111TH CONGRESS
1ST SESSION

S. 921

To amend chapter 35 of title 44, United States Code, to recognize the interconnected nature of the Internet and agency networks, improve situational awareness of Government cyberspace, enhance information security of the Federal Government, unify policies, procedures, and guidelines for securing information systems and national security systems, establish security standards for Government purchased products and services, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 28, 2009

Mr. CARPER introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To amend chapter 35 of title 44, United States Code, to recognize the interconnected nature of the Internet and agency networks, improve situational awareness of Government cyberspace, enhance information security of the Federal Government, unify policies, procedures, and guidelines for securing information systems and national security systems, establish security standards for Government purchased products and services, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''United States Information and Communications Enhancement Act of 2009'' or the ''U.S. ICE Act of 2009''.

SEC. 2. FINDINGS.

The Congress finds the following:

(1) The development of an interconnected global information infrastructure has significantly enhanced the productivity, prosperity, and collaboration of people, business, and governments worldwide.

(2) The information infrastructure of the United States is a strategic national resource vital to our democracy, economy, and security.

(3) The Federal Government must increasingly rely on a trusted and resilient information infrastructure to effectively and efficiently communicate with and deliver services to citizens, enhance economic prosperity, defend the Nation from attack, and recover from natural disasters.

(4) Since 2002 the Federal Government has experienced multiple high-profile breaches that resulted in the theft of sensitive information amounting to more than the entire print collection contained in the Library of Congress, including personally identifiable information, advanced scientific re-

search, and prenegotiated United States diplomatic positions.

(5) On March 12, 2008 witnesses testified before a hearing held by the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security of the Committee on Homeland Security and Governmental Affairs of the Senate that—

(A) implementation of the Federal Information Security Management Act of 2002 (Public Law 107–296; 116 Stat. 2135) wastes agency resources on paperwork exercise instead of security;

(B) agencies do not fully understand what information they hold, who has access to that information, and whether the information has been compromised; and

(C) agencies lack effective coordination for mitigating and responding to cyber-related incidents.

(6) The Federal Information Security Management Act of 2002 (Public Law 107–296; 116 Stat. 2135) needs to be amended to increase the coordination of agency activities to enhance situational awareness throughout the Federal Government using

more effective enterprise-wide automated monitoring, detection, and response capabilities.

SEC. 3. COORDINATION OF FEDERAL INFORMATION POLICY.

Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Definitions

''(a) Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

''(b) In this subchapter:

''(1) The term 'adequate security' means security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification, of information.

''(2) The term 'Director' means the Director of the National Office for Cyberspace.

''(3) The term 'incident' means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or

imminent threat of violation of security policies, security procedures, or acceptable use policies.

''(4) The term 'information infrastructure' means the underlying framework that information systems and assets rely on in processing, transmitting, receiving, or storing information electronically.

''(5) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

''(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

''(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

''(C) availability, which means ensuring timely and reliable access to and use of information.

''(6) The term 'information technology' has the meaning given that term in section 11101 of title 40.

''(7)(A) The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''§ 3552. National Office for Cyberspace

''(a) There is established within the Executive Office of the President an office to be known as the National Office for Cyberspace.

''(b) There shall be at the head of the Office a Director who shall be appointed by the President, by and with the advice and consent of the Senate. The Director of the National Office for Cyberspace shall administer all functions under this subchapter and collaborate to the extent practicable with the heads of the appropriate agencies, the private sector, and international partners. The Office shall serve as the principal office for coordinating issues relating to achieving an assured, reliable, secure, and survivable global information and communications infrastructure and related capabilities.

''§ 3553. Authority and functions of the National Office for Cyberspace

''(a) The Director shall develop and implement a comprehensive national cyberspace strategy to ensure a trusted and resilient communications and information infrastructures that—

''(1) enhances economic prosperity and facilitates market leadership for the United States information and communications industry;

''(2) deters, prevents, detects, defends against, responds to, and remediates interruptions and damage to United States information and communications infrastructure;

''(3) ensures United States capabilities to operate in cyberspace in support of national goals; and

''(4) protects privacy rights and preserving civil liberties of United States persons.

''(b) Notwithstanding any provision of law, regulation, rule, or policy to the contrary, the National Office for Cyberspace may—

''(1) direct the sponsorship of the security clearances for Federal officers and employees (including experts and consultants employed under section 3109) whose responsibilities involve critical infrastructure in the interest of national security; and

''(2) employ experts and consultants under section 3109 for cyber security-related work.

