Legislative Language

SEC. 1. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—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. Purposes**

‘‘ The purposes of this subchapter are to—

‘‘ (1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

‘‘ (2) recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

‘‘ (3) provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture; and

‘‘ (4) provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

‘‘ **§ 3552. Definitions**

‘‘ (a) Except as provided under subsection (b), the definitions under section 3502 of this title (including for “agency” and “information system”) shall apply to this subchapter.

‘‘ (b) In this subchapter—

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

‘‘ (2) The term “Director” means the Director of the Office of Management and Budget unless otherwise specified.

‘‘ (3) The term ‘incident’ means an occurrence that—

‘‘ (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

“ (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

‘‘ (4) 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 proof of origin of data 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 by authorized persons, processes, or devices.

‘‘ (5) The term ‘information technology’ has the meaning given that term in section 11101 of title 40, United States Code.

‘‘ (6) 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—

‘‘ (A) 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 (C), is critical to the direct fulfillment of military or intelligence missions; or

‘‘ (B) 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.

‘‘ (C) Subparagraph (A)(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).

‘‘ (7) The term “Secretary” means the Secretary of Homeland Security unless otherwise specified.

‘‘ **§ 3553. Federal information security authority and coordination.—**

‘‘ (a) IN GENERAL—The Secretary shall exercise primary responsibility within the executive branch for information security, including implementation of information security policies and directives and compliance with the requirements of this subchapter, except as provided in subsections (d) and (e).

‘‘ (b) The Secretary shall—

“ (1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

‘‘ (A) policies and directives consistent with the standards promulgated under section 11331 of title 40, United States Code, to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

‘‘ (i) information collected or maintained by or on behalf of an agency; or

‘‘ (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) minimum operational requirements for Federal Government network operations centers and security operations centers to protect agency information systems and provide common situational awareness across all agency information systems;

‘‘ (C) reporting requirements, consistent with relevant law, regarding information security incidents;

‘‘ (D) requirements for agency-wide information security programs;

‘‘ (E) performance requirements and metrics for the security of agency information systems;

‘‘ (F) training requirements to ensure that agencies are able to fully and timely comply with direction issued by the Secretary under this subchapter;

‘‘ (G) training requirements regarding privacy, civil rights and civil liberties, and information oversight for agency information security personnel;

‘‘ (H) requirements for the annual reports to the Secretary under section 3554(c); and,

" (I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads.

'' (2) review agency information security programs required under section 3554(b);

" (3) designate an entity to receive reports and information about information security incidents, threats, and vulnerabilities affecting agency information systems.

'' (c) When issuing policies and directives under subsection (b), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology (NIST) and issued by the Secretary of Commerce under section 11331 of title 40, United States Code. The Secretary shall consult with the Director of the NIST when such policies and directives implement standards or guidelines developed by NIST.

'' (d) The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

'' (e) The authorities and responsibilities of the Secretary under paragraphs (1) and (2) of subsection (b) shall be carried out by the Secretary of Defense for non-national security systems under the control of the Department of Defense.

" (f) Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any Head of a federal agency over such agency.

'' **§ 3554. Agency responsibilities**

'' (a) The head of each agency shall—

'' (1) be responsible for—

" (A) complying with the policies and directives issued under section 3553.

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

'' (i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an 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;

‘‘ (C) complying with the requirements of this subchapter, including—

‘‘ (i) information security standards promulgated under section 11331 of title 40, United States Code;

“ (ii) information security policies, directives, standards and guidelines for national security systems issued as directed by the President; and

“ (iii) information security policies and directives for non-national security systems issued under section 3553(b);

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

“ (E) reporting and sharing, for those agencies operating or exercising control of a national security system, information about information security incidents, threats, and vulnerabilities to the entity designated by the Secretary under section 3553(b)(3) and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

‘‘ (F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, threats, and vulnerabilities to the entity designated by the Secretary of Homeland Security under section 3553(b)(3) and to other appropriate entities to the extent consistent with policies and directives for non-national security systems as prescribed under section 3553(b);

‘‘ (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 impact that could result from the unauthorized access, use, disclosure, disruption, modification, 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 policies and directives issued under section 3553(b) and standards promulgated under section 11331 of title 40, United States Code, for information security classifications and related requirements;

‘‘ (C) implementing policies, procedures, and capabilities to cost-effectively reduce risks to an acceptable level;

‘‘ (D) actively monitoring the effective implementation of information security controls and techniques; and

‘‘ (E) reporting information about information security incidents, threats, and vulnerabilities in a timely manner to the entity designated under section 3553(b)(3) in accordance with paragraph (1);

‘‘ (3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

‘‘ (4) designate the agency Inspector General (or, if the agency does not have an Inspector General, an independent entity selected in consultation with the Secretary) to conduct the annual independent evaluation required under section 3556; provided however, that the agency Inspector General may contract with an independent entity to perform such evaluation;

