



3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008, USA

Telephone: 847.253.1545
Facsimile: 847.253.1443

Web Site: www.isaca.org

17 September 2009

The Honorable John D. (Jay) Rockefeller IV, Chairman
Committee on Commerce, Science and Transportation
US Senate

The Honorable Olympia J. Snowe
Committee on Commerce, Science and Transportation
US Senate

The Honorable Bill Nelson
Committee on Commerce, Science and Transportation
US Senate

The Honorable Evan Bayh
Committee on Commerce, Science and Transportation
US Senate

RE: Senate Bill 773—Cybersecurity Act of 2009

Dear Chairman Rockefeller, Senator Snowe, Senator Nelson and Senator Bayh:

Congratulations on the progress that has been made on the United States Cybersecurity Act of 2009. ISACA continues to follow the development of this significant legislation, and we appreciate the opportunity to again provide our comments. As stated in our previous communication, ISACA views the introduction of this legislation as a critical step in addressing the significant threats to our nation's digital infrastructure.

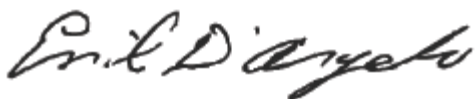
You will recall that ISACA is an international association of professionals who provide security, risk management and assurance services to their organizations/clients in order to help protect the cyberinfrastructure. With 86,000 constituents in more than 160 countries, ISACA members have developed, implemented, managed and assessed security controls in leading critical infrastructure organizations, as well as governments, on a global basis. As an organization, ISACA provides for the continued development of its members through certifications, training and research, much of which is accomplished by leveraging the significant knowledge and experience base of the collective organization. ISACA members also participate in the development of international security standards through a liaison relationship with the International Organization for Standardization. We have developed frameworks such as COBIT[®], which are accepted internationally and have become *de facto* standards for defining controls in IT environments. COBIT is already utilized by a number of federal agencies' Inspectors General, and has been successfully implemented in organizations such as the Department of Veterans Affairs and the Federal Savings and Loan Insurance Corporation.

ISACA continues to be supportive of the overall intent of this legislation. It is very apparent that the bill has been revised to address many of the concerns cited by ISACA and other organizations when the first draft was circulated earlier this year. There remain several sections of the bill, however, that require further expansion or clarification. These sections are discussed in detail in the attachment. As before, we have limited our detailed comments to those sections of the draft bill that we believe will have the greatest impact on the effectiveness of this legislation and that represent the areas of greatest interest for our membership. Our comments encompass the following general themes:

- Cybersecurity certification and training are already well established in the private sector. The federal government should leverage these resources as opposed to undertaking the complex and costly task of recreating and maintaining them.
- Private-sector organizations should not be compelled to adhere to government-developed standards when international standards that are already in use appropriately address cybersecurity requirements. The primary issue is not the lack of effective standards, but the lack of consistency and permanence in their application. Ensuring that companies are equipped and incented to meet and adhere to existing standards should be the focus.
- NIST is a nonregulatory agency whose stated mission is “to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology...” (www.nist.gov/public_affairs/general2.htm). While NIST information security standards are certainly used in the private sector, they are used voluntarily. Private organizations should continue to have the ability to choose standards that best fit their particular business and operational model. In turn, NIST should continue to partner with ANSI and other public-sector organizations to foster continued improvement of security standards and best practices across all sectors.
- Nationally focused overtures in an area that has such significant international aspects are counterproductive.
- While progress has been made with this new draft, greater clarity and better definition of terms are still needed throughout the bill.

Again, we appreciate the opportunity to comment on the draft Senate Bill 773—Cybersecurity Act of 2009 and thank you for considering our views. We would be happy to discuss them with you in further detail and provide any other assistance that might be required to ensure that efforts to provide a safe and secure cyberinfrastructure are successful and lasting.

Respectfully submitted,



Emil D'Angelo, CISA, CISM
International President
ISACA (www.isaca.org)

Attachment

Cybersecurity Act of 2009—Specific Comments

Title I—Workforce Development

Sec 101 Certification and Training of Cybersecurity Professionals

(a) IN GENERAL—As stated in our comments to the original draft, as a credentialing organization for information security and assurance professionals, ISACA certainly supports the concept of certification for professionals within the cybersecurity field. We are concerned that the revised language—while admittedly somewhat ambiguous—still seems to imply that a government-developed certification program would result in the creation of one or more new certifications. Should this be true, then ISACA vigorously recommends that this direction be reconsidered, for reasons that provided below. If this is not the case, the language should be clarified to indicate that the proposed program will leverage public-sector certifications, similar to the definition found in the US Department of Defense’s Information Assurance Workforce Improvement Program Manual (DoD 8570.01-M). The Manual identifies a specific subset of private-sector certifications that map to the various information assurance roles within the US military. The credentials chosen by the DoD are required to be accredited by the American National Standards Institute (ANSI), attesting to the rigor and comprehensiveness of each certification’s credentialing process. The DoD recognized existing globally accepted credentials and leveraged the effort used in creating the well-established certification criteria and processes that have been extensively reviewed and vetted not only by ANSI, but also by industry and government IT professionals throughout the world for more than 40 years. The model put forward by DoD will work just as effectively for all federal agencies and critical infrastructure organizations. Its adoption will save the federal government and private sector significant time, effort and expense. It is our sincere hope that this is the direction that this legislation will take.

Should the development of a specific government cybersecurity certification still be planned, there are several points that should be considered:

- **Multiple certifications would be required:** In order to certify the pool of highly competent cybersecurity specialists that the government requires, no single certification will provide any level of assurance that an individual indeed possesses deep skills in a specific security discipline, such as secure code development, digital forensics or network security. Each of these areas certainly shares common concepts, but there are also significant differences that demand distinct, specialized knowledge, skills and abilities, and separate, distinct certifications which attest to these skills.
- **Management and oversight of multiple certifications would require significant resources:** Developing and managing a certification program will require a significant investment in time and resources. A comprehensive certification program will require several years’ investment to identify job classifications, knowledge and skills and to relate them to the content for a certification, followed by development of the resulting certification examinations, continuing professional educational processes and all of the related training/development programs. While the federal government may have the resources, time is certainly not on the nation’s side. There is also the consideration that those who would develop a “new” certification will more than likely be cybersecurity

professionals who already have the very certifications this approach would choose to ignore.

- **“National” certification would be in conflict with international objectives:** A “national” certification program is somewhat at odds with **SEC. 207** of this legislation, **“International Norms and Cybersecurity Deterrent Measures,”** which calls for the President to “work with representatives of foreign governments to develop norms, organizations, and other cooperative activities...to improve cybersecurity” and to “encourage international cooperation in improving cybersecurity on a global basis.”

Promoting a US-centric certification program will more than likely alienate the very governments we seek to engage, particularly when these governments may already recognize commercial certifications. Furthermore, multinational companies would be faced with one certification standard for the US, and potentially numerous others for countries where they operate—particularly should these countries follow the lead established by the US and develop their own independent certification. Finally, multinational organizations would be faced with having to implement different security standards in different countries, which could very well weaken their existing security programs by introducing confusion and conflicting practices.

ISACA firmly believes that the certification needs of the wide spectrum of security and assurance professionals are already more than fulfilled by ISACA and other certifying organizations within the private sector. Each of these organizations offers unique certifications that address specific skill sets within the information security discipline, from the deeply technical fields such as forensics, to security program management and leadership. Currently, ISACA offers two professional certifications that would be of great benefit to professionals who provide assurance services or manage information security programs and processes. They are both ANSI-accredited under International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17024:2003 and each is among the few certifications formally approved by the US Department of Defense in its Information Assurance Workforce Improvement Program Manual (DoD 8570.01-M). The Certified Information System Auditor™ (CISA®) certification, which was first offered in 1978, has been awarded to more than 70,000 professionals since the program’s inception. The Certified Information Security Manager® (CISM®) designation, which is specifically intended to demonstrate professional excellence in developing and managing cybersecurity programs, has been awarded to more than 11,000 professionals since 2002. The CISA and CISM certifications are based on a rigorous job practice analysis, which captures the critical knowledge that assurance and security management personnel need in their positions and in the essential tasks required to help protect organizations from cyberthreats.

A related matter is the term “cybersecurity professional.” This is very broad term, which needs further definition within the bill. Identification of specific roles and associated skill sets will guide the certification requirements for each subdiscipline, and in turn indicate which of the available certification programs is appropriate. This task would appropriately fall to the Office of Personnel Management. This recognition of diversity with the ranks of cybersecurity professionals is actually supported by language in **Section 104 (c) Classification**, which states that “the President’s cybersecurity coordinator or his designee, in consultation with affected Federal agencies and councils, shall coordinate the establishment of new job classifications for

cybersecurity functions in government and certification requirements for each job category.” Note that this job classification for security professionals is long overdue, and ISACA strongly supports this effort. However, unless it is the aim of this legislation to develop a number of specialized certifications, which is an onerous task at best, the most logical and expedient approach is to leverage the already well-developed certifications that exist in the public sector and map them to the appropriate job classifications, as the DoD has done with its program.

(b) TRAINING AND DEVELOPMENT—ISACA has a longstanding relationship with the academic community. For many years we have worked with leading academic institutions to develop model curriculum and supporting course materials in the areas of assurance, information security management, risk management, and IT governance. Based on this experience, we can assure the federal government that there already exists in both the commercial market and within higher education institutions a significant selection of training resources pertaining to all aspects of information security, from the highly technical to broad management-level courses. ISACA believes that, just as with certifications, the federal government will be much better served by leveraging the significant resources already available in the private sector as opposed to developing its own training program and supporting materials.

Title II—Plans and Authority

Section 201 Cybersecurity Responsibilities and Authority.

(10) This language is unclear. ISACA recommends that this section be expanded or otherwise revised.

Section 204 NIST Cybersecurity Performance Measures and Compliance.

