PROTECTING CYBERSPACE AS A NATIONAL ASSET ACT OF 2010

Homeland Security and Governmental Affairs Committee
Chairman Joe Lieberman
Ranking Member Susan Collins
Senator Carper

Title I – White House Office of Cyberspace Policy

Section 101: This section establishes an Office of Cyberspace Policy within the Executive Office of the President (EOP). The Office will be responsible for developing a national strategy to increase the security and resiliency of cyberspace as well as oversee, coordinate, and integrate all policies and activities of the federal government related to ensuring the security and resiliency of cyberspace.

Section 102: The Office will be headed by a Director who is appointed by the President and confirmed by the Senate. The Director will advise the President on all cyber security matters, work with federal agencies and other EOP offices to ensure the implementation of the national strategy, coordinate efforts by the various federal agencies developing regulations and standards applicable to the national information infrastructure, and resolve any interagency disputes. The Director will also ensure that cyber security policies safeguard privacy and civil liberties.

Section 103: The Director of Cyberspace Policy will be prohibited from participating in political campaigns.

Section 104: The Director of Cyberspace Policy will be required to review each federal agency's budget submission to the Office of Management and Budget (OMB) to determine the adequacy of the request with respect to the implementation of the national strategy and make recommendations to the Director of OMB based on the review.

Section 105: The Director of Cyberspace Policy shall have access to any information possessed by a federal agency that is relevant to cyber security policy.

Section 106: The Director of Cyberspace Policy may consult with any Presidential and other Advisory bodies while executing the responsibilities of the Office.

Section 107: The Director of Cyberspace Policy must submit an annual report to Congress on the activities carried out by the Office of Cyberspace Policy.

Title II -National Center for Cybersecurity and Communications

Section 201: Amends Title II of the Homeland Security Act of 2002 to add the following sections.

Section 241: Definitions.

Section 242: This section establishes a National Center for Cybersecurity and Communications (NCCC or the Center) within the Department of Homeland Security. The Center will be headed by a Director appointed by the President and confirmed by the Senate. The Director will report directly to the Secretary of Homeland Security and serve as the principal advisor to the Secretary on cybersecurity and communications matters. The Director will regularly advise the President on the enforcement of policies pertaining to the security of federal government networks. The Center will have at least two Deputy Directors: one responsible for coordination with the Office of Infrastructure Protection and one responsible for coordination with the Intelligence Community. The Center will also have detailees from the Departments of Defense, Justice, and Commerce as well as the intelligence community and the National Institute of Standards and Technology (NIST). The Center will also benefit from a full-time Chief Privacy Officer who will report to the Director.

The Director will be responsible for leading the federal effort to secure, protect, and ensure the resiliency of the information infrastructure of the United States, including: assisting in the identification, remediation, and mitigation of vulnerabilities; providing dynamic, comprehensive, and continuous situational awareness; conducting risk based assessments; assisting NIST in developing standards; providing agencies mandatory security controls to mitigate and remediate vulnerabilities; developing policies and guidance for federal procurements; assisting with international engagement; overseeing the development, implementation, and management of external access points for federal networks; establishing, developing and overseeing capabilities and operations within the United States Computer Emergency Readiness Team (US-CERT); fostering collaboration with federal, state, and local governments; and overseeing the operations of the National Communications System.

The Director will be required to ensure the Center's activities comply with applicable privacy and civil liberties laws.

The Director also may analyze the budgets of other federal agencies and make recommendations to OMB and the White House Office of Cyberspace Policy regarding the adequacy of the proposed budgets to secure federal networks.

The Director of OMB is required to submit to Congress a report detailing the resources and personnel necessary to establish the Center and carry out its mission. The Government Accountability Office will review the plan.

Section 243: This section requires coordination between the Director of the Center and the Assistant Secretary for Infrastructure Protection.

Section 244: This section codifies the United States Computer Emergency Readiness Team (US-CERT) within the NCCC. US-CERT will be responsible for the collection, coordination, and dissemination of information regarding risks to the federal information infrastructure and the enhancement of security of the federal information infrastructure and the national information infrastructure. US-CERT will be the primary point of contact within the NCCC for other federal agencies, state and local governments, and the private sector.

US-CERT also has responsibilities relating to monitoring, analysis, warning, and response. Under this rubric, US-CERT will provide analysis and report to federal agencies on the security of their networks; provide continuous, automated monitoring of the federal information infrastructure at the external access points; develop, recommend, and deploy security controls; support federal agencies in conducting risk assessments; develop predictive analysis tools; and aid in the detection of and warn owners/operators of the national information infrastructure regarding risks.

To facilitate information sharing with other federal agencies, US-CERT will designate a principal point of contact for each federal agency in order to maintain communication and respond to inquiries or requests.

The establishment of the NCCC does not absolve the head of each federal agency of their existing responsibility to secure their agency's networks, as described in Title III of this Act (or Sect 3353 of title 44).

Section 245: The Director of the NCCC shall have access to any information possessed by a federal agency that is relevant to the execution of the responsibilities of the position.

The Director of the NCCC may conduct risk-based operational evaluations (known as "red teaming" and "blue teaming") to evaluate the security of the federal information infrastructure. If the Director determines through the operational evaluation that a federal agency is not in compliance with federal guidelines, the Director, working in conjunction with the head of the agency, may direct implementation of corrective measures and mitigation plans. If the agency fails to take the directed corrective measures and this failure presents a significant risk to the Federal information infrastructure, the Director may direct the isolation of the agency's information infrastructure, consistent with the contingency or continuity of operations applicable to that agency, until the agency takes necessary corrective measures.

Section 246: The Director of the NCCC is responsible for developing information sharing programs between and among federal agencies, state and local governments, the private sector, and international partners. The Center will establish policies and procedures for sharing classified and unclassified information relevant to the security of the federal and national information infrastructure, including threats, vulnerabilities, incidents, anomalous activities. The policies and procedures will establish mechanisms for sharing the information, offer guidance on what information should be shared, and protect the information from disclosure.

Owners and operators of covered critical infrastructure will be required to report to the NCCC breaches of their networks that could lead to the disruption of the critical function(s) of the covered critical infrastructure. The bill, however, explicitly clarifies that this requirement does not affect the requirements of the Wiretap Act, the Electronic Communications Privacy Act, or the Foreign Intelligence Surveillance Act.

Section 247: The Director of the NCCC will regularly engage with standards setting bodies to encourage the development of, and recommend changes to, cyber security standards and guidelines. The Director will also establish a program to promote cyber security best practices

and provide technical assistance relating to the implementation of best practices, and related standards and guidelines, for securing the national information infrastructure. To the extent practicable, these best practices should be based on existing standards developed by the private sector or standard setting bodies.

Section 248: The Director of the NCCC will work with the private sector and relevant sector-specific agencies to identify and evaluate cyber vulnerabilities to covered critical infrastructure on a sector-by-sector basis. The Director will submit the findings to Congress within 120 days.

The Director of the NCCC will then work with the private sector and relevant sector-specific agencies to issue interim final regulations establishing risk-based security performance requirements to secure the covered critical infrastructure against the identified cyber vulnerabilities. Owners and operators of the covered critical infrastructure will be informed of identified vulnerabilities, select security measures that satisfy the security performance requirement, and submit a plan to the Director detailing how they will meet the performance requirements. Owners and operators will have the flexibility to implement any security measure that the Director determines satisfies the security performance requirements. The Director, however, will not have the authority to mandate that the plans include any specific security measure – only that the plans meet the mandatory security performance requirements. The Director will also work with owner and operators of covered critical infrastructure outside the United States to inform them of cyber vulnerabilities and appropriate security measures.

Section 249: If the President determines there is a credible threat to exploit cyber vulnerabilities of the covered critical infrastructure, the President may declare a national cyber emergency, with notification to Congress and owners and operators of affected covered critical infrastructure. The notification must include the nature of the threat, the reason existing security measures are deficient, and the proposed emergency measures needed to address the threat. If the President exercises this authority, the Director of the NCCC will issue emergency measures necessary to preserve the reliable operation of covered critical infrastructure. Any emergency measures issued under this section will expire after 30 days unless the Director of the NCCC or the President affirms in writing that the threat still exists or the measures are still needed. Emergency measures imposed by the Director must be the least disruptive means feasible, and such emergency measures cannot be used to set aside the requirements of the Wiretap Act, the Electronic Communications Privacy Act, or the Foreign Intelligence Surveillance Act of 1978. This section does not authorize any new surveillance authorities or permit the government to "take over" private networks. While complying with the mandatory emergency measures, owners and operators of covered critical infrastructure will have the flexibility to propose alternative security measures that address the national cyber emergency and, once approved by the Director, implement those security measures in lieu of the original mandatory emergency measures.

Owners and operators of covered critical infrastructure who comply with the requirements can in certain circumstances receive liability protections that range from limitations on some damages to immunity from suit.

The Director will also work with owner and operators of covered critical infrastructure outside the United States to inform them of cyber threats and vulnerabilities and appropriate security measures.

Section 250: Once regulations have been promulgated, on an annual basis, the owners and operators of the covered critical infrastructure shall certify in writing to the Director of the NCCC that they are in compliance with the security measures. The Director may perform risk-based evaluations of the covered infrastructure to determine compliance. Any failure to comply may result in civil penalties.

Owners and operators of covered critical infrastructure who are in compliance with the security performance requirements can in certain circumstances receive specified liability protection.

Section 251: Information submitted by the private sector to the NCCC under the information sharing improvements established by the bill will be protected from public disclosure. The Director of the NCCC shall develop guidelines detailing how relevant information, including information regarding threats, vulnerabilities, and incidents, will be shared with appropriate government and private sector partners as necessary to implement this Act. This section does not abrogate existing disclosure. Except as expressly provided, this provision does not alter the obligation of any entity to provide information pursuant to another law or regulation.

Section 252: The heads of each sector-specific agency and the heads of other federal agencies with responsibilities for regulating the covered critical infrastructure will be required to coordinate with the Director of the NCCC on activities related to the security and resiliency of the national information infrastructure. Efforts should be made to avoid duplication in reporting requirements. These agencies will also be required to coordinate with the Director prior to establishing any requirements or other measures related to the security of the national information infrastructure to ensure, to the maximum extent practicable, that the Federal government takes a coordinated approach to any regulations or other matters related to cybersecurity.

Section 253: The Secretary of DHS, with other federal agencies and industry, will be required to develop, update, and implement a supply chain risk management strategy that will ensure the security of the communications and information technology products and services purchased by the federal government. The Federal Acquisition Regulatory Council will be required to amend the Federal Acquisition Regulation to implement the supply chain risk management strategy and to direct that all software and hardware purchased by the federal government provide additional security.

Title III – FISMA Reform

Section 301: Amends the Federal Information Security Management Act of 2002 (FISMA) by striking subchapters II and III of chapter 35 of title 44 USC and inserting the following sections. Many of the original FISMA requirements are retained in this language.

Section 3550: This section states that the purpose of Title III is to provide a comprehensive risk-based framework that enhances the effectiveness of information security controls in the federal information infrastructure; recognize the highly networked nature of the current federal information infrastructure environment; and provide for the development and maintenance of controls required to protect the federal information infrastructure.

Section 3551: Definitions.

Section 3552: This section tasks the Director of the NCCC with the responsibility for developing, overseeing, and enforcing information security throughout the federal government. In the past, the OMB Office of Electronic Government and Information Technology has executed this responsibility.

Specifically, the Director of the NCCC is responsible for providing agencies prioritized risk-based security controls that will mitigate and remediate vulnerabilities, attacks, and exploitations. In addition, this section requires the Director of the NCCC to ensure agencies are in compliance with government-wide policies and to review no less than annually whether agency information security programs are effective.

Section 3553: In general, this section requires agency heads to follow the policy of the NCCC and for each agency to develop and maintain an effective risk-based information security program. In order to accomplish this, the head of each agency is responsible for delegating to a senior official, known as a Chief Information Security Officer (CISO) the authority to develop, oversee, and enforce risk-based information security policies that are integrated with the strategic and operational processes of the agency. The CISO's authority extends to the entire department, including contractors operating on behalf of the agency.

This section also emphasizes the fact that attacks come at light-speed and that CISOs should be highly qualified cyber security experts and – to the extent possible – automate their defenses to detect, report, and respond to security incidents. The section shifts resources away from the current wasteful, paperwork-laden compliance process required by the the current law and puts the emphasis on active detection and prevention of threats.

Specifically, each agency will be required to have an agency-wide security program, including all subcomponents of an agency, that is approved by the NCCC and must include: risk-based vulnerability assessments and penetration tests on agency networks; procedures to ensure that information security vulnerabilities are remediated in a timely fashion; role-based security awareness training for employees; automated and continuous monitoring of network defenses; and plans and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency. This section allows CISOs to require more stringent standards above and beyond those required by the Director of the NCCC.

If an incident does occur and information or an information system is compromised, this section explicitly requires that CISOs will be responsible for mitigating and remediating risks associated with known penetrations before substantial damage is done and to report any incidents to the appropriate authorities.

Finally, this section requires each agency to submit an annual report on the effectiveness of their information security program to Congress, the Government Accountability Office, and the NCCC.

Section 3554: This section requires each agency to conduct annual operational evaluations, also known as "red-teaming" and "blue-teaming", to test an agency's information security program developed under Section 3553. The operational evaluations will be overseen by the Director of the NCCC and prioritized based on risk.

Following an operational evaluation, the CISO of the agency will have to submit a risk-based corrective action plan to the Director of the NCCC for mitigating and remediating any vulnerabilities identified as a result of the evaluation. The Director of the NCCC will have fifteen days upon receipt of the plan to approve, disapprove, and comment on the effectiveness of the plan. If the Director approves the plan, then the agency head must ensure that the plan is effectuated.

In the unlikely event that an operational evaluation brings to light severe deficiencies which represent a significant danger to the federal information infrastructure, then the Director of the NCCC may order the isolation of any system from the federal information infrastructure, consistent with the contingency or continuity of operations applicable to that agency, until the agency takes necessary corrective measures.

Section 3555: This section will establish a Federal Information Security Taskforce within the executive branch. The Taskforce will be headed by the Director of the NCCC and be comprised of the Administrator of the Office of Electronic Government; the CISO of every agency; the CISOs of the Army, Navy, and Air Force; representatives from the Office of the Director of National Intelligence, US-CERT, the Intelligence Community Incident Response Center, the Committee on National Security Systems, NIST, State and local government, and any other person designated by the chairperson.

The Federal Information Security Taskforce will serve as the principal interagency forum for agencies to develop and share best practices for enhancing the security of their systems and networks. The Taskforce will be the vehicle through which the Director of the NCCC establishes policies and guidelines to conduct operational evaluations required under Section 3554. In addition, the Taskforce will promote the development and use of standard performance measures for agency information security that are outcome-based, focus on risk management, align with business and program goals of the agency, measure improvements over time, and reduce burdensome compliance measures.

The Taskforce will terminate after four years unless extended by Executive Order or an act of Congress.

Title IV – Federal Workforce

Section 401: Definitions.

Section 402: This section requires the Director of the Office of Personnel Management (OPM) to assess the readiness and capacity of the federal workforce to meet the needs of the cybersecurity mission of the federal government. Within 180 days, the Director of OPM shall develop and implement a comprehensive workforce strategy that includes a five-year plan on recruitment of personnel and ten- and twenty- year projections on workforce needs.

Section 403: This section requires the head of each federal agency to develop a strategic cybersecurity workforce plan which details how the agency plans to recruit, hire, and train necessary cybersecurity personnel.

Section 404: This section requires the Director of OPM to develop and issue comprehensive occupation classifications for federal employees engaged in the cybersecurity mission. The Director of OPM shall ensure that the classifications may be used throughout the federal government.

Section 405: The head of each agency will be required to develop a system to measure the effectiveness the agency's recruitment and hiring program.

Section 406: The Director of OPM will be required to establish a cybersecurity awareness program for all federal employees and federal contractors and a program to provide training to improve the technical skills and capabilities of federal employees engaged in the cybersecurity mission.

The Director of OPM will be required to develop and implement a strategy to provide federal employees who work in cybersecurity missions with the opportunity to obtain additional education at the expense of the government. The Director will also develop strategies and programs to recruit students from undergraduate, graduate, vocational, and technical institutions to serve as federal employees working in cyber missions. Finally, the Director of OPM will provide internships and part-time work opportunities for students from the above institutions.

The Secretary of Education, working with state and local governments, will be required to develop curriculum standards, guidelines, and recommended courses to address cyber safety, cybersecurity, and cyber ethics for students in kindergarten through grade twelve as well as undergraduate, graduate, vocational, and technical institutions.

The Director of the NCCC will be required to establish a program to advance national and statewide cyber competitions and challenges that can identify talented individuals and encourage them to pursue careers in cybersecurity.

Section 407: This section requires that when the President or the head of agency awards bonuses to recognize an employee, they must consider the success of that employee in fulfilling the objectives of the National Strategy. The head of an agency must also adopt best practices regarding effective ways to educate and motivate employees to demonstrate leadership in cybersecurity.

Section 408: This section would provide hiring and pay flexibilities to the Director of the NCCC to help establish and grow the Center including: the authority to directly appoint up to 500 cybersecurity specialists into the competitive service; the authority to grant competitