112TH CONGRESS
2D SESSION

S. 2151

To improve information security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MARCH 1, 2012

Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To improve information security, 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; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

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

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that may be indicative of or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that may signify malicious intent;

(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or information that would foster situational awareness of the United States security posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information

exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination thereof.

(5) CYBERSECURITY CENTER.—The term ''cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

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

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

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

(C) availability, by ensuring timely and reliable access to and use of information.

(9) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(10) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for ac-

tively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(11) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(12) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(13) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(14) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(15) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

SEC. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in

the course of providing information security products or services under contract to another entity, that entity shall, at any time prior to disclosure of such information, be given a reasonable opportunity to authorize or prevent such disclosure or to request anonymization of such information.

(b) REQUIRED DISCLOSURE.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or cybersecurity services under contract to a Federal agency or department shall immediately provide to such agency or department, and may provide to a cybersecurity center, any cyber threat information directly related to such contract that is obtained, identified, or otherwise possessed by such entity.

(2) DISCLOSURE TO CYBERSECURITY CENTERS.—A Federal agency or department receiving cyber threat information under paragraph (1) shall immediately disclose such information to a cybersecurity center.

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to and used by—

(A) any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code; or

(B) an entity that is acting as a provider of electronic communication services, remote computing service, or cybersecurity services to a Federal agency or department for purposes related to such services;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government

and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(5) shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records;

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or

government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent pos-

sible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or other-

wise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN PRIVATE ENTITIES.—

(1) IN GENERAL.—A private entity sharing cyber threat information with another private entity under this title may restrict the use or sharing of such information by such other private entity.

(2) FURTHER SHARING.—Cyber threat information shared by any private entity with another private entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the private entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any private entity to gain an unfair competitive advantage to the detriment of the private entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title

shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(f) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This section supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section.

(2) STATE LAW ENFORCEMENT.—Nothing in this section shall be construed to supercede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement techniques.

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to

any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed as creating any immunity against, or otherwise affecting, any action brought by the Federal government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of Na-

tional Intelligence and the Secretary of Defense shall, in consultation with the heads of the appropriate Federal departments or agencies, develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions

of this section, unclassified cyber threat information in the possession of the Federal government—

(1) is shared in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

(d) UTILIZING EXISTING PROCESSES.—Procedures developed under this section shall coordinate with existing processes utilized by sector specific information sharing and analysis centers.

SEC. 104. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1)(A) of this Act;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) with respect to an entity providing electronic communication services, remote computing service, or cybersecurity services to a Federal agency or department, a description of any violations of the requirements of subsection (b) or (c) of section 102 of this Act related to the performance of such services;

(7) a list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(8) a description of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(9) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 105. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'';

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 106. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clear-

ance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. 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—

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

''(2) to 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) to 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;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to 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

''In this subchapter:

''(1) ADEQUATE SECURITY.—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) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that may be indicative of or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that may signify malicious intent;

''(G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or information that would foster situational awareness of the United States security posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination thereof.

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) 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.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

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

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

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

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

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

''(13) MALICIOUS RECONNAISSANCE.—The term 'malicious reconnaissance' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical

vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—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) LIMITATION.—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).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to

protect the confidentiality, integrity, and availability of the system and its information.

''(19) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

"§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with 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 and guidelines 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 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 and cyber threat information;

"(D) requirements for agencywide 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 the policies and directives issued by the Secretary under this subchapter;

"(G) training requirements regarding privacy, civil rights, and civil liberties, and infor-

mation oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

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

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

"(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

"(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

"(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

"(c) LIMITATION OF AUTHORITY.—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.

"(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

"§ 3554. Agency responsibilities

''(a) IN GENERAL.—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 and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives,

standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

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

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center 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, cyber threat infor-

mation, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a); including information to assist the Secretary of Homeland Security with carrying out the ongoing security analysis under section 3555.

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(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 level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for infor-

mation security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

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

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(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 an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to 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)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the

Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

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

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) security engineering throughout the development and acquisition lifecycle;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) 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 security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

"(i) mitigating risks associated with such information security incidents;

"(ii) notifying and consulting with the entity designated under section 3555; and

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

"(I) law enforcement and the relevant Office of the Inspector General; and

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

"(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

"(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

"(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for in-

formation security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the 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 any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(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) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agency-wide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

"§ 3555. Multiagency ongoing threat assessment

''(a) PURPOSE.—The purpose of this section is to provide a framework for each agency to provide to the designee of the Secretary of Homeland Security under subsection (b)—

''(1) timely and actionable cyber threat information; and

''(2) information on the environment of operation of an agency information system.

''(b) DESIGNEE.—The Secretary of Homeland Security shall designate an entity within the Department of Homeland Security—

''(1) to conduct ongoing security analysis concerning agency information systems—

''(A) based on cyber threat information;

''(B) based on agency information system and environment of operation changes, including—

''(i) an ongoing evaluation of the information system security controls; and

''(ii) the security state, risk level, and environment of operation of an agency information system, including—

''(I) a change in risk level due to a new cyber threat;

''(II) a change resulting from a new technology;

''(III) a change resulting from the agency's mission; and

''(IV) a change resulting from the business practice; and

''(C) using automated processes to the maximum extent possible—

''(i) to increase information system security;

''(ii) to reduce paper-based reporting requirements; and

''(iii) to maintain timely and actionable knowledge of the state of the information system security.

''(2) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(3) COMPLIANCE.—The head of each appropriate agency shall be responsible for ensuring compliance with this section. The Secretary of Homeland Security, in consultation with the head of each appropriate agency, shall—

''(A) monitor compliance under this section;

''(B) develop a timeline for each agency—

''(i) to adopt any technology, system, or method that facilitates continuous monitoring of an agency information system; and

''(ii) to adopt any technology, system, or method that satisfies a requirement under this section.

''(4) LIMITATION OF AUTHORITY.—The authorities of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(5) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Secretary of Homeland Security shall report to Congress each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Sec-

retary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

"§ 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—

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

''(2) 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.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of

this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and

Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(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)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 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 prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) 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)(2) and (a)(3)).

''(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 STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines 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 AND GUIDELINES.—

"(A) IN GENERAL.—Standards and guidelines 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) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

"(c) 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.

"(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—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 and guidelines the Secretary of Commerce pre-

scribes under this section if the more stringent standards and guidelines—

"(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

"(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

"(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

"(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of

the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provi-

sions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that

purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) gas and oil production, storage, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy

statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research,

development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15

U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

"(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

"(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

"(A) the advisory committee under subsection (b); and

"(B) the stakeholders under section 102(a)(3).

"(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

"(A) the advisory committee under subsection (b);

"(B) the Committee on Commerce, Science, and Transportation of the Senate; and

"(C) the Committee on Science and Technology of the House of Representatives.".

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Compo-

nent Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Tech-

nology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

(1) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively;

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other

means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

"SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from

institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

"SEC. 102. PROGRAM IMPROVEMENTS.

"(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

"(1) to provide technical and administrative support to—

"(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

"(B) the advisory committee under section 101(b);

"(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

"(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from aca-

demia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Pol-

icy that is provided by each agency participating in the Program for each fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 404. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following new paragraph:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORM-**

ANCE COMPUTING'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including

networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 401(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-perform-

ance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is

amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation shall continue a Federal Cyber Scholarship-for-Service program under section 5(a) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)) to increase the capacity of the higher education system to produce an information technology workforce with the skills necessary to enhance the security of the Nation's communications and information infrastructure and to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) provide, through qualified institutions of higher education, scholarships that provide tuition, fees, and a competitive stipend for up to 2 years to students pursuing a bachelor's or master's degree and up to 3 years to students pursuing a doctoral degree in a cybersecurity field;

(2) provide the scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the Federal information technology workforce;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times the length of the study following graduation in that field;

(4) increase the capacity of institutions of higher education throughout all regions of the United States to produce highly qualified cybersecurity professionals, through the award of competitive, merit-reviewed grants that support such activities as—

(A) faculty professional development, including technical, hands-on experiences in the private sector or government, workshops, seminars, conferences, and other professional devel-

opment opportunities that will result in improved instructional capabilities;

(B) institutional partnerships, including minority serving institutions and community colleges; and

(C) development of cybersecurity-related courses and curricula;

(5) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(6) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an individual in the Federal civil service, upon the successful completion of the degree, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

(2) COMPETITIVE SERVICE.—Upon satisfactory fulfillment of the service term under paragraph (1), an individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—A scholarship under this section shall be available only to a student who—

(1) is a citizen or permanent resident of the United States;

(2) is a full time student in an eligible degree program, as determined by the Director, that is focused on computer security or information assurance at an awardee institution;

(3) accepts the terms of a scholarship under this section;

(4) obtains a minimum SAT/College Board score of 1600 (1100 Critical Reading and Math, 500 in Writing) or ACT score of 25;

(5) maintains a GPA of 3.0 or above on a 4.0 scale;

(6) demonstrates a commitment to a career in improving the security of the information infrastructure; and

(7) has demonstrated a level of proficiency in math or computer sciences.

(e) SERVICE OBLIGATION.—

(1) IN GENERAL.—If an individual receives a scholarship under this section, as a condition of receiving such scholarship, the individual upon completion of the degree must serve as a cybersecurity professional within the Federal workforce for a period of time as provided in subsection (g).

(2) NOT OFFERED EMPLOYMENT.—If a scholarship recipient is not offered employment by a Federal agency or a federally funded research and development center, the service requirement can be satisfied at the Director's discretion by—

(A) serving as a cybersecurity professional in a State, local, or tribal government agency; or

(B) teaching cybersecurity courses at an institution of higher education.

(f) CONDITIONS OF SUPPORT.—As a condition of acceptance of a scholarship under this section, a scholarship recipient shall agree to provide the awardee institution

with annual verifiable documentation of employment and up-to-date contact information.

(g) LENGTH OF SERVICE.—The length of service required in exchange for a scholarship under this section shall be 1 year more than the number of years for which the scholarship was received.

(h) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) GENERAL RULE.—A scholarship recipient under this section shall be liable to the United States under paragraph (3) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section; or

(E) fails to fulfill the service obligation of the individual under this section.

(2) MONITORING COMPLIANCE.—As a condition of participating in the program, a qualified institution of higher education receiving a grant under this section shall—

(A) enter into an agreement with the Director of the National Science Foundation to monitor the compliance of scholarship recipients with respect to their service obligations; and

(B) provide to the Director, on an annual basis, post-award employment information for scholarship recipients through the completion of their service obligations.

(3) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid or such amount shall be treated as a loan to be repaid in accordance with subparagraph (C).

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph

(D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid or such amount shall be treated as a loan to be repaid in accordance with subparagraph (C).

(C) REPAYMENTS.—A loan described under subparagraph (A) or (B) shall be treated as a Federal Direct Unsubsidized Stafford Loan under part D of title IV of the Higher Education Act of 1965 (20 U.S.C. 1087a et seq.), and shall be subject to repayment, together with interest thereon accruing from the date of the scholarship award, in accordance with terms and conditions specified by the Director (in consultation with the Secretary of Education) in regulations promulgated to carry out this paragraph.

(4) COLLECTION OF REPAYMENT.—

(A) IN GENERAL.—In the event that a scholarship recipient is required to repay the

scholarship under this subsection, the institution providing the scholarship shall—

(i) be responsible for determining the repayment amounts and for notifying the scholarship recipient and the Director of the amount owed; and

(ii) collect such repayment amount within a period of time as determined under the agreement under paragraph (2) or the repayment amount shall be treated as a loan in accordance with paragraph (3)(C).