''(c) With respect to responsibilities with the Federal Government, the National Office for Cyberspace shall—

''(1) provide recommendations to agencies on measures that shall be required to be implemented

to mitigate vulnerabilities, attacks, and exploitations discovered as a result of activities required pursuant to this section;

''(2) oversee the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 3556;

''(3) to the extent practicable—

''(A) prioritize the policies, principles, standards, and guidelines developed under section 3556 based upon the threat, vulnerability and consequences of an information security incident; and

''(B) develop guidance that requires agencies to actively monitor the effective implementation of policies, principles, standards, and guidelines developed under section 3556;

''(4) require agencies, consistent with the standards promulgated under such section 3556 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(A) information collected or maintained by or on behalf of an agency; or

''(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(5) coordinate and ensure that the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and standards and guidelines developed for national security systems are, to the maximum extent practicable, complementary and unified;

''(6) oversee agency compliance with the requirements of this subchapter, including coordinating with the Office of Management and Budget to use any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements;

''(7) review at least annually, and approving or disapproving, agency information security programs required under section 3554(b); and

''(8) coordinate information security policies and procedures with related information resources management policies and procedures.

''(d)(1) After consultation with the appropriate agencies, the Director shall oversee the effective implementation of governmentwide operational evaluations on a frequent and recurring basis to evaluate whether agencies effectively—

''(A) monitor, detect, analyze, protect, report, and respond against known vulnerabilities, attacks, and exploitations;

''(B) report to and collaborate with the appropriate public and private security operation centers and law enforcement agencies; and

''(C) mitigate the risk posed by previous successful exploitations in a timely fashion and in order to prevent future vulnerabilities, attacks, and exploitations.

''(2) Not later than 30 days after receiving an operational evaluation under this subsection, the Director shall ensure agencies evaluated under paragraph (1) develop a plan for addressing recommendations and mitigating vulnerabilities contained in the security reports identified under paragraph (1), including a timeline and budget for implementing such plan.

''(e) Not later than March 1 of each year, the Director shall submit a report to Congress on the overall infor-

mation security posture of the communications and information infrastructure of the United States, including—

''(1) the evaluations conducted under subsection (d) for the United States Government;

''(2) a detailed assessment of the overall resiliency of the communications and information infrastructure effectiveness of the United States and the United States Government including the ability to monitor, detect, mitigate, and respond to an incident;

''(3) a detailed assessment the information security effectiveness of each agency, including the ability to monitor, detect, mitigate, collaborate, and respond to an incident;

''(4) a detailed assessment of operational evaluations performed during the preceding fiscal year, the results of such evaluations, and any actions that remain to be taken under plans included in corrective action reports under subsection (d);

''(5) a detailed assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and promulgated under section 3554, and recommendations for enhancement;

''(6) a detailed assessment of significant deficiencies in the information security and reporting practices of the Federal Government as applicable to each agency;

''(7) planned remedial action to address deficiencies described under paragraph (6), including an associated budget and recommendations for relevant executive and legislative branch actions;

''(8) a summary of the results of the independent evaluations under section 3555; and

''(9) a detailed assessment of the effectiveness of reporting to the National Cyber Investigative Joint Task Force under section 3554.

''(f) Evaluations and any other descriptions of information systems under the authority and control of the Director of National Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

''(g)(1) In collaboration with the private sector and in coordination with the Director of the Office of Management and Budget, the National Institute of Standards and Technology, and the General Service Administration, the Director shall develop and implement policy, guidance,

and regulations that cost effectively enhance the security of the Federal Government, including policy, guidance, and regulations that—

"(A) to the extent practicable, standardize security requirements (also known as 'lock-down configurations') of commercial off-the-shelf products and services (including cloud products and services) purchased by the Federal Government;

"(B) to the extent practicable, obtain products and services with security configuration baselines consistent with available security standards and configurations and guidelines developed by the National Institute of Standards and Technology;

"(C) incentivize agencies to purchase standard products and services through the General Service Administration in order to reduce the vulnerabilities and costs associated with custom products and services; and

"(D) enable purchasing decisions to reasonably and appropriately account for significant supply chain security risks associated with any particular product or service.

''(2) Not later than 180 days after the date of enactment of the United States Information and Communications Enhancement Act of 2009, and annually thereafter, the Director shall submit a report to Congress that includes—

''(A) a description of the cost savings and security enhancements that can be achieved by using the purchasing power of the Federal Government; and

''(B) recommendations for legislative or executive branch actions necessary to achieve such cost savings.

''§ 3554. Agency responsibilities

''(a) The head of each agency shall—

''(1) be responsible for—

''(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of the agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

''(i) information security standards promulgated under section 3556;

''(ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

''(iii) ensuring the standards implemented for information systems and national security systems under the agency head are complementary and uniform, to the extent practicable; and

''(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

''(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modi-

fication, or destruction of such information or information systems;

''(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 3556, for information security classifications and related requirements;

''(C) implementing policies and procedures to cost effectively reduce risks to an acceptable level; and

''(D) continuously testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

''(3) delegate to an agency official designated as the Chief Information Security Officer the authority to ensure and enforce compliance with the requirements imposed on the agency under this subchapter, including—

''(A) overseeing the establishment and maintenance of a security operations capability that on an automated and continuous basis can—

''(i) detect, report, respond to, contain, and mitigate incidents that impair

adequate security of the information and information infrastructure, in accordance with policy provided by the Director, in consultation with the Chief Information Officers Council, and guidance from the National Institute of Standards and Technology;

''(ii) collaborate with the National Office for Cyberspace and appropriate public and private sector security operations centers to address incidents that impact the security of information and information infrastructure that extend beyond the control of the agency; and

''(iii) not later than 24 hours after discovery of any incident described under subparagraph (A), unless otherwise directed by policy of the National Office for Cyberspace, provide notice to the appropriate security operations center, the National Cyber Investigative Joint Task Force, and inspector general;

''(B) collaborating with the Administrator for E-Government and the Chief Information Officer to establish, maintain, and update an

enterprise network, system, storage, and security architecture framework documentation to be submitted quarterly to the National Office for Cyberspace and the appropriate security operations center, that includes—

''(i) documentation of how technical, managerial, and operational security controls are implemented throughout the agency's information infrastructure; and

''(ii) documentation of how the controls described under subparagraph (A) maintain the appropriate level of confidentiality, integrity, and availability of information and information systems based on—

''(I) the policy of the Director;

''(II) the National Institute of Standards and Technology guidance; and

''(III) the Chief Information Officers Council recommended approaches;

''(C) developing, maintaining, and overseeing an agency wide information security program as required by subsection (b);

''(D) developing, maintaining, and overseeing information security policies, procedures, and control techniques to address all applicable requirements, including those issued under sections 3553 and 3556;

''(E) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

''(F) assisting senior agency officials concerning their responsibilities under paragraph (2);

''(4) ensure that the agency has trained and cleared personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines;

''(5) ensure that the agency Chief Information Security Officer, in coordination with other senior agency officials, reports biannually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions; and

''(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; and has information security duties as the primary duty of that official.

''(b) Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3553(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

''(1) periodic assessments—

''(A) of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency; and

''(B) that recommend a prioritized description of which data and applications should be removed or migrated to more secure networks or standards;

''(2) penetration tests commensurate with risk (as defined by the National Institute of Standards

and Technology and the National Office for Cyberspace) for agency information systems;

''(3) information security vulnerabilities are mitigated based on the risk posed to the agency;

''(4) policies and procedures that—

''(A) are based on the risk assessments required by paragraph (1);

''(B) cost effectively reduce information security risks to an acceptable level;

''(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

''(D) ensure compliance with—

''(i) the requirements of this subchapter;

''(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 3556;

''(iii) minimally acceptable system configuration requirements, as determined by the Director; and

''(iv) any other applicable requirements, including standards and guidelines for national security systems issued in ac-

cordance with law and as directed by the President;

''(5) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

''(6) role-based security awareness training to inform personnel with access to the agency network, including contractors and other users of information systems that support the operations and assets of the agency, of—

''(A) information security risks associated with their activities; and

''(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

''(7) to the extent practicable, automated and continuous technical monitoring for testing, and evaluation of the effectiveness and compliance of information security policies, procedures, and practices, including—

''(A) management, operational, and technical controls of every information system identified in the inventory required under section 3505(b); and

"(B) management, operational, and technical controls relied on for an evaluation under section 3555;

"(8) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

"(9) to the extent practicable, continuous technical monitoring for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued by the Director, including—

"(A) mitigating risks associated with such incidents before substantial damage is done;

"(B) notifying and consulting with the appropriate security operations response center; and

"(C) notifying and consulting with, as appropriate—

"(i) law enforcement agencies and relevant Offices of Inspectors General;

"(ii) the National Office for Cyberspace; and

''(iii) any other agency or office, in accordance with law or as directed by the President; and

''(10) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

''(c) Each agency shall—

''(1) submit an annual report on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b) to—

''(A) the National Office for Cyberspace;

''(B) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(C) the Committee on Commerce, Science, and Transportation of the Senate;

''(D) the Committee on Government Oversight and Reform of the House of Representatives;

''(E) the Committee on Homeland Security of the House of Representatives;

''(F) other appropriate authorization and appropriations committees of Congress; and

''(G) the Comptroller General.