‘‘ (5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent) the authority and primary responsibility to implement an agency-wide information security program to be reviewed under section 3553(b)(2) and to provide information security for the information collected and maintained by the agency or by another agency, contractor, or other source on behalf of the agency and information systems that support the operations, assets, and mission of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

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

‘‘ (i) detect, report, respond to, contain, and mitigate information security incidents that impair adequate security of the agency’s information and information system, in a timely manner and in accordance with policies and directives issued under section 3553(b); and

‘‘ (ii) report any information security incident described under clause (i) to the entity designated under section 3553(b)(3) in accordance with applicable policies and directives;

‘‘ (B) developing, maintaining, and overseeing an agency-wide information security program as required in subsection (b);

‘‘ (C) developing, maintaining, and overseeing information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 and section 11331 of title 40, United States Code;

‘‘ (D) training and overseeing agency personnel with significant responsibilities for information security with respect to such responsibilities; and

‘‘ (E) assisting the Chief Information Officer or senior agency official concerning their responsibilities under paragraph (2);

‘‘ (6) delegate to appropriate agency officials who are responsible for particular agency systems or subsystems the responsibility to ensure and enforce compliance with all requirements of the agency’s information security program as outlined in paragraph (5) above in coordination with the senior agency official designated under that paragraph;

‘‘ (7) ensure that the agency has trained personnel who have obtained security clearances that will permit them to assist the agency in complying with the requirements of this subchapter and policies and directives issued under section 3553(b);

‘‘ (8) ensure that the Chief Information Officer or senior agency official designated under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agency information security program, including the progress of remedial actions; and

‘‘ (9) ensure that the senior agency official designated under paragraph (5) possesses the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

‘‘ (b) The agency-wide information security programs described in subsection (a)(5) shall include—

‘‘ (1) the development and maintenance of a risk management strategy for information security that considers information security threats, vulnerabilities and consequences 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, including those provided or managed by another agency, contractor, or other source;

‘‘ (2) security testing commensurate with risk and impact;

‘‘ (3) mitigation of information security vulnerabilities commensurate with risk and impact;

‘‘ (4) policies and procedures that—

‘‘ (A) are based on the risk management strategy required by paragraph (1);

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

‘‘ (C) ensure that cost-effective and adequate 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) information security policies and directives issued under section 3553(b); and

‘‘ (iii) any other applicable requirements;

‘‘ (5) information security, privacy, civil rights, civil liberties, and information oversight training that meets requirements issued in accordance with section 3553(b) to inform information security personnel with access to agency information systems, 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) individual responsibilities in complying with agency policies and procedures designed to reduce those risks;

‘‘ (6) risk-based continuous monitoring of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of management, operational, and technical controls of information systems identified in the inventory required under section 3505(c);

‘‘ (7) a process for ensuring that remedial actions have been taken to address any deficiencies in the information security policies, procedures, and practices of the agency;

‘‘ (8) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, consistent with policies and directives issued under section 3553(b), including—

‘‘ (A) mitigating risks associated with such information security incidents;

‘‘ (B) notifying and consulting with the entity designated under section 3553(b)(3); and

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

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

‘‘ (ii) any other entity, in accordance with law and as directed by the President; and

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

‘‘ (c) Each agency shall annually submit a report on its information security program and information systems to the Secretary in accordance with applicable policies and directives issued pursuant to section 3553(b).

‘‘ **§ 3555. Periodic assessments**

‘‘ (a) Except as provided in subsection (b), the Secretary shall prepare, based on the annual agency reports required under section 3554(c), annual independent evaluations under section 3556, the results of any continuous monitoring, and other available information, periodic summaries of agency security programs and practices. Such summaries may—

‘‘ (1) assess the effectiveness of agency information security policies, procedures, and practices;

‘‘ (2) provide an overall assessment of federal government-wide agency information system security posture; and

‘‘ (3) include recommendations for improving agency specific and federal government-wide agency information system security;

‘‘ (b)(1) Periodic summaries described in subsection (a) relating to national security systems shall be prepared as directed by the President.

‘‘ (2) Periodic summaries described in subsection (a) relating to agency information systems under the control of the Department of Defense shall be prepared by the Secretary of Defense in accordance with government wide reporting requirements.

‘‘ (c) In conducting assessments under this section, the Secretary shall take appropriate actions 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 policies.

‘‘ (d) The Secretary, in coordination with the Secretary of Defense, shall evaluate and report to Congress annually on the adequacy and effectiveness of the information security programs and practices summarized under this section.

‘‘ § 3556. Independent Evaluations

‘‘ (a) The Council of Inspectors General on Integrity and Efficiency, in consultation with the Director and Secretary, shall issue and maintain criteria for timely, cost-effective, risk-based, and independent evaluations of agency information security programs and practices to determine the effectiveness of such information security programs and practices. Such criteria shall include measures to assess whether agency information security programs include appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

‘‘ (b) Agencies shall perform an annual independent evaluation of agency information security programs and practices in accordance with the criteria developed under paragraph (a), to determine the effectiveness of such programs and practices.

