



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

Telephone: 847.253.1545
Facsimile: 847.253.1443

Web Sites: www.isaca.org

13 July 2009

The Honorable Thomas R. Carper
Committee on Homeland Security and Governmental Affairs
United States Senate
513 Hart Building
Washington, DC 20510

RE: Senate Bill 921—United States Information and Communication Enhancement Act of 2009
(US ICE)

Dear Senator Carper,

Congratulations on the issuance of the marked-up bill titled United States Information and Communication Enhancement Act of 2009 (US ICE) (“the draft”). We very much appreciate the opportunity to provide our comments regarding this draft legislation. ISACA views the introduction of this and related legislation as a critical step in addressing the still significant security gaps that exist today in the federal cyberinfrastructure, and considers this renewed and intensified focus on these difficult issues as essential not only to preserve our domestic security and way of life, but also as a gesture of global leadership in a time of dire need.

ISACA is an international association of professionals who provide security and assurance services to their organizations/clients to help protect the cyberinfrastructure. With 86,000 constituents in more than 160 countries, ISACA’s members have developed, implemented, managed and assessed security controls in leading critical infrastructure organizations, as well as governments, on a global basis. We provide for the continued development of our members through training and research. We also offer several distinct certifications for assurance professionals, two of which directly relate to information assurance. The Certified Information System Auditor™ (CISA®) certification, which was first offered in 1978, has been awarded to more than 60,000 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 10,000 professionals since 2002. Both certifications are American National Standards Institute (ANSI) accredited under International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17024:2003 and each is included in the select certifications formally approved by the US Department of Defense in its Information Assurance Workforce Improvement Program Manual (DoD 8570.01-M).

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 *Control Objectives for Information and related Technology* (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 agency Inspectors General and has been successfully implemented within organizations such as the Department of Veterans Affairs and the Federal Savings and Loan Insurance Corporation.

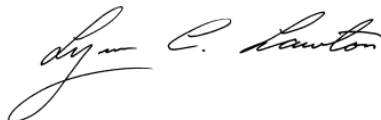
While ISACA applauds and supports the intent of, and concepts contained within, this bill, there are some areas that we feel warrant further consideration. In general terms, a key opportunity we see for this legislation is to reintroduce the concept of *audit*, as opposed to *evaluation*, into the oversight of the federal information security program. There are a number of important reasons for this position, but perhaps the most compelling is the widely acknowledged fact that much of the current evaluation processes surrounding FISMA are paper exercises that are focused simply on the existence, not efficacy, of a control—which often leaves vulnerabilities in place because the controls are not appropriately tested. This is, in part, why many cyberattackers are still able to penetrate defenses and inadvertent data losses continue to occur, as highlighted in the recent revelations regarding the data theft of over a terabyte of sensitive Joint Strike Fighter information and the exposure of Marine One data to global Internet file-sharing sites by an inappropriate use of peer-to-peer (P2P) networking. Senator Carper, your quote puts it all into perspective:

My investigative hearings have uncovered that the federal government's efforts to prepare for and prevent cyber attacks by hackers, terrorists or even other nations are largely uncoordinated, duplicative and ineffective. Federal agencies are spending billions on ineffective security measures that often involve nothing but paperwork, all the while leaving our federal computer networks vulnerable.—
Senator Carper's May 29th response to the President's announcements regarding cybersecurity (emphasis added).
(<http://carper.senate.gov/press/record.cfm?id=313794>)

We have limited our comments to those sections that we believe will have the greatest impact on the effectiveness of this legislation to further protect the national cyberinfrastructure. We have listed these comments in attachment A.

Again, we appreciate the opportunity to comment on the draft Senate Bill 921—United States Information and Communication Enhancement Act of 2009 (US ICE). Thank you for considering our views, which reflect the issues of greatest concern to our membership. 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 national cyberinfrastructure are successful and lasting.

