information to include security controls from NIST800-53;[54] health data are regulated by the Health Insurance Portability and Accountability Act (HIPAA) regulations;[55] student data are regulated by the Family Educational Rights and Privacy Act (FERPA) regulations;[56] and there are many other sector-based laws. This is also the case at the state level, and overlapping state and federal laws regulate private industry. In some cases, a single entity has to comply with several different, but deceptively similar, information security requirements and mistakenly meets the less rigorous requirements of FERPA, for instance, when the data and law require implementing the more rigorous HIPAA requirements, resulting in insufficient security controls for the risk and risk tolerance actually needed.

FISMA and NIST800-53 can be used as a crosswalk between the security controls and implementation details required for these different laws and regulations for the purpose of organizing the information security program and compliance to ensure all of the requirements are met. When a facility has an information security incident, an analysis can be performed to identify the root cause and determine what security control could have been used to prevent or minimize the impact of the incident. This new security control can then be implemented across the facility and potentially address requirements from other laws or regulations. For example, if a computer used for storing and managing a facility's inventory was improperly disposed of and then sold to an unauthorized party, the responsible official (RO) and information security team could perform

an information security incident response to manage the incident, identify that full disk encryption could have protected the data stored on the incorrectly disposed computer, and then implemented security measures on other computers at risk to prevent future similar incidents. Encryption on computers is mentioned in the Guidance, but not with specific details of how or where encryption should be used or managed as covered in FISMA.

The Guidance Versus FISMA

The Guidance[36] for work with select agents helped bring together the biosecurity and IT communities. The results of these interactions revealed that researchers overestimated the robustness of systems already in place. Discussions between information security staff at different institutions implementing prior requirements in 2013,[35] including an earlier iteration of the Guidance, revealed that they were all facing similar challenges.

As the IT security community "discovered" a new industry, using computing for their work that required high security, they had to critically evaluate systems at their respective institutions, as well as compare the Guidance to that in other areas of research with rigorous information security requirements, such as the Nuclear Regulatory Commission, which has its own information security standard[57] and challenges that are not unlike those of the select agent program, which could also perhaps be mitigated with FISMA standards.

The need to implement certain changes became apparent: For example, software and hardware manufacturers needed to redesign their products with the new requirements in mind, and institutions were required to adjust budgets to provide the resources necessary to devise customized solutions for meeting these standards.

Despite this new understanding, a major limitation of the Guidance is that it does not meet the FISMA baseline. Specifically, the Guidance requires broad controls to be in place only to protect select agent information systems, including inventory access logs; passwords; entry access logbooks; rosters of individuals approved for access to select agents; access control systems; security system infrastructure, including floor plans, on-site guards, closed-circuit televisions, and intrusion detection systems; security plans; and incident response plans. In contrast, FISMA and derived guidance document NIST800-53 require much more comprehensive security controls (Table 1). NIST800-53 elaborates on each security control with subcontrols and potential control enhancements, depending on the security requirements. The security categorization process culminating in determination of these requirements is detailed in FIPS199,[58] where guidance is provided for determining the worst case scenario from a loss in confidentiality, integrity, or availability of data. For example, the security categorization for an information system used in research on highly pathogenic avian influenza viruses, which are select agents and fall under DURC policies, could be "high impact" if data became unavailable, considering the dependence of the World Health Organization on information gained through these experiments to make seed stockpiles of vaccines against viruses with pandemic potential.

After a security categorization is made, the research institution would then determine minimum security requirements using FIPS200.[59] FISMA also uses the Risk Management Framework as described in NIST800-37[60] to assess operational risk across an entire system or organization as a foundation for the information security program. This is also a risk-based approach using security categorization and defining the minimum-security baseline for security control selection. The control selection takes into account effectiveness, efficiency, and constraints of the security controls. An organization would be able to implement the security controls based on their risk tolerance, scope, complexity, and resources to achieve a system that meets the requirements of the researchers and the defined security controls.

