I

111TH CONGRESS
2D SESSION

H. R. 6423

To enhance homeland security, including domestic preparedness and collective response to terrorism, by amending the Homeland Security Act of 2002 to establish the Cybersecurity Compliance Division and provide authorities to the Department of Homeland Security to enhance the security and resiliency of the Nation's cyber and physical infrastructure against terrorism and other cyber attacks, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 17, 2010

Mr. THOMPSON of Mississippi (for himself, Ms. CLARKE, and Ms. HARMAN) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Oversight and Government Reform, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To enhance homeland security, including domestic preparedness and collective response to terrorism, by amending the Homeland Security Act of 2002 to establish the Cybersecurity Compliance Division and provide authorities to the Department of Homeland Security to enhance the security and resiliency of the Nation's cyber and physical infrastructure against terrorism and other cyber attacks, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Homeland Security Cyber and Physical Infrastructure Protection Act of 2010''.

SEC. 2. OFFICE OF CYBERSECURITY AND COMMUNICATIONS AND CYBERSECURITY COMPLIANCE DIVISION.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by redesignating sections 221 through 225 in order as section 226 through 229, respectively, and by inserting before section 222 (as so redesignated) the following:

''SEC. 221. DEFINITIONS.

''In this subtitle:

''(1) COMMON CRITERIA FOR INFORMATION TECHNOLOGY SECURITY EVALUATION.—The term 'common criteria for information technology security evaluation' means international standard for computer security codified in the International Organization for Standardization and the International Electrotechnical Commission standard 15408 (ISO/IEC 15408).

''(2) COVERED CRITICAL INFRASTRUCTURE.—The term 'covered critical infrastructure' means systems and assets designated by the Director under section 224(e).

''(3) CYBER INCIDENT.—The term 'cyber incident' means an occurrence that jeopardizes the security of data or the physical security of a computer network owned or operated by a Federal agency or covered critical infrastructure.

''(4) FIRST-PARTY REGULATORY AGENCY.—The term 'first-party regulatory agency' means a Federal agency that is not a sector-specific agency but that has primary regulatory authority for a specific critical infrastructure sector or sub-sector.

''(5) SECTOR-SPECIFIC AGENCY.—The term 'sector-specific agency' means the agency that, as of the date of enactment of this section, is designated under Homeland Security Presidential Directive 7 as the lead Federal agency responsible for securing a specific critical infrastructure sector.

"SEC. 222. OFFICE OF CYBERSECURITY AND COMMUNICATIONS.

''(a) ESTABLISHMENT.—

''(1) IN GENERAL.—There shall be in the Department an Office of Cybersecurity and Communications.

''(2) ASSISTANT SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS.—The Assistant Sec-

retary for Cybersecurity and Communications shall be the head of the Office.

''(3) COMPONENTS.—The Office shall include—

''(A) the United States Computer Emergency Readiness Team, as in effect on the date of enactment of this section;

''(B) the Cybersecurity Compliance Division established by subsection (b); and

''(C) other components of the Department that have primary responsibilities for emergency or national communications or cybersecurity.

''(b) CYBERSECURITY COMPLIANCE DIVISION.—

''(1) IN GENERAL.—There is established in the Office of Cybersecurity and Communications a Cybersecurity Compliance Division.

''(2) DIRECTOR.—The Cybersecurity Compliance Division shall be headed by a Director, who shall be appointed by the Secretary or the Secretary's designee from among individuals who possess—

''(A) demonstrated knowledge and ability in cybersecurity, information technology, infrastructure protection, and the operation, security, and resilience of communications networks;

''(B) significant executive leadership, regulatory, and management experience in the public or private sector; and

''(C) other skills or attributes the Secretary considers necessary.

''(3) DUTIES AND RESPONSIBILITIES.—The Director—

''(A) shall issue risk-based, performance-based regulations, after notice and comment, in accordance with section 224;

''(B) shall serve as the first-party regulatory agency to enforce regulations under section 224 for computer networks and assets in critical infrastructure sectors for which the Office of Cybersecurity and Communications or any of its components is the designated sector-specific agency;

''(C) may require a first-party regulatory agency or sector-specific agency to coordinate with the Director to—

''(i) develop and publish, for covered critical infrastructure sectors or subsectors, risk-based and performance-based regulations after notice and comment in accordance with paragraph (1), with any

appropriate modifications, as identified by the Director, necessary for application to a specific critical infrastructure sector or subsector; and

''(ii) enforce the regulations promulgated under paragraph (1); and

''(D) may delegate part or all of the responsibilities and authorities for securing private sector networks under this section to an appropriate first-party regulatory agency or sector-specific agency, which shall report to the Director all activities it carries out pursuant to such delegation.

''(4) RESOURCES.—There is authorized to be appropriated such sums as may be necessary for the operations of the Cybersecurity Compliance Division for each of fiscal years 2012, 2013, and 2014.

''SEC. 223. DEPARTMENT RESPONSIBILITIES AND AUTHORITIES FOR SECURING FEDERAL GOVERNMENT NETWORKS.

''(a) IN GENERAL.—The Secretary, acting through the Assistant Secretary for Cybersecurity and Communications or the Director of the Cybersecurity Compliance Division pursuant to subparagraphs (B), (C), and (D) of subsection (b)(2), shall establish and enforce cybersecurity

requirements for civilian nonmilitary and nonintelligence community Federal systems to prevent, deter, prepare for, detect, report, attribute, mitigate, respond to, and recover from cyber attacks and other cyber incidents.

''(b) INTERAGENCY WORKING GROUP.—

''(1) IN GENERAL.—The Assistant Secretary for Cybersecurity and Communications shall establish and chair an interagency working group that shall include, at a minimum, representation of all chief information officers from all Federal civilian agencies, the Director of the Cybersecurity Compliance division, the Assistant Secretary for Infrastructure Protection, and the White House Cybersecurity Coordinator. The Assistant Secretary shall invite the Secretary of Defense, the Director of the National Security Agency, and the Director of National Intelligence to participate as nonvoting representatives for purposes of advising the interagency working group.

''(2) FUNCTIONS.—The interagency working group shall—

''(A) meet at the call of the Chair;

''(B) develop and adopt risk-based, performance-based cybersecurity requirements for

civilian Federal agency computer networks and federally owned critical infrastructure;

''(C) develop and adopt a range of remedies, including penalties, for noncompliance of the requirements adopted under paragraph (2), each agency having one vote;

''(D) develop recommended budgets for security of the civilian nonmilitary and non-intelligence community Federal agency computer networks; and

''(E) propose updates, as necessary, for the Common Criteria for Information Technology Security Evaluation as part of a supply chain risk management strategy designed to ensure the security and resilience of the Federal information infrastructure, including protection against unauthorized access to, alteration of information in, disruption of operations of, interruption of communications or services of, and insertion of malicious software, engineering vulnerabilities, or otherwise corrupting software, hardware, services, or products intended for use in Federal information infrastructure.

''(3) ADOPTION BY VOTE.—Adoption of requirements and remedies under subparagraphs (B) and

(C) of paragraph (2) shall be by a majority vote of the members of the interagency working group, in which each agency with a voting representative on the interagency working group has one vote.

''(e) CODIFICATION OF AGREEMENTS.—All measures adopted under subsection (b) shall be submitted by the Secretary to the Office of Management and Budget for establishment in a binding Governmentwide memo or circular.

''(d) ENFORCEMENT OF CYBERSECURITY REQUIREMENTS FOR FEDERAL GOVERNMENT NETWORKS.—The Assistant Secretary, acting through the Director of the Cybersecurity Compliance Division, may enforce all requirements adopted under subsection (b)(2)(B).

''(e) CERTIFICATIONS, AUDITS, AND INSPECTIONS.—The Director of the Cybersecurity Compliance Division, in carrying out the Assistant Secretary for Cybersecurity and Communications' enforcement authority under subsection (d), shall require a certification of compliance from the head of each civilian Federal agency that is subject to the requirements under subsection (b)(2)(B), and may conduct announced or unannounced audits and inspections of any network owned, operated, or used by a Federal civilian agency.

''(f) ENFORCEMENT.—If a certification, audit, or inspection carried out under subsection (e) shows noncompliance with a requirement under subsection (b)(2)(B), Assistant Secretary, acting through the Director of the Cybersecurity Compliance Division, may identify the appropriate remedies, including penalties, under subsection (b)(2)(C).

''(g) EXECUTION OF PENALTIES BY OMB.—The Director of the Office of Management and Budget shall execute each remedy identified by the Director of the Cybersecurity Compliance Division under subsection (f) on behalf of the Assistant Secretary.

''(h) REPORTING OF CYBER INCIDENTS ON FEDERAL NETWORKS.—The requirements under subsection (b)(2)(B) shall include a requirement that all Federal entities report any cyber incidents on their computer networks to the Director and to the United States Computer Emergency Readiness Team.

