TITLE XX: [FISMA REFORM]

(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 to improve and continuously monitor the security of agency information security programs and systems through a focus on continuous monitoring of agency information systems and streamlined reporting requirements rather than over 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 '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.

"(3) 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 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.

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

"(5) 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).

"(6) The term "Secretary" means the Secretary of Homeland Security unless otherwise specified.

"§ 3553. Federal information security authority and coordination

"(a) IN GENERAL--The Secretary of Homeland Security shall exercise primary responsibility within the executive branch for information security, including development and oversight 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 of Homeland Security 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 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, including information security continuous monitoring;

"(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) develop and conduct risk assessments for federal information and information systems in consultation with the heads of other agencies or governmental and private entities that own and operate such systems, that may include threat, vulnerability, and impact assessments and penetration testing;

" (4) operate consolidated intrusion detection, prevention, or other protective capabilities and the use of associated countermeasures for the purpose of protecting federal information and information systems from cybersecurity threats;

‘‘ (5) assess and foster the development, in conjunction with other governmental entities and the private sector, of essential information security technologies and capabilities for protecting federal information systems, including comprehensive protective capabilities and other technological solutions;

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

"(7) coordinate with appropriate agencies and officials to ensure, to the maximum extent feasible, that standards and guidelines developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) are complementary with

" (A) policies and directives issued under paragraph (b), and

"(B) standards and guidelines developed for national security systems.

"(c) REQUIRED SECURITY ACTION--(1) In response to a known or reasonably suspected cybersecurity threat or incident, the Secretary may direct officials of agencies that own, operate, lease, or otherwise control an information system, including information systems used or operated by another

entity, including contractors, on behalf of a Federal agency, to take any lawful action with respect to the operation of such information system for the purpose of protecting that information system from or mitigating a cybersecurity threat.

"(1) The authorities of the Secretary under this subsection shall not apply to the systems described in paragraphs (2), (3), and (4) of subsection (e).

"(2) The Secretary shall—

"(A) establish, in coordination with the Director of the Office of Management and Budget, procedures governing the circumstances under which such directive may be issued under this section, including—

"(i) thresholds and other criteria;

"(ii) privacy and civil liberties protections; and

"(iii) notice to potentially affected third parties as may be applicable;

"(B) specify the reasons for the required action and the duration of such directive;

"(C) minimize the impact of directives under this section by adopting the least intrusive means possible to secure the federal system or systems under the particular circumstances for the shortest time practicable; and

"(D) notify the Director of the Office of Management and Budget and head of any affected agency immediately upon the issuance of directives under this section.

"(3) When the Secretary determines that there is an imminent threat to federal information systems and a directive under subsections (1) and (2) is not reasonably likely to result in a timely response to the threat, the Secretary may authorize use of protective capabilities under the Secretary's control on communications or other system traffic transiting to or from or stored on a federal information system without prior consultation with the affected agency for the purpose of ensuring the security of that information system or other federal information systems, provided that—

"(A) the authorities under this subsection are not delegated below the level of Assistant Secretary;

"(B) the Secretary or the Secretary's designee immediately notifies the Director of the Office of Management and Budget, head of the affected agencies, and associated Chief Information Officers of any action taken under this subsection as to the reasons, duration, and nature of the action; and

"(C) the Secretary's actions are otherwise consistent with applicable law.

"(d) The authorities of the Secretary of Homeland Security 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) Department of Defense, Central Intelligence Agency, and Office of the Director of National Intelligence Systems.—

(1) The authorities of the Secretary described in paragraphs (1), (2), (3) and (4) of subsection (b) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2), to the Director of Central Intelligence in the case of systems described in paragraph (3), and to the Director of National Intelligence in the case of systems described in paragraph (4).

(2) The systems described in this paragraph are non-national security systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

(3) The systems described in this paragraph are non-national security systems that are operated by the Central Intelligence Agency, a contractor of the Central Intelligence Agency, or another entity on behalf of the Central Intelligence Agency that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Central Intelligence Agency.

(4) The systems described in this paragraph are non-national security systems that are operated by the Office of the Director of National Intelligence, a contractor of the Office of the Director of National Intelligence, or another entity on behalf of the Office of the Director of National Intelligence that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Office of the Director of National Intelligence.

(5) Integration of Information. – The Secretary of Defense, the Director of the Central Intelligence Agency, and the Director of National Intelligence shall share timely and relevant information with the Secretary of Homeland Security relevant to the security of the Information Infrastructure for purposes of comprehensive situational awareness.

“§ 3554. Agency responsibilities

“(a) AGENGY HEAD. The head of each agency shall--

“(1) be responsible for--

“(A) 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;

“(B) complying with the requirements of this subchapter, including--

“(i) policies and directives issued under section 3553;

“(ii) information security standards promulgated under section 11331 of title 40;

“(iii) information security policies, directives, standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

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

"(D) 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

"(E) 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) of this title and standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

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

"(D) continuously 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) delegate 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 for ensuring compliance with the requirements imposed on the agency under this subchapter, including --

"(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)(6) 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;

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

"(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

"(5) 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 (4) above in coordination with the senior agency official designated under that paragraph;

"(6) ensure that the agency has trained and cleared personnel sufficient to assist the agency in complying with the requirements of this subchapter and policies and directives issued under section 3553(b);

"(7) ensure that the Chief Information Officer (or other senior agency official designated under paragraph (4)), 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

"(8) ensure that the Chief Information Officer (or other senior agency official designated under paragraph (4)), 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) AGENCY PROGRAM.— Each agency shall develop, document, and implement an agencywide information security program, to be reviewed under section 3553(b)(2), 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) the development, execution, and maintenance of a risk management strategy for information security that

"(A) 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, and

"(B) includes periodic assessments of the risk to information and information systems supporting agency operations and assets;

"(2) policies and procedures that--

"(A) are based on the risk management strategy and assessment results 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;

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

"(4) security awareness training in accordance with requirements issued under section 3553(b) to inform personnel with access to agency information systems, including information security personnel, 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;

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

"(C) requirements for fulfilling privacy, civil rights, civil liberties and other information oversight responsibilities;

"(5) security testing and evaluation commensurate with risk and impact that includes

"(A) 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),

"(B) penetration testing exercises in accordance with requirements issued under section 3553(b) to evaluate whether the agency adequately protects against, detects, and responds to incidents,

"(C) vulnerability scanning, intrusion detection and prevention, and penetration testing, in accordance with requirements issued under section 3553(b), and

"(D) Any other periodic testing and evaluation, in accordance with requirements issued under section 3553(b)

"(6) a process for ensuring that remedial actions are taken to mitigate information security vulnerabilities commensurate with risk and impact, and otherwise address any deficiencies in the information security policies, procedures, and practices of the agency;

"(7) 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

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

"(c) AGENCY REPORTING. Each agency shall

"(1) report annually to the Secretary on the adequacy and effectiveness of information security policies, procedures, and practices, including—

"(A) Compliance with the requirements of this subchapter;

"(B) A conclusion as to the effectiveness of the agency's information security policies, procedures, and practices based on a determination of the aggregate effect of identified deficiencies;

"(C) An identification and analysis of, including actions and plans to address, any significant deficiencies identified in such policies, procedures and practices; and

"(D) Reporting requirements issued pursuant to section 3553 (b);

"(2) make the report required under paragraph (1) available to the appropriate authorization and appropriations committees of Congress, and the Comptroller General;

"(3) otherwise address the adequacy and effectiveness of information security policies, procedures, and practices in management and budget plans and reports, as appropriate.

"§ 3555. Periodic assessments

"(a) Except as provided in paragraph (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 assessments of agency security programs and practices. Such assessments shall--

"(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;

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

"(4) for each agency-specific assessment, be made available to the head of the agency being assessed.

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

"(2) Periodic assessments described in (a) shall be prepared in accordance with government wide reporting requirements by

"(A) the Secretary of Defense for agency information systems under the control of the Department of Defense ,

"(B) the Director of the Central Intelligence Agency for agency information systems under the control of the Central Intelligence Agency, and

"(C) the Director of National Intelligence for agency information systems under the control of the Office of the Director of National Intelligence.

"(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 of Homeland Security, in coordination with the Secretary of Defense, the Director of the Central Intelligence Agency, and the Director of National Intelligence, shall evaluate and report to Congress annually on the adequacy and effectiveness of the information security programs and practices assessed under this section.

"§ 3556. Independent Evaluations

"(a) Not less than every two years, each agency shall have performed an independent evaluation of the information security program and practices of that agency in accordance with the criteria developed under paragraph (a) to determine the effectiveness of such program and practices.

"(b) Each evaluation under this section shall include—

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

"(2) an assessment of compliance with the requirements of this subchapter and any significant deficiencies; and

"(3) a conclusion as to the effectiveness of the agency's information security policies, procedures, and practices based on a determination of the aggregate effect of identified deficiencies; and

"(c) Subject to subsection (d), evaluations under this section shall be performed by the agency Inspector General (or, if the agency does not have an Inspector General, an independent entity selected in consultation with the Secretary); provided that the agency Inspector General may contract with an independent entity to perform such evaluation;

"(d) The Council of Inspectors General on Integrity and Efficiency, in consultation with the Director of Office of Management and Budget and Secretary, shall issue and maintain guidance for timely, cost-effective, and risk-based evaluations under this section.

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

"(f) Evaluations involving national security systems shall be conducted as directed by President.

"(g) Comptroller General.--The Comptroller General shall periodically evaluate and report to Congress on—

"(1) the adequacy and effectiveness of agency information security policies and practices; and

"(2) implementation of the requirements of this subchapter.

“§ 3557. United States Computer Emergency Readiness Team

‘‘The Secretary shall designate and maintain a center to serve as a focal point within the federal government for cybersecurity with responsibilities that include the protection of the information and information systems under the purview of the Secretary, as described in Section 3553, and the coordination of cyber incident response and that will—

‘‘(a) facilitate information sharing, interactions and collaborations among and between agencies; State, local, tribal and territorial governments; the private sector; academia and international partners;

‘‘(b) work with appropriate agencies; State, local, tribal and territorial governments; the private sector; academia; and international partners, to prevent and respond to cybersecurity threats and incidents;

‘‘(c) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security of federal and private sector information and information systems;

‘‘(d) integrate information from federal government and non-federal network operation centers and security operations centers to

> “(1) maintain dynamic, comprehensive, continuous situational awareness of the security of federal information and information systems;
>
> “(2) provide situational awareness of the Nation’s information security posture; and
>
> “(3) foster information security collaboration among information system owners and operators.

‘‘(e) compile and analyze information about risks and incidents that threaten federal and private sector information and information systems; and

‘‘(f) provide incident detection, analysis, mitigation, and response information and remote or on-site technical assistance to

> “(1) heads of agencies; and
>
> “(2) upon request and at the discretion of the Secretary, private sector entities.

“§ 3557. National security systems

“The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

“(a) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized use, disclosure, disruption, modification, or destruction of the information contained in such system;

“(b) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

“(c) complies with the requirements of this subchapter.

“§ 3558. Authorization of appropriations

“There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2012 through 2017.

"§ 3557. Effect on existing law and savings provisions

"(a) EFFECT ON EXISTING LAW.--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.

"(b) SAVINGS PROVISIONS.--

"(1) Policy and compliance guidance issued by the Director of the Office of Management and Budget prior to the effective date of this Act pursuant to section 3543(a)(1) of title 44 (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) of title 44, as added by this Act.

"(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) CLERICAL AMENDMENT.--

The table of sections for chapter 35 of title 44 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. National Security Systems.

"3558. Authorization of Appropriations.

"3559. Effect on Existing Law and Savings Provisions.

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 otherwise authorized by law and 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.

"(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 (15 U.S.C. 278g-3).

"(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.

"(3) National security system.--The term "national security system" has the meaning given that term in section 3552 of title 44.

(b) TECHNICAL AND CONFORMING AMENDMENTS.--Section 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-4) is amended as follows:

(1) Section 21(b)(2) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-4) 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 (15 U.S.C. 278g-4) is amended after "the Secretary of Commerce" by inserting "Secretary of Homeland Security".

(c) 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)".

(d) Title 10 of the United States Code is amended as follows:

(1) Section 2222(j)(6) is amended by striking "section 3542(b)(2))" and inserting "section 3551(b)".

(2) Section 2223(c)(3) is amended, by striking "section 3542(b)(2)" and inserting "section 3551(b)".

(3) Section 2315 is amended by striking "section 3542(b)(2))" and inserting "section 3551(b)".

(e) 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)".