(B) RETURNED TO TREASURY.—Except as provided in subparagraph (C), any such repayment shall be returned to the Treasury of the United States.

(C) RETAIN PERCENTAGE.—An institution of higher education may retain a percentage of any repayment the institution collects under this paragraph to defray administrative costs associated with the collection. The Director shall establish a single, fixed percentage that will apply to all eligible entities.

(5) EXCEPTIONS.—The Director may provide for the partial or total waiver or suspension of any

service or payment obligation by an individual under this section if—

(A) compliance by the individual with the obligation is impossible;

(B) compliance by the individual would involve extreme hardship to the individual; or

(C) enforcement of such obligation with respect to the individual would be unconscionable.

(i) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(j) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Secretary may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the

hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 408. CYBERSECURITY STRATEGIC RESEARCH AND DEVELOPMENT PLAN.

(a) IN GENERAL.—Not later than 12 months after the date of enactment of this Act, the agencies designated under subsection 101(a)(3)(B) (i) through (xi) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)(B) (i) through (xi)) (working through the National Science and Technology Council) shall transmit to Congress a strategic plan based on an assessment of cybersecurity risk to guide the overall direction of Federal cybersecurity and information assurance research and development for information technology and networking systems. Once every 3 years after the initial strategic plan is transmitted to Congress under this section, the agencies shall prepare and transmit to Congress an update of the strategic plan.

(b) CONTENTS OF PLAN.—The strategic plan under subsection (a) shall—

(1) specify and prioritize—

(A) near-term, mid-term, and long-term research objectives, including objectives associated with the research areas identified in section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)); and

(B) how the near-term objectives complement research and development areas in which the private sector is actively engaged;

(2) describe how the National Networking and Information Technology Research and Development Program will focus on innovative, transformational technologies with the potential to enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure, and to protect consumer privacy;

(3) describe how the Program will foster the rapid transfer of research and development results into new cybersecurity technologies and applications for the timely benefit of society and the national interest, including through the dissemination of best practices and other outreach activities;

(4) describe how the Program will establish and maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems;

(5) describe how the Program will facilitate access by academic researchers to the infrastructure described in paragraph (4), as well as to relevant data, including event data; and

(6) describe how the Program will engage females and individuals identified in section 33 or 34 of the Science and Engineering Equal Opportunities Act (42 U.S.C. 1885a and 1885b) to foster a more diverse workforce in this area.

(c) DEVELOPMENT OF IMPLEMENTATION ROADMAP.—The agencies described in subsection (a) shall develop and annually update an implementation roadmap for the strategic plan under this section. The implementation roadmap shall—

(1) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated;

(2) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

(3) estimate the funding required for each major research objective of the strategic plan for the following 3 fiscal years.

(d) RECOMMENDATIONS.—In developing and updating the strategic plan under subsection (a), the agencies involved shall solicit recommendations and advice from—

(1) the advisory committee established under section 101(b)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)(1)); and

(2) a wide range of stakeholders, including industry, academia (including representatives of minority serving institutions and community colleges), National Laboratories, and other relevant organizations and institutions.

(e) REPORT APPENDIX.—The implementation roadmap under subsection (c), and its annual updates, shall be appended to the report under section 101(a)(2)(D) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)(D)).

(f) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Secretary may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 409. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 410. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information

technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 411. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

''(K) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end of the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end of the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124

Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end of the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end of the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end of the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Secretary finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(g) CYBERSECURITY FACULTY DEVELOPMENT TRAINEESHIP PROGRAM.—Section 5(e)(9) of the Cyber Security Research and Development Act (15 U.S.C.

7404(e)(9)) is amended by striking ''2007'' and inserting ''2007 and for each of fiscal years 2012 through 2014''.

○