''(i) RESPONDING TO CYBER INCIDENTS ON FEDERAL NETWORKS.—If an incident is reported under subsection (h), the United States Computer Emergency Readiness Team shall, in coordination with the reporting agency, research the incident to determine and report to the Director and the reporting agency—

''(1) the extent of any compromise;

''(2) an identification of any attackers, including any affiliations with terrorists, terrorist organizations, criminal organizations, state entities, and nonstate entities;

''(3) the method of penetration;

''(4) ramifications of any such compromise on future operations;

''(5) secondary ramifications of any such compromise on other Federal or non-Federal networks;

''(6) ramifications of any such compromise on national security, including war fighting capability; and

''(7) recommended mitigation activities.

''SEC. 224. DEPARTMENT RESPONSIBILITIES AND AUTHORITIES FOR SECURING PRIVATE SECTOR NETWORKS.

''(a) FINDINGS.—Congress finds that—

''(1) pursuant to Homeland Security Presidential Directive 7 the Department established public-private partnerships including Government Coordinating Councils (GCCs) and Sector Coordinating Councils (SCCs) to aid in the task of protecting the Nation's critical infrastructures;

''(2) as part of this structure, each critical infrastructure sector has a designated sector-specific agency;

''(3) the designated sector-specific agency for the Information Technology sector is the Office of Cybersecurity and Communications, and the designated sector-specific agency for the communications sector is the National Communications System, which resides within the Office of Cybersecurity and Communications;

''(4) if cybersecurity regulation are necessary, the Department, consistent with the entire GCC/SCC structure, as the sector-specific agency, will be the regulator for cybersecurity requirements within the information technology and communications sectors; and

''(5) in other critical infrastructure sectors, enforcement of cybersecurity regulations should be accomplished through appropriate first-party regulatory agencies or sector-specific agencies.

''(b) GENERAL AUTHORITY.—The Secretary, acting through the Director, may establish and enforce risk-based cybersecurity requirements for private sector computer networks within covered critical infrastructures.

''(c) RISK-BASED CYBERSECURITY REQUIREMENTS FOR CRITICAL INFRASTRUCTURE.—

''(1) IN GENERAL.—The Director shall promulgate risk-based, performance-based cybersecurity requirements for covered critical infrastructures, that are designed to prevent, deter, prepare for, detect, report, attribute, mitigate, respond to and recover from cyber incidents.

''(2) RISK FACTORS.—The requirements shall be based on the risk factors of threats, vulnerabilities, and consequences, as follows:

''(A) THREATS.—The requirements shall be based on terrorist or other known adversary capabilities and intent, or the likelihood of a potential terrorist or other adversary attacking or causing a cyber incident against critical infrastructure, as identified by the Secretary in consultation with the Director of National Intelligence, including—

''(i) theft, modification, compromise, damage, or destruction of data or databases;

''(ii) physical compromise, damage, or destruction of covered critical infrastructures; and

"(iii) national, corporate, or personal espionage.

"(3) VULNERABILITIES.—The requirements shall require security measures based on—

"(A) preparedness;

"(B) target attractiveness; and

"(C) deterrence capabilities.

"(4) CONSEQUENCES.—The requirements shall require security measures based on—

"(A) the potential extent and likelihood of death, injury, or serious adverse effects to human health and safety caused by a disruption of the reliable operation of covered critical infrastructure;

"(B) the threat to or potential impact on national security caused by a disruption of the reliable operation of covered critical infrastructure;

"(C) the extent to which the disruption of the reliable operation of covered critical infrastructure will disrupt the reliable operation of other covered critical infrastructure;

"(D) the potential for harm to the economy that would result from a disruption of the

reliable operation of covered critical infrastructure; and

''(E) other risk-based security factors that the Director, in consultation with the head of the sector-specific agency that is the first-party regulatory agency with responsibility for the covered critical infrastructure concerned, determines to be appropriate and necessary to protect public health and safety, critical infrastructure, national security, or economic security.

''(d) CONSULTATION.—In establishing security performance requirements under subsection (c), the Director shall, to the maximum extent practicable, consult with—

''(1) the Assistant Secretary for Infrastructure Protection of the Department;

''(2) the Officer for Civil Rights and Civil Liberties of the Department;

''(3) the Chief Privacy Officer of the Department;

''(4) the Under Secretary for Intelligence and Analysis;

''(5) the Director of National Intelligence;

''(6) the Director of the National Security Agency;

''(7) the Director of the National Institute of Standards and Technology;

''(8) the heads of sector-specific agencies;

''(9) the heads of first-party regulatory agencies;

''(10) private sector companies or industry groups, including but not limited to members of appropriate sector coordinating councils;

''(11) State, local, and tribal agency representatives;

''(12) academic institutions and think tanks;

''(13) private sector, government, and nonprofit entities that specialize in privacy and civil liberties; and

''(14) the White House Cybersecurity Coordinator.