Table 1. Security Control Identifiers and Family Names

ID	*Family*	*ID*	*Family*
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Note. Each family contains security controls related to the general security topic of the family. A 2-character identifier uniquely identifies security control families—for example, PS = Personnel Security.

This is another risk management area where the granularity of FISMA-derived guidelines eclipses the requirements thus far provided to the select agent research community. When starting to implement FISMA "low level" (FISMA has 3 levels of security: high, moderate, and low), an entity could document the scope of the select agent research and perform a gap assessment on the FISMA low-security control usage as well as identify any improvements necessary or newly needed security controls. This approach would allow an entity to get started while other details around specific risks, threats, security controls, or legal updates are discussed and decided upon. There would be many challenges with implementing low-level FISMA around changing human behavior to adopt the new security controls and trying to identify whether a particular device or data should be included in the scope of the work. There would be specific challenges in laboratory activities, because many information security controls assume easy and flexible access to a computer or device in the scope. In a laboratory in which researchers are in personal protective equipment, including gloves, for instance, it is challenging to bring additional computer equipment in on a regular basis, to implement new security controls such as fingerprints for authentication, or to connect a physical token to the computer without putting researchers at heightened risk of a biosafety incident. Thus, any new security control, regardless of the security framework used, would need to be carefully evaluated to identify any unintended consequences and safety risks in the laboratory environment.

Another shortcoming of the Guidance has to do with determining the scope of information security requirements, also known as "scoping." Scoping the security requirements too narrowly could result in an information system relevant to select agent research on campus being excluded from consideration, and scoping too broadly would result in inefficient use of resources and undue burdening of research efforts. Should any system with select agent data be included or only systems controlling physical access to the agents? Should any industrial control systems or laboratory devices with network connections or with computers connected that are used for select agent research be included in the scope? The Guidance mentions the example of a researcher using a laptop in the laboratory and in his or her office to emphasize the necessity of securing the laptop and the data stored on its hard drive in both places (ie, not just in the select agent–registered space), but it does not require that the same security controls be in place in both spaces.

Shared systems and laboratory equipment capable of storing or transmitting data are also in question when it comes to scoping. There can be a lack of awareness that everything connected to a computer network is vulnerable, even if does not look like a computer, and devices are usually not configured securely by default, as software and hardware vendors typically do not ship in a secure configuration but in a configuration that would work for most customers.

Even industrial control systems that do not traditionally get connected to a computer network may need to be in scope if their control systems are used in select agent research. If an industrial control system is used in the select agent–registered space, then the system should be included in the FISMA scope, and the NIST Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82)[61] should specifically be used for securing these systems to support FISMA security. For example, if a centrifuge is used in a select agent–registered space and the centrifuge has a computerized control or a connection to a network, the centrifuge should be included in the scope and secured appropriately so that it cannot be illicitly manipulated to cause a biosafety incident.

Finally, if an individual uses an account to log in to a computer in the select agent–registered space, do the account and account management system need to be within the scope? FISMA provides clearer guidance relative to scoping that could be used to strengthen select agent information security and reduce any gaps not addressed in the current Guidance. Given the many layers of security necessary in a system, the scope should be broad enough to encompass systems an attacker could use to penetrate the security of the system to access the regulated data and systems.

The Guidance indicates the same expectation for information security as physical security controls, but the IT security controls are not as rigorous as the physical security controls. For instance, does an organization need to be able to respond within 15 minutes if there is an information security incident, as it is required to do in the event of a breach of select agent Tier 1 physical security? Should there be 3 barriers to data access, as there are to physical access (ie, barriers at the building door, external door to the anteroom, and internal door in the lab)? A videocamera records any movement in or out of restricted spaces, but should all activities on IT systems be logged?

Incident response for information systems is difficult to compare to that for physical security and difficult to define and separate for the purpose of designing and implementing countermeasures. If an unauthorized individual disables a physical security control through an IT breach, it is both an information security incident and a physical security incident. If an individual not approved by a security risk assessment accesses, modifies, or deletes select agent inventory data, could that lead to physical access and unauthorized removal of the actual agent?

Other Challenges

The threat and vulnerability guidance from 1995[62] and 1996[63] cited in the Guidance have been superseded in the past 20 years by other NIST publications. One of the difficult aspects of determining the necessary IT security baseline is understanding an acceptable level of risk. Responsible officials need additional information regarding

the threats they need to most focus on when striving to protect the IT infrastructure supporting select agent research. For example, defending an IT system against a student in a dorm trying to access data to see if he can do it is much different from defending the system against a state-sponsored attacker or terrorist. It is impossible to know all threats an entity could face, but there needs to be sufficient security to stop reasonable threats to the entity.

Should controls include a review of all activities on the information system? When making decisions on resource allocations, the responsible official should consider possible risks and vulnerabilities in the areas of physical security, access control, medical and research devices, inventory, and the environment (see Appendix table at http://online.liebertpub.com/hs). As mentioned in the Guidance, the responsible official should contact his or her IT department to thoroughly discuss the IT security requirements for the particular circumstances, but the need to include individuals with special expertise in IT security in this conversation should be emphasized.

Another critical challenge has been in communications between IT security and other personnel. These difficulties are not limited to lack of understanding between scientists and IT security personnel, but also include miscommunication between the latter and individuals managing facilities, safety, and physical security, law enforcement officials, subcontractors, government agencies, and others critically involved, including IT personnel not directly involved in security. Overlapping terminology is partly to blame: for example, the use of the nonspecific term "intrusion detection system," which could apply to both physical and cybersecurity. An IT security person might hear that an intrusion detection system is necessary but fail to realize that it should be designed to detect both types of intrusions, not just cybersecurity breaches.

Finally, a key element to improving IT security in select agent–registered entities and supporting communications among regulatory agencies and select agent–registered entities is the need for ongoing and specialized training of CDC DSAT and USDA select agent program file managers and inspectors in these areas so that they can be knowledgeable and can work effectively with entity IT security staff to ensure an effective IT security infrastructure has been developed and implemented to support critical work with select agents.

Conclusions

The fast-changing biosecurity requirements and the challenges outlined here are not intractable, but more and better-targeted guidance is needed. Responsible officials and entities can strengthen physical security by enhancing information security supporting select agent research in a number of ways while minimizing the long-term impacts on research.

FISMA standards should be implemented for select agent restricted data and research data. While FISMA was written for the security of government information systems and requires significant resources to implement, it can, with careful planning, be used to improve the IT security infrastructure required for work with select agents. FISMA will not solve all of the information security challenges for select agents, but it is actively maintained by information security professionals at NIST responsible for technology standards, widely known in the government, and has been widely adopted. FISMA will not replace good judgment or solid risk management, but it could focus an institution on the areas of highest risk to ensure a consistent approach in risk management of select agent research. In fact, good judgment and an understanding of the threats may even be more important than the specific information security framework used. Despite the recommendation to use FISMA standards, we fully acknowledge its limitations because of variations in select agent lists internationally and over time. As a part of FISMA, an annual cycle should be undertaken of reassessing the entity to identify changes since the last assessment and determining if any changes need to be made to the environment to provide sufficient protection.

The strategies mandated by FISMA are used in the Cybersecurity Framework for Critical Infrastructure (the Framework),[64] a guidance document released in February 2014 for nongovernment organizations and created in response to Executive Order 13636 (particularly section 4), which requires more threat sharing between government and nongovernment entities. The Department of Energy worked with the Electricity Subsector and Oil & Natural Gas Subsector Coordinating Councils, along with other sector-specific agencies, on adopting the Framework for improving critical infrastructure cybersecurity.[65] Practices consistent with FISMA and this Framework should become increasingly common in entities contracting with the government and others, including many research institutions. This uniform approach would result in a more consistent knowledge base and application of FISMA requirements among entities. In addition, knowledge of information security controls necessary for all sensitive research environments would allow for lessons learned in other areas to be applied by the biosecurity community. It may also help reduce some of the costs of biosecurity by eliminating security controls in the select agent scopes or even in scopes of programs in other parts of an institution that would duplicate or unnecessarily add to those provided by the overall institutional information security program.

Select agent–registered entities using this Framework will also remove the need for the select agent program to maintain separate information security guidance beyond FISMA. By starting with implementation of the lowest level of FISMA security controls, entities could set plans to reach the FISMA "moderate" level required to secure IT systems to the extent needed for select agent research and then

perform a data categorization and risk assessment to determine if additional security controls are needed, or the select agent regulator could specify the FISMA level of security required.

Entities would be apt to achieve a FISMA "low" level compliance within a year. This could be accomplished by establishing a self-imposed implementation time period coinciding with the annual select agent program internal inspections required to be completed by each entity with select agent–registered laboratories. During this effort and after CDC/APHIS releases guidance on what can be shared, institutions could benchmark among themselves without fear of sanctions, release pertinent data on threats to biosecurity, and expand communications with the biosecurity community around IT security.

A FISMA "moderate" level could be reached in 3 or 4 years and eventually verified during DSAT renewal inspections. Subsequently, select agent regulations may be updated to incorporate FISMA, with input from the biosecurity community regarding the impact on the research enterprise and the effectiveness of these short- and long-term enhancements to information security.

Another worthwhile modification to the select agent program would be to train the DSAT inspectors on the minimal aspects of information security so inspections include formal questions on IT security in the context of biosecurity. Once existing information security controls are replaced with FISMA, the select agent program and the research community can work together toward more customized security categorization and derive necessary security controls uniquely suited to select agent research. The concept of good judgment also needs to be applied throughout the select agent community so that if an entity disagrees with a restriction on sharing of information, it is provided with a suitable outlet to resolve this conflict, because an information security control framework will be powerless to stop an entity from sharing data it believes should be public. This work could also involve international entities so that consistent protections are in place where there is restricted access to pathogens of consequence.

There should be a secure platform to share biosecurity IT information. The FBI or select agent program should act as a conduit for the release of information on threats and incidents specifically targeting research facilities, including root causes and attack techniques, or alternatively facilitate that exchange of information among IT personnel. This would be similar to the ongoing exchange of information regarding laboratory incidents involving select agents[66] and would help institutions learn from the failures of others and verify that their own systems could withstand similar threats. This is consistent with a 2014 report from US Transportation Command that addressed the benefits of incident sharing; it also mentioned privacy concerns that could be reduced by sharing data only in secure closed communities with a minimum of personally identifiable information shared.[67] Additionally, timely knowledge regarding patterns of attacks, either perpetuated by advanced assailants with significant resources or less capable ones, would help institutions focus their efforts and resources where they are most urgently needed. For instance, if an entity experienced a cyber-incident where the root cause was determined to be a failure to change a default password on a physical security system, thereby allowing an intruder to unlock doors to gain access to select agents, then other entities could verify that all of their own physical security systems had their default passwords changed. Alternatively, if accidental failures of physical security control systems were known to occur frequently, institutions could make sure to design redundancies in those systems. A rapid exchange of critical intelligence could take place through a secure information-sharing and analysis center that would also serve as a platform to plan workshops designed to improve dialogue and understanding among the research, IT, and security communities.[68] The defense industrial base has suffered from attacks by advanced attackers in which the incident data was shared through an information security investigation company and other entities were able to use the shared data to identify whether their systems had been breached so that they could then initiate an incident response.[69]

An improvement in the state of information security in biosecurity seems daunting, but it is necessary in order to stop current threats and prepare for future ones. The benefits of a proactive approach to making the necessary changes now will, in the authors' opinion, outweigh the monetary costs and prevent the security and research expenses of reactive measures that would need to be implemented if a major security breach were to occur. While initially implementation costs of FISMA standards may compound the substantial financial burden borne by institutions where select agent research is conducted, this possibility cannot preclude a discussion of implementing better standards. In-depth cost-benefit analyses are notoriously difficult to implement before a regulation becomes effective in a new environment, and sometimes even afterward, but policies and procedures based on risk analysis that includes scoping and common security controls, leading to the elimination of control redundancies, are more likely to produce cost-effective risk reduction at the institutional level than are the current standards.[70] Additionally, metrics of and measures of metrics of cybersecurity may be institution-specific,[71] adding to the challenge of defining costs and benefits across the board.

References

1. Additional Requirements for Facilities Transferring or Receiving Select Agents. 42 CFR 72, 1997.
2. Cole LA. Bioterrorism: still a threat to the United States. January 18, 2012. Combating Terrorism Center website.

https://www.ctc.usma.edu/posts/bioterrorism-still-a-threat-to-the-united-states. Accessed April 7, 2015.
3. Federal Select Agent Program. About Us. 2014. http://www.selectagents.gov/about.html. Accessed April 7, 2015.
4. US Government Accountability Office. *High-Containment Laboratories: National Strategy for Oversight Is Needed.* GAO-09-574. Washington, DC: GAO; 2009. http://www.gao.gov/new.items/d09574.pdf. Accessed April 7, 2015.
5. Committee on Laboratory Security and Personnel Reliability Assurance Systems for Laboratories Conducting Research on Biological Select Agents and Toxins. *Responsible Research with Biological Select Agents and Toxins.* Washington, DC: National Academies Press; 2009.
6. US Government Accountability Office. *Overlap and Duplication: Federal Inspections of Entities Registered with the Select Agent Program.* GAO-13-154. Washington, DC: GAO; 2013. http://www.gao.gov/assets/660/651730.pdf. Accessed April 7, 2015.
7. US Government Accountability Office. Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. *High-Containment Biosafety Laboratories: Preliminary Observations on the Oversight of the Proliferation of BSL-3 and BSL-4 Laboratories in the United States.* Statement of Keith Rhodes, Chief Technologist, Center for Technology and Engineering, Applied Research and Methods. GAO-08-108T. Washington, DC: GAO; 2007. http://www.gao.gov/assets/120/117997.pdf. Accessed April 7, 2015.
8. *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism.* New York: Vintage Books; 2008. http://www.absa.org/leg/WorldAtRisk.pdf. Accessed April 7, 2015.
9. US Department of Agriculture. *Report of the Trans-Federal Task Force on Optimizing Biosafety and Biocontainment Oversight.* July 2009. http://www.ars.usda.gov/is/br/bbotaskforce/biosafety-FINAL-REPORT-092009.pdf. Accessed April 7, 2015.
10. Ad Hoc Committee on the Safe Shipment and Handling of Etiologic Agents, Center for Disease Control. *Classification of Etiologic Agents on the Basis of Hazard*. 4th ed. Center for Disease Control, Office of Biosafety; 1974.
11. National Cancer Institute. *Safety Standards for Research Involving Oncogenic Viruses.* Washington, DC: US Department of Health, Education and Welfare; Public Health Service; National Institutes of Health; 1974.
12. National Institutes of Health. *NIH Guidelines for Research Involving Recombinant DNA Molecules.* 2013.
13. Antiterrorism and Effective Death Penalty Act of 1996. Pub. L. No. 104-132, 110 Stat. 1214. http://www.gpo.gov/fdsys/pkg/PLAW-104publ132/html/PLAW-104publ132.htm. Accessed April 7, 2015.
14. Public Health Security and Bioterrorism Preparedness and Response Act of 2002. 42 U.S.C. 262a, 2002. http://www.gpo.gov/fdsys/pkg/PLAW-107publ188/pdf/PLAW-107publ188.pdf. Accessed April 7, 2015.
15. US Department of Agriculture. Agricultural Bioterrorism Protection Act of 2002 and Related Provisions. *Fed Regist* 2002;77(194):61056-61081. http://www.gpo.gov/fdsys/pkg/FR-2012-10-05/pdf/2012-24434.pdf. Accessed April 7, 2015.
16. Possession, Use, and Transfer of Select Agent and Toxins. 7 CFR 3.331, 2013.
17. Possession, Use, and Transfer of Select Agents and Toxins, Subchapter E – Viruses, Serums, Toxins, and Analogous Products; Organisms and Vectors. 9 CFR 1.121, 2013.
18. Select Agents and Toxins Subchapter F – Quarantine, Inspection, Licensing. 42 CFR 1.73, 2013.
19. *Biosafety in Microbiological and Biomedical Laboratories.* 5th ed. Washington, DC: US Department of Health and Human Services; 2009. http://www.cdc.gov/biosafety/publications/bmbl5/BMBL5_introduction.pdf. Accessed April 7, 2015.
20. Franz DR. The dual use dilemma: crying out for leadership. *Saint Louis University Journal of Health Law & Policy* 2013; 7(1):5-58.
21. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. P.L. 107-56, 2001. http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/content-detail.html. Accessed April 7, 2015.
22. Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, National Research Council. *Biotechnology Research in an Age of Terrorism.* Washington, DC: National Academies Press; 2004.
23. National Science Advisory Board for Biosecurity. *Enhancing Personnel Reliability among Individuals with Access to Select Agents.* Washington, DC: NSABB; 2009.
24. Herfst S, Schrauwen EJ, Linster M, et al. Airborne transmission of influenza A/H5N1 virus between ferrets. *Science* 2012;336(6088):1534-1541.
25. Imai M, Watanabe T, Hatta M, et al. Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets. *Nature* 2012;486(7403):420-428.
26. United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern. Washington, DC: National Institutes of Health; Office of Science Policy; 2012. http://osp.od.nih.gov/sites/default/files/resources/United_States_Government_Policy_for_Oversight_of_DURC_FINAL_version_032812_1.pdf. Accessed April 7, 2015.
27. United States government policy for institutional oversight of life sciences dual use research of concern. *Fed Regist* 2013; 78:12369-12372. https://federalregister.gov/a/2013-04127. Accessed April 7, 2015.
28. Malakoff D, Enserink M. Dual use research. New U.S. rules increase oversight of H5N1 studies, other risky science. *Science* 2013;339(6123):1025.
29. Office of the Assistant Secretary for Preparedness and Response. *Report of the Working Group on Strengthening the Biosecurity of the United States.* 2009. http://orise.orau.gov/emi/scapa/files/biosecurity-report.pdf. Accessed April 7, 2015.
30. US Department of Health and Human Services; US Department of Agriculture. *Select Agents and Toxins Security Plan Template.* 2007. http://www.selectagents.gov/resources/Security_Plan_Template_Final_APHIS-CDC-English.pdf. Accessed April 7, 2015.
31. US Government Accountability Office. *Biosafety Laboratories: Perimeter Security Assessment of the Nation's Five BSL-4 Laboratories.* Washington, DC: GAO; 2008.
32. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. *Report of the Defense Science*

Board Task Force on Department of Defense Biological Safety and Security Program. Washington, DC: Defense Science Board; 2009.
33. The White House. Executive Order 13546—Optimizing the Security of Biological Select Agents and Toxins in the United States. July 2, 2010. https://www.whitehouse.gov/the-press-office/executive-order-optimizing-security-biological-select-agents-and-toxins-united-stat. Accessed April 7, 2015.
34. US Department of Health and Human Services; US Department of Agriculture. Federal Experts Security Advisory Panel Recommendations Concerning the Select Agent Program. November 2, 2010. http://www.phe.gov/Preparedness/legal/boards/fesap/Documents/fesap-recommendations-101102.pdf. Accessed April 7, 2015.
35. Centers for Disease Control and Prevention; Animal and Plant Health Inspection Service. *Security Guidance for Select Agent or Toxin Facilities.* 2013. http://www.selectagents.gov/resources/Security_Guidance_v3-English.pdf. Accessed April 7, 2015.
36. Animal and Plant Health Inspection Service; Centers for Disease Control and Prevention. *Information Systems Security Control Guidance Document*. 2014. http://www.selectagents.gov/resources/Information_Systems_Security_Control_Guidance_version_3_English.pdf. Accessed April 7, 2015.
37. Berger KM, Roderick J. *Bridging Science and Security for Biological Research: Personnel Security Programs.* Washington, DC: American Association for the Advancement of Science; 2014. http://www.aaas.org/report/bridging-science-and-security-biological-research-personnel-security-programs. Accessed April 7, 2015.
38. Bashour N. The big data blog, part V: interview with Dr. Ivo Dinov. AAAS website. April 28, 2014. http://www.aaas.org/news/big-data-blog-part-v-interview-dr-ivo-dinov. Accessed April 7, 2015.
39. Berger KM, Roderick J. *National and Transnational Security Implications of Big Data in the Life Sciences.* Washington, DC: American Association for the Advancement of Science; 2014. http://www.aaas.org/report/national-and-transnational-security-implications-big-data-life-sciences. Accessed April 7, 2015.
40. National Science Advisory Board for Biosecurity. *Addressing Biosecurity Concerns Related to the Synthesis of Select Agents.* Washington, DC: NSABB; 2006.
41. Richards SL, Pompei VC, Anderson A. BSL-3 laboratory practices in the United States: comparison of select agent and non–select agent facilities. *Biosecur Bioterror* 2014;12(1):1-7
42. US Department of Health and Human Services; Office of Inspector General. *Summary Report on Universities' Compliance with Select Agent Regulations.* Washington, DC: DHHS; 2006. https://oig.hhs.gov/oas/reports/region4/40502006.pdf. Accessed April 7, 2015.
43. US Department of Health and Human Services; Office of Inspector General. *Summary Report on Select Agent Security at Universities.* Washington, DC: DHHS; 2004. https://oig.hhs.gov/oas/reports/region4/40402000.pdf. Accessed April 7, 2015.
44. Herley C. So long, and no thanks for the externalities: the rational rejection of security advice by users. Proceedings of the 2009 New Security Paradigms workshop; Oxford, United Kingdom. http://www.nspw.org/proceedings/2009. Accessed April 7, 2015.
45. US Department of Health and Human Services; Office of Inspector General. *Summary Report on State, Local, Private, and Commercial Laboratories Compliance with Select Agent Regulations.* Washington, DC: DHHS; 2008. http://oig.hhs.gov/oas/reports/region4/40601033.pdf Accessed April 7, 2015.
46. US Department of Agriculture. *Audit Report: Animal and Plant Health Inspection Service Evaluation of the Implementation of the Select Agent or Toxin Regulations Phase II.* Washington, DC: USDA; 2006. http://www.usda.gov/oig/webdocs/33601-3-AT.pdf. Accessed April 7, 2015.
47. Kissel R, ed. *Glossary of Key Information Security Terms.* 2d ed. Washington, DC: National Institute of Standards and Technology; 2013. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf. Accessed April 7, 2015.
48. Federal Information Security Management Act of 2002. P.L. 107-347, 44 U.S.C. 3541-3549, 2002. http://www.dhs.gov/federal-information-security-management-act-fisma. Accessed April 7, 2015.
49. Notice Regarding the Applicability of the Federal Information Security Management Act to NIH Grantees. January 9, 2008. http://grants.nih.gov/grants/guide/notice-files/NOT-OD-08-032.html. Accessed April 7, 2015.
50. *Security and Privacy Controls for Federal Information Systems and Organizations.* Revision 4. Washington, DC: National Insitute of Standards and Technology; 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Accessed April 7, 2015.
51. Office of Management and Budget. *Annual Report to Congress: Federal Information Security Management Act*. May 1, 2014. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2013_fisma_report_05.01.2014.pdf. Accessed April 7, 2015.
52. Office of Management and Budget. Memorandum for Heads of Executive Departments and Agencies: FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. April 21, 2010. https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf. Accessed April 7, 2015.
53. Department of the Navy. *DoD Information Assurance Certification and Accreditation Process (DIACAP) Handbook.* Version 1.0. July 15, 2008. http://www.acqnotes.com/Attachments/NAVY%20DoD%20Information%20Assurance%20Certification%20and%20Accreditation%20Process%20Handbook.pdf. Accessed April 7, 2015.
54. Disclosure of Information, 48 CFR 252.204-7000, 1991.
55. US Department of Health and Human Services. HIPAA Administrative Simplification Statute and Rules. 45 CFR 160, 162, and 164, 2013. http://www.hhs.gov/ocr/privacy/hipaa/administrative/. Accessed April 7, 2015.
56. Family Educational Rights and Privacy, 34 CFR 1.99, 2011.
57. Information security. US Nuclear Regulatory Commission website. Updated January 9, 2015. http://www.nrc.gov/security/info-security.html. Accessed April 7, 2015.
58. *Standards for Security Categorization of Federal Information and Information Systems.* Gaithersburg, MD: National Institute of Standards and Technology; 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf. Accessed April 7, 2015.
59. *Minimum Security Requirements for Federal Information and Information Systems.* Gaithersburg, MD: National Institute