Overall, this section represents significant progress from its predecessor, and is a strong indicator that the authors of this bill are listening to and acting on the comments that were previously provided. There are, however, some areas that still leave much open for interpretation.

(a) IN GENERAL—The concept of collaboration with the private sector (“regulatory entities, industry sectors, and non-governmental organizations”) is a welcome addition to this section. However, subsequent language, specifically “. . .the National Institute of Standards and Technology . . .shall establish or recognize measurable and auditable cybersecurity risk management metrics, measures, and best practices” should be clarified to indicate that NIST will “establish” these metrics and best practices for the federal government institutions, but will “recognize” selected existing industry standards for private-sector critical infrastructure organizations. This would provide assurance that “risk management metrics, measures, and best practices” developed by NIST will not be imposed on private industry, regardless of its designation of critical infrastructure. This is not to say that organizations could not or would not choose NIST standards over ISO or others, particularly if they were creating a new program. However the *imposition* of a new set of government standards, particularly for already highly regulated industries that may be designated as critical infrastructure, would most certainly add confusion, cost and complexity to their security programs. These industries, such as banking or health care, already use internationally accepted standards to manage their information security. The focus should be on ensuring that these companies are sufficiently staffed and incented to meet and adhere to standards already in place.

(b) CRITERIA FOR STANDARDS—This section is unclear. ISACA recommends expansion or revision.

(d) COMPLIANCE—A strong cybersecurity program must undergo frequent audits to ensure that organizations remain in compliance with all relevant standards and policies. ISACA strongly endorses the requirement of independent audits, and is very pleased to see that the language that suggested government audits of private organizations has been removed. A remaining concern, however, is what standards these independent audits will utilize. The current language calls for “an independent audit that evaluates compliance with the standards established under this section.” As noted above, it is unclear whether this means standards authored by NIST or instead audits will be more appropriately based on generally accepted international standards that are already in use by the institution in question.

Sec 207 International Norms and Cybersecurity Deterrence Measures.

As noted earlier, ISACA believes that the inclusion of the international security community is critical to the success of this legislation. The collaboration that is promoted in this section is somewhat at odds with the idea of “national” certification discussed in Section 101. ISACA strongly recommends that the federal government follow the lead established in DoD 8570.01-M and leverage internationally accepted and accessible security certifications rather than undertake the development of a US-centric certification program.

Sec 208 Federal Secure Products and Services Acquisitions.

(a) ACQUISITION REQUIREMENTS—ISACA approves most changes made to this section and strongly endorses the use of the federal government’s significant buying power to drive greater security for commercially available products and services. This is not to say that the government should impose standards on private industry. Rather, by the careful documentation of security requirements within requests for proposals (RFPs) and consistent enforcement of these requirements, the government can ensure that vendors will make a concerted effort to integrate more effective security controls and features into their products and services.

There is one component of this section that ISACA believes needs greater clarification: the reference to cybersecurity professional certifications described in Section 101. As stated previously, these certifications should be those already in existence, as opposed to any new government-sponsored certification. If the program described in Section 101 is indeed intended to leverage existing private-sector certifications, there is no issue.

(c) ACQUISITION COMPLIANCE—The wording in this section is not clear and should be revisited. The language “any proposal submitted...shall demonstrate compliance with any such applicable standard” does not clearly explain what standards are applicable. Requirements for security should be part of any RFP that involves IT products or services; however, it is not appropriate to compel private industry to meet federal standards that dictate how those requirements are met.

Title IV Public-Private Coordination

SEC 402 State and Regional Cybersecurity Enhancement Program.

(a) CREATION AND SUPPORT OF CYBERSECURITY CENTERS—ISACA embraces the concept of regional centers and believes they have great potential to support small and medium-sized businesses as they wrestle with the need to implement effective security while working with limited resources. Two significant issues faced by smaller enterprises are the lack of awareness of security requirements and insufficient in-house resources necessary to take appropriate measures to secure systems. These proposed centers have great potential to effectively address these issues. Through the combined efforts of our Chicago-based international office and constantly expanding network of local chapters (currently 69 chapters exist across the United States, with a current membership of nearly 34,000 security and assurance professionals), ISACA will be able to provide significant support for this proposed program.

(b) PURPOSE—(1) The bill states that “The purpose of the centers...is the promotion of available and widely accepted cybersecurity standards developed at the National Institute of Standards and Technology to Centers and...to small and medium-sized companies throughout the United States.” As discussed earlier, ISACA views the imposition of NIST standards on private industry as problematic. Also, it is not necessarily accurate that NIST security standards are “widely accepted” in private industry. Many companies, while perhaps not advanced in their security programs, already have in place public-sector best practices and standards that are equivalent to NIST standards. In addition, the anticipated volunteers that will work with this program, in many cases, will have much greater experience with internationally accepted standards such as ISO 270001, as well as good and best practices promoted by organizations such as ISACA, (ISC)2, SANS and many others. ISACA recommends that this language be changed to allow for the promotion of “widely accepted and available security standards applicable to small and medium-sized companies,” striking out the reference to NIST.