''(e) COVERED CRITICAL INFRASTRUCTURES.—

''(1) DESIGNATION.—The Director shall—

''(A) determine, in consultation with the heads of sector-specific agencies and the heads of first-party regulatory agencies, which systems or assets of critical infrastructure shall be subject to the requirements of this section and designate them as covered critical infrastructures for purposes of this section;

''(B) notify each first-party regulatory agency or sector-specific agency of each such determination; and

''(C) acting through the corresponding first-party regulatory agency or sector-specific agency, notify owners or operators of covered critical infrastructure sectors of the requirements of this subtitle.

''(2) REQUIREMENTS.—A system or asset may not be designated as covered critical infrastructure under paragraph (1) unless—

''(A) the system or asset meets the requirements for inclusion on the prioritized critical infrastructure list established by the Secretary under section 210E(a)(2);

''(B) the system or asset is a component of the national information infrastructure or the national information infrastructure is essential to the reliable operation of the system or asset; or

''(C) the destruction or the disruption of the reliable operation of the system or asset would cause a national or regional catastrophe.

''(3) FACTORS TO BE CONSIDERED.—In designating systems or assets under this section, the Di-

rector shall consider cyber risks and consequences by sector, including—

"(A) the factors listed in section subsection (c);

"(B) known cyber incidents or cyber risks identified by existing risk assessments;

"(C) interdependencies between components of covered critical infrastructure; and

"(D) the potential for the destruction or disruption of the system or asset to cause—

"(i) a mass casualty event with an extraordinary number of fatalities;

"(ii) severe economic consequences;

"(iii) mass evacuations with a prolonged absence; or

"(iv) severe degradation of national security capabilities, including intelligence and defense functions.

"(4) RECONSIDERATION.—Prior to a final designation of a system or asset of critical infrastructure under this subsection, the Director shall provide the owner or operator of the system or asset an opportunity to appeal the determination made under paragraph (1)(A).

''(f) CYBERSECURITY PLANS.—The Director shall require entities determined under subsection (e) to be covered critical infrastructures to comply with the requirements under subsection (c) and to submit to the first-party regulatory agency or sector-specific agency, a proposed cybersecurity plan to satisfy the security performance requirements described in subsection (c) on a timeline determined by the Director.

''(g) CYBERSECURITY PLAN REVIEW.—Upon submission of the plan, the first-party regulatory agency or sector-specific agency shall, based on guidance provided by the Director—

''(1) review cybersecurity plans submitted pursuant to subsection (f);

''(2) approve or disapprove each cybersecurity plan;

''(3) notify the submitter of the cybersecurity plan of approval or disapproval;

''(4) in the case of disapproval, provide a clear explanation of the reasons for disapproval, possible changes that would result in approval, and provide a timetable for resubmission for compliance; and

''(5) inform the Director of any approvals or disapprovals.

"(h) IMPLEMENTATION OF CYBERSECURITY PLANS.—

"(1) IN GENERAL.—The owners and operators of covered critical infrastructure shall have flexibility in their cybersecurity plans to implement any cybersecurity measure, or combination thereof, to satisfy the cybersecurity performance requirements described in subsection (c) and the first-party regulatory agency or sector-specific agency may not disapprove under this section any proposed cybersecurity measures, or combination thereof, based on the presence or absence of any particular cybersecurity measure if the proposed cybersecurity measures, or combination thereof, satisfy the cybersecurity performance requirements established by the Director under subsection (c).

"(2) RECOMMENDED CYBERSECURITY MEASURES.—The Assistant Secretary for Cybersecurity and Communications may, at the request of an owner and operator of covered critical infrastructure, recommend a specific cybersecurity measure, or combination thereof, that will satisfy the cybersecurity performance requirements established by the Director. The absence of the recommended security measures, or combination thereof, may not serve as the

basis for a disapproval of the security measure, or combination thereof, proposed by the owner or operator of covered critical infrastructure if the proposed security measure, or combination thereof, otherwise satisfies the security performance requirements established by the Director under (c).

''(i) ENFORCEMENT CERTIFICATIONS, AUDITS AND INSPECTIONS.—The sector-specific agency or first-party regulatory agency, in enforcing the requirements under subsection (c), shall require an entity with a cybersecurity plan approved under subsection (g) to certify that the cybersecurity plan has been implemented, and may conduct announced or unannounced audits and inspections of any such entity to determine compliance.

''(j) REPORTING OF CYBER INCIDENTS ON COVERED CRITICAL INFRASTRUCTURE NETWORKS.—The requirements under subsection (c) shall include a requirement that each covered critical infrastructure entity report any cyber incidents on its networks to the first-party regulatory agency for the entity or to the sector-specific agency for the entity (if there is no first-party regulatory agency), and to US CERT.

''(k) RESPONDING TO CYBER INCIDENTS ON PRIVATE NETWORKS.—If an incident is reported under subsection (j), the United States Computer Emergency Readi-

ness Team may, at the invitation of and in coordination with the reporting entity, investigate the incident to determine and report to the Director and the reporting entity—

''(1) the extent of any compromise;

''(2) an identification of any attackers, including any affiliations with terrorists, terrorist organizations, state entities, and nonstate entities;

''(3) the method of penetration;

''(4) ramifications of any such compromise on future operations;

''(5) secondary ramifications of any such compromise on other Federal or non-Federal networks;

''(6) ramifications of any such compromise on national security, including war fighting capability; and

''(7) recommended mitigation activities.

''(l) SAFETY ACT INCENTIVES.—The Director may recommend SAFETY Act designation and certification to entities determined under subsections (g) and (i) to be in compliance with the requirements of this section.

''(m) PENALTIES.—In the case of noncompliance with the requirements of this section the Director may recommend recision or suspension of SAFETY Act designation and certification during the period of noncompliance,

and may levy civil penalties, not to exceed $100,000 per day, for each instance of noncompliance.''.

(b) DEADLINES.—The Cybersecurity Compliance Division of the Department of Homeland Security shall—

(1) not later than six months after such date of enactment of this Act, publish a notice of proposed rulemaking for regulations required under section 224of the Homeland Security Act of 2002, as amended by this section; and

(2) not later than one year after such date of enactment of this Act, promulgate final regulations required under such section.

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide authority to any sector-specific agency or first-party regulatory agency to establish standards or other measures outside of the requirements of this Act except as required by this Act and the amendments made by this Act.

(d) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by striking the items relating to sections 221 through 225 and inserting the following:

SEC. 3. INFORMATION SHARING.

The Assistant Secretary for Cybersecurity and Communications of the Department of Homeland Security in coordination with the Assistant Secretary Infrastructure Protection of the Department of Homeland Security shall, to the maximum extent possible, consistent with rules for the handling of classified information, share relevant information regarding cybersecurity threats and vulnerabilities, and any proposed actions to mitigate them, with all Federal agencies, appropriate State, local, or tribal authority representatives, and all covered critical infrastructure owners and operators, including by expediting necessary security clearances for designated points of contact for critical infrastructures.

SEC. 4. INFORMATION PROTECTION.

The Assistant Secretary for Cybersecurity and Communications of the Department of Homeland Security shall designate, as appropriate, information received from Federal agencies pursuant to the requirements enacted by section 2 (including the amendments made by such section), information received from covered critical infrastructure owners and operators pursuant to such section, and information provided to Federal agencies or covered

critical infrastructure owners and operators pursuant to this section as sensitive security information and shall require and enforce sensitive security information requirements for handling, storage, and dissemination of any such information.

SEC. 5. CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—The Under Secretary for Science and Technology of the Department of Homeland Security shall support research, development, testing, evaluation, and transition of cybersecurity technology, including fundamental, long-term research to improve the ability of the United States to prevent, protect against, detect, respond to, and recover from acts of terrorism and cyber attacks, with an emphasis on research and development relevant to large-scale, high-impact attacks.

(b) ACTIVITIES.—The research and development supported under subsection (a) shall include work to—

(1) advance the development and accelerate the deployment of more secure versions of fundamental Internet protocols and architectures, including for the domain name system and routing protocols;

(2) improve and create technologies for detecting attacks or intrusions, including real-time monitoring and real-time analytic technologies;

(3) improve and create mitigation and recovery methodologies, including techniques and policies for real-time containment of attacks, and development of resilient networks and systems that degrade gracefully;

(4) develop and support infrastructure and tools to support cybersecurity research and development efforts, including modeling, test beds, and data sets for assessment of new cybersecurity technologies;

(5) assist the development and support of technologies to reduce vulnerabilities in process control systems;

(6) develop and support cyber forensics and attack attribution; and

(7) test, evaluate, and facilitate the transfer of technologies associated with the engineering of less vulnerable software and securing the information technology software development lifecycle.