Respectfully submitted,



Lynn Lawton, CISA, FBCS CITP, FCA, FIIA
International President 2007-09
ISACA (www.isaca.org)

Attachment A

General Comments

As discussed previously, ISACA strongly supports the concepts presented in this bill. It is important to note a strength of this legislation is it seeks to build on the significant work that has preceded it. FISMA went far in creating a framework to address the substantive problems the government faced in securing the nation's cyberinfrastructure. However, while progress has been made, wide gaps in compliance still exist across the federal cyberinfrastructure—due not so much to shortcomings of the legislation but rather challenges with implementation.

As an organization that has long promoted the concepts of effective governance, risk management, and effective audit practices, ISACA is uniquely equipped to assist the federal government, utilizing the many tools and frameworks that we have developed in our 40-year history. Many of the concepts and tools that we promulgate are relevant to the major themes contained within this legislation; we are pleased to note the presence of these ideas and anticipate that their effective application will help the government make significant progress in reaching its goal to better secure the cyberinfrastructure.

ISACA acknowledges the following strengths of this bill, and notes that these strengths align closely with ISACA's IT governance and management philosophies which are reflected in our tools, frameworks and publications:

- A focus on coordination
- A focus on measured effectiveness, not simply paper compliance (though this could be further strengthened)
- The mandate of a clear role for agency chief information security officers (CISOs)
- Emphasis on accountability for agency heads
- Promotion of risk management and governance principles
- Promotion of coordination among agency CISOs

Specific Comments

Section 2 (5B) (Findings) *...agencies do not fully understand what information they hold, who has access to that information, and whether the information has been compromised...*

While this assertion is made in the findings section of the bill, there is no specific reference afterwards that addresses this critical shortcoming. Foundational to the protection of any information is a clear understanding of what information exists, where it is located, and what value it has. Without this knowledge, it is impossible to assure it is appropriately and effectively secured. Notably, information inventory and classification, which address this statement, were among the principal goals of FISMA.

Section 3 - Sec. 3552 National Office for Cyberspace: ISACA regards this as a critical position, and believes that a principal responsibility of this role should be to ensure coordination among all agency CISOs.

Section 3 - Sec. 3553 Authority and Functions of the National Office for Cyberspace:

ISACA strongly recommends that the terms “evaluate” and “evaluation” within this section of the legislation be changed to “audit.” The term “audit” in this legislation should be defined as “a formal audit performed in accordance with the Government Auditing Standards issued by the Government Accountability Office.”

Section 3 - Sec. 3554 Agency Responsibilities:

ISACA strongly recommends that the terms “evaluate” and “evaluation” within this section of the legislation be changed to “audit.” The term “audit” in this legislation should be defined as “a formal audit performed in accordance with the Government Auditing Standards issued by the Government Accountability Office.”

Section 3 - Sec 3554 (a) *The head of each agency shall— (6) ensure that the Chief Information Security Officer possesses necessary qualifications, including education, professional certifications, training, experience, and the security clearance required to administer the functions described under this subchapter;*

ISACA strongly recommends that professional security and assurance certifications for CISOs and other assurance personnel be earned from globally recognized and accredited organizations such as ISACA, as opposed to looking to the government to create a national certification and licensure program, as suggested in related draft legislation. If the government were to embark on such a program, it would likely create significant turmoil throughout the security profession and industry in general, reduce the pool of qualified candidates, and isolate the US internationally.

Section 3 - Sec. 3555 Annual Independent Evaluation

ISACA strongly recommends that the terms “evaluate” and “evaluation” within this section of the legislation be changed to “audit.” The term “audit” in this legislation should be defined as “a formal audit performed in accordance with the Government Auditing Standards issued by the Government Accountability Office.”

(a)(4) ISACA recommends that the government consider formally adopting COBIT to use in conjunction with NIST SP 800-53 (Recommended Security Controls for Federal Information Systems and Organizations) to enhance the audit program. COBIT provides a broad framework that includes the concept of governance, which is absent from the NIST standard. Significant work has been already accomplished mapping NIST SP 800-53 to COBIT and, as mentioned earlier, COBIT is already in use within many government agencies today, e.g., by a number of federal agency Inspectors General, the Department of Veterans Affairs and the Federal Savings and Loan Insurance Corporation. COBIT is also accepted internationally and has become the *de facto* standard for defining controls in IT environments.