of Standards and Technology; 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf. Accessed April 7, 2015.
60. US Department of Commerce. *Guide for Applying the Risk Management Framework to Federal Information Systems.* Gaithersburg, MD: National Institute of Standards and Technology; 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf. Accessed April 7, 2015.
61. *Guide to Industrial Control System Security.* SP 800-82. Gaithersburg, MD: National Institute of Standards and Technology; 2015. http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_draft.pdf. Accessed April 15, 2015.
62. *An Introduction to Computer Security: The NIST Handbook.* Gaithersburg, MD: National Institute of Standards and Technology; 1995. http://www.davidsalomon.name/CompSec/auxiliary/handbook.pdf. Accessed April 7, 2015.
63. Swanson M, Guttman B. *Generally Accepted Principles and Practices for Securing Information Technology Systems.* Gaithersburg, MD: National Institute of Standards and Technology; 1996. http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf. Accessed April 7, 2015.
64. *Framework for Improving Critical Infrastructure Cybersecurity.* Gaithersburg, MD: National Institute of Standards and Technology; 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. Accessed April 7, 2015.
65. *Energy Sector Cybersecurity Framework Implementation Guidance*. Washington, DC: US Department of Energy; 2015. http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf. Accessed April 15, 2015.
66. Henkel RD, Miller T, Weyant RS. Monitoring select agent theft, loss and release reports in the United States—2004-2010. *Appl Biosaf* 2012;17(4):171-180.
67. *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors.* Report of the Committee on Armed Services, U.S. Senate. 2014. http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf. Accessed April 15, 2015.
68. National Council of Information Sharing and Analysis Centers website. http://www.isaccouncil.org/. Accessed April 15, 2015.
69. Sanger D, Barboza D, Perlroth N. Chinese army is seen as tied to hacking against U.S. *NY Times* February 18, 2013. http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?_r=0. Accessed April 15, 2015.
70. Ross R, Katzke S, Toth P, eds. The new FISMA standards and guidelines changing the dynamic of information security for the federal government. Military Communications Conference, 2005 MILCOM 2005 IEEE; October 17-20, 2005. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1605789&tag=1. Accessed April 7, 2015.
71. Black PE, Scarfone K, Souppaya M. Cyber security metrics and measures. In: Voeller JG, ed. *Wiley Handbook of Science and Technology for Homeland Security:* New York: John Wiley & Sons; 2008.

Manuscript received December 5, 2014;
accepted for publication March 4, 2015.

Address correspondence to:
Carole R. Baskin, DVM, MSc, CPIA
Associate Professor
Environmental & Occupational Health
Institute for Biosecurity
Saint Louis University
3545 Lafayette Room 464
St Louis, MO 63104

E-mail: cbaskin2@slu.edu