''(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

''(A) annual agency budgets;

''(B) information resources management of this subchapter;

''(C) information technology management under this chapter;

''(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

''(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);

''(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note);

''(G) internal accounting and administrative controls under section 3512 of title 31; and

''(H) performance ratings, salaries, and bonuses provided to the Chief Information Security Officer and supporting personnel taking into account program performance; and

''(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)—

''(A) as a material weakness in reporting under section 3512 of title 31; and

''(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

''(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the National Office for Cyberspace, shall include as part of the performance plan required under section 1115 of title 31 a description of—

''(A) the time periods; and

''(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

''(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1) and operational evaluations required under section 3553(d).

''(e) Each agency shall provide the public with timely notice and opportunities for comment on proposed infor-

mation security policies and procedures to the extent that such policies and procedures affect communication with the public.

"§ 3555. Annual independent evaluation

''(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

''(2) Each evaluation under this section shall consist of—

''(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the information systems of the agency; and

''(B) an assessment (made on the basis of the results of the testing) of compliance with—

''(i) the requirements of this subchapter; and

''(ii) related information security policies, procedures, standards, and guidelines.

''(b)(1) For each agency with an Inspector General appointed under the Inspector General Act of 1978 (5 U.S.C. App.) or any other law, the annual evaluation required by this section shall be performed by the Inspector

General or by an independent external auditor, as determined by the Inspector General of the agency.

''(2) For each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

''(c) The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

''(d) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

''(e) Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

''(f) The Comptroller General shall—

''(1) not later than 180 days after the date of enactment of the United States Communications and Information Enhancement Act of 2009 and after collaboration with the Director and the Inspectors General, develop and deliver standards for independent evaluations as required under this section that are risk-based and cost effective;

''(2) periodically evaluate and report to Congress on—

''(A) the adequacy and effectiveness of agency information security policies and practices; and

''(B) the implementation of the requirements of this subchapter.

''§ 3556. Responsibilities for Federal information systems standards

''(a)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), prescribe standards and guidelines pertaining to information systems, including national security systems.

''(2)(A) Standards prescribed under subsection (a)(1) shall include information security standards that—

''(i) to the extent practicable, are unified with standards and guidelines developed for information systems and national security systems to ensure the adequacy and effectiveness of information security and information sharing;

''(ii) provide minimum information security requirements as determined under section 20(b) of the

National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(iii) are otherwise necessary to improve the security of information and information systems, including information stored by third parties on behalf of the Federal Government.

''(B) Information security standards described in subparagraph (A) shall be compulsory and binding.

''(b) The President may disapprove or modify the standards and guidelines referred to in subsection (a)(1) if the President determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

''(c) To ensure fiscal and policy consistency, the Secretary shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director of the Office of Management and Budget and the National Office for Cyberspace.

''(d) The National Office for Cyberspace and the head of an agency may employ standards for the cost ef-

fective information security for information systems within or under the supervision of that agency that are more stringent than the standards the Secretary prescribes under this section if the more stringent standards—

''(1) contain at least the applicable standards made compulsory and binding by the Secretary; and

''(2) are otherwise consistent with policies and guidelines issued under section 3553.

''(e) The decision by the Secretary regarding the promulgation of any standard under this section shall occur not later than 6 months after the submission of the proposed standard to the Secretary by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).''.

SEC. 4. AUTHORITY AND RESPONSIBILITY OF THE UNITED STATES COMPUTER EMERGENCY READINESS TEAM IN RELATION TO FEDERAL AGENCIES.

(a) DEFINITION.—In this section:

(1) The term ''agency'' has the meaning given under section 3502(1) of title 44, United States Code.

(2) The term ''US–CERT'' means the United States Computer Emergency Readiness Team.

(b) PURPOSES.—The purposes of this section are to recognize that US–CERT—

(1) is charged with providing response support and defense against cyber attacks for agencies and information sharing and collaboration with State and local government, industry, and international partners;

(2) interacts with agencies, industry, the research community, State and local governments, and others to disseminate reasoned and actionable cyber security information to the public;

(3) provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the United States Government about cyber security; and

(4) has continually enhanced its ability to monitor, detect, and respond to information security incidents that affect the Federal Government.