‘‘ (c) Reports prepared under this section shall be provided to the Secretary upon delivery of the report by the agency head.

‘‘ (d) Evaluations involving national security systems shall be conducted as directed by President.

‘‘ § 3557. Savings Provisions and Technical and Conforming Amendments

‘‘ (a) SAVINGS PROVISIONS.—

‘‘ (1) Policy and compliance guidance issued by the Director prior to the effective date of this Act pursuant to section 3543(a)(1) of title 44, United States Code, (as in effect prior to the effective date) shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(b)(1).

‘‘ (2) Standards and guidelines issued by the Secretary of Commerce or by the Director of the Office of Management and Budget prior to the effective date of this Act pursuant to section 11331(a)(1) of title 40 (as in effect prior to the effective date) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1), as added by this Act.

‘‘ (b) TECHNICAL AND CONFORMING AMENDMENTS.—

‘‘ (1) 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

‘‘ 3551. Purposes.

‘‘ 3552. Definitions.

‘‘ 3553. Federal information security authority and coordination.

‘‘ 3554. Agency responsibilities.

‘‘ 3555. Periodic assessments.

‘‘ 3556. Independent Evaluations.

“ 3557. Savings Provisions and Technical and Conforming Amendments.

“ (2) OTHER REFERENCES.—

“ (A) 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)’’.

“ (B) Section 2222(j)(6) of title 10 is amended by striking ‘‘section 3542(b)(2))’’ and inserting ‘‘section 3551(b)’’.

“ (C) Section 2223(c)(3) of title 10 is amended, by striking ‘‘section 3542(b)(2))’’ and inserting ‘‘section 3551(b)’’.

“ (D) Section 2315 of title 10 is amended by striking ‘‘section 3542(b)(2))’’ and inserting ‘‘section 3551(b)’’.

“ (E) 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)’’.

" (F) 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. 2. MANAGEMENT OF INFORMATION TECHNOLOGY. —

'' (a) IN GENERAL.— Section 11331 of title 40, United States Code, is amended by striking the section and inserting the following:

'' **§ 11331 Responsibilities for federal information systems standards.**

'' (a) STANDARDS AND GUIDELINES.—

'' (1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall, in consultation with the Secretary of Homeland Security, on the basis of standards and guidelines developed by the National Institute of Standards and Technology pursuant to 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 Federal information systems.

'' (2) NATIONAL SECURITY SYSTEMS. —Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as directed by the President.

'' (b) MANDATORY REQUIREMENTS.—

'' (1) AUTHORITY TO MAKE MANDATORY.—The Secretary of Commerce shall make standards prescribed under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

'' (2) REQUIRED MANDATORY STANDARDS.—

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

'' (i) 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

'' (ii) are otherwise necessary to improve the security of Federal information and information systems.

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

'' (c) AUTHORITY TO DISAPPROVE OR MODIFY. —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 be delegated to the Director of the Office of Management and Budget. 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 or the Director of the Office of Management and Budget.

‘‘ (d) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce 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.

‘‘ (e) APPLICATION OF MORE STRINGENT STANDARDS. —The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards the Secretary of Commerce prescribes under this section if the more stringent standards—

> ‘‘ (1) contain at least the applicable standards made compulsory and binding by the Secretary of Commerce; and
>
> ‘‘ (2) are otherwise consistent with directives and implementation memoranda issued under section 3553(b) of title 44, United States Code.

‘‘ (f) DECISIONS ON PROMULGATION OF STANDARDS. —The decision by the Secretary of Commerce 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 of Commerce by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (section 278g-3 of title 15, United States Code).

‘‘ (g) DEFINITIONS. —In this section—

> ‘‘ (1) FEDERAL INFORMATION SYSTEM. —The term “Federal information system” means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
>
> ‘‘ (2) INFORMATION SECURITY. —The term “information security” has the meaning given that term in section 3552 of title 44, United States Code.
>
> ‘‘ (3) NATIONAL SECURITY SYSTEM. —The term “national security system” has the meaning given that term in section 3552 of title 44, United States Code.

“ (b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 21of the National Institute of Standards and Technology Act (section 278g–4 of title 15, United States Code) is amended as follows:

“ (1) Section 21(b)(2) of the National Institute of Standards and Technology Act (section 278g–4 of title 15, United States Code) is amended after ‘‘the Institute’’ by inserting ‘‘Secretary of Homeland Security’’.

“ (2) Section 21(b)(3) of the National Institute of Standards and Technology Act (section 278g–4 of title 15, United States Code) is amended after ‘‘the Secretary of Commerce’’ by inserting ‘‘Secretary of Homeland Security’’.