(c) COORDINATION.—In carrying out this section, the Under Secretary shall coordinate activities with—

(1) the Under Secretary for National Protection and Programs, the Assistant Secretary for Cybersecurity and Communications, and the Assistant Secretary for Infrastructure Protection of the Department of Homeland Security; and

(2) the heads of other relevant Federal departments and agencies, including the National Science Foundation, the Defense Advanced Research Projects Agency, the Information Assurance Directorate of the National Security Agency, the National Institute of Standards and Technology, the Department of Commerce, and other appropriate working groups established by the President to identify unmet needs and cooperatively support activities, as appropriate.

SEC. 6. CYBER WORKFORCE RECRUITMENT, DEVELOPMENT, AND RETENTION.

(a) WORKFORCE PLAN.—Not later than 180 days after the date of enactment of this Act and in every subsequent year, the Assistant Secretary for Cybersecurity and Communication of the Department of Homeland Security shall develop a strategic cybersecurity workforce plan as part of the Federal agency performance plan required under section 1115 of title 31, United States Code, that includes—

(1) a description of the Department's cybersecurity mission; and

(2) a description and analysis, relating to the specialized workforce needed by the Department to

fulfill the Federal agency's cybersecurity mission, including—

(A) the cybersecurity workforce needs of the Department on the date of the report, and near-, mid-, and long-term projections of workforce needs;

(B) hiring projections to meet cybersecurity workforce needs, including, for at least a 2-year period, specific occupation and grade levels;

(C) long-term and short-term strategic goals to address critical skills deficiencies, including analysis of the numbers of and reasons for attrition of employees;

(D) recruitment strategies to attract highly qualified candidates from diverse backgrounds and geographic locations;

(E) an assessment of the sources and availability of individuals with needed expertise;

(F) ways to streamline the hiring process;

(G) the barriers to recruiting and hiring individuals qualified in cybersecurity and recommendations to overcome the barriers; and

(H) a training and development plan to enhance and improve the knowledge of employees.

(b) TRAINING.—

(1) FEDERAL GOVERNMENT EMPLOYEES AND FEDERAL CONTRACTORS.—The Assistant Secretary for Cybersecurity and Communications shall establish a cybersecurity awareness and education curriculum that shall be required for all Federal employees and contractors engaged in the design, development, or operation of civilian Federal agency computer networks.

(2) CONTENTS.—The curriculum established under paragraph (1) may include—

(A) role-based security awareness training;

(B) recommended cybersecurity practices;

(C) cybersecurity recommendations for traveling abroad;

(D) unclassified counterintelligence information;

(E) information regarding industrial espionage;

(F) information regarding malicious activity online;

(G) information regarding cybersecurity and law enforcement;

(H) identity management information;

(I) information regarding supply chain security;

(J) information security risks associated with the activities of Federal employees; and

(K) the responsibilities of Federal employees in complying with policies and procedures designed to reduce information security risks identified under subparagraph (J).

(c) EDUCATION OPPORTUNITIES.—The Assistant Secretary for Cybersecurity and Communications shall develop and implement a strategy to provide Federal employees who work in cybersecurity-related areas with the opportunity to obtain additional education.

(d) DIRECT HIRE AUTHORITY.—Without regard to the civil service laws (other than sections 3303 and 3328 of title 5, United States Code), the Secretary, acting through the Assistant Secretary For Cybersecurity and Communications, in consultation with the Under Secretary for Management, may appoint not more than 500 employees under this subsection to carry out the requirements of this Act at a rate of pay that may not exceed the maximum rate of basic pay payable under section 5376 of title 5, United States Code, upon certification to the Congress that standard Federal hiring processes have

not resulted in the required number of critical cybersecurity positions being filled.

(e) RETENTION BONUSES.—Notwithstanding section 5754 of title 5, United States Code, the Director may pay a retention bonus under that section to any individual appointed under this section, if the Secretary, acting through Assistant Secretary for Cybersecurity and Communications, in consultation with the Under Secretary for Management, determines that, in the absence of a retention bonus, there is a high risk that the individual would likely leave employment with the Department. The Secretary shall submit a written explanation of this determination to Congress prior to announcing the use of this authority.

○