(c) COORDINATION WITH US–CERT.—The head of each agency shall ensure that the Chief Information Officer, Chief Information Security Officer, and security operations centers under the direction of that agency head shall establish policies, procedures, and guidance to effectively coordinate with the Director of US–CERT in a timely fashion to detect, report, respond to, contain, and

mitigate incidents that impair adequate security of the information and information infrastructure.

(d) REVIEW AND APPROVAL.—In coordination with the Administrator for Electronic Government and Information Technology, the Director of the National Office for Cyberspace shall review and approve the policies, procedures, and guidance established in subparagraph (c) to ensure that US–CERT has the capability to effectively and efficiently detect, correlate, respond to, contain, and mitigate incidents that impair the adequate security of the information and information infrastructure of more than 1 agency. To the extent practicable, the capability shall be continuous and technically automated.

(e) SECURITY CLEARANCES; EXPERTS AND CONSULTANTS.—Notwithstanding any provision of law, regulation, rule, or policy to the contrary, the Director of US–CERT may—

(1) direct the sponsorship of the security clearances for Federal officers and employees (including experts and consultants employed under section 3109) whose responsibilities involve critical infrastructure in the interest of national security; and

(2) employ experts and consultants under section 3109 for cyber security-related work.

SEC. 5. AUTHORITY AND RESPONSIBILITY OF DEPARTMENTS NOT RELATED TO MILITARY FUNCTIONS.

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency''—

(A) means—

(i) an Executive department defined under section 101 of title 5, United States Code; and

(ii) an Executive agency that has multiple components which have separate and distinct enterprise architectures; and

(B) shall not include—

(i) the Department of Defense; or

(ii) any component of an Executive agency that is performing any national security function, including military intelligence.

(2) EXECUTIVE AGENCY.—The term ''Executive agency'' has the meaning given under section 105 of title 5, United States Code.

(b) PURPOSE.—The purpose of this section is to recognize that—

(1) agencies have developed and maintained separate and distinct enterprise architectures that inhibit the ability of an agency to ensure that com-

ponents of that agency have effectively implemented security policies, procedures, and practices;

(2) the separate and distinct enterprise architectures have in many instances been at the detriment of securing the agency information infrastructure (the civilian cyberspace) and exposed that infrastructure to unnecessary risk for an extended period of time; and

(3) a more uniform agency enterprise architecture will be more efficient and effective for the purposes of information sharing and ensuring the appropriate confidentiality, integrity, and availability of information and information systems.

(c) AGENCY COORDINATION.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the head of each agency shall ensure that components of that agency shall establish an automated reporting mechanism that allows the Chief Information Security Officer and security operations center at the total agency level to implement and monitor the implementation of appropriate security policies, procedures, and controls of agency components.

(2) APPROVAL AND COORDINATION.—The activities conducted under paragraph (1) shall be—

(A) approved by the Director of the National Office for Cyberspace; and

(B) to the extent practicable, in coordination and complementary with activities—

(i) described under section 4; and

(ii) conducted by the Administrator for E-Government and Information Technology.

SEC. 6. TECHNICAL AND CONFORMING AMENDMENTS.

(a) TABLE OF SECTIONS.—The table of sections for chapter 35 of title 44, United States Code, is amended by striking the matter relating to subchapters II and III and inserting the following:

"SUBCHAPTER II—INFORMATION SECURITY

"Sec. 3551. Definitions.
"Sec. 3552. National Office for Cyberspace.
"Sec. 3553. Authority and functions of the National Office for Cyberspace.
"Sec. 3554. Agency responsibilities.
"Sec. 3555. Annual independent evaluation.
"Sec. 3556. Responsibilities for Federal information systems standards.".

(b) OTHER REFERENCES.—

(1) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(c)(1)(A)) is amended by striking "section 3532(3)" and inserting "section 3551(b)".

(2) Section 2222(j)(6) of title 10, United States Code, is amended by striking "section 3542(b)(2))" and inserting "section 3551(b)".

(3) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2))'' and inserting ''section 3551(b)''.

(4) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2))'' and inserting ''section 3551(b)''.

(5) Section 20(a)(2) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by striking ''section 3532(b)(2)'' and inserting ''section 3551(b)''.

(6) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)''.

SEC. 7. EFFECTIVE DATE.

This Act (including the amendments made by this Act) shall take effect 30 days after the date of enactment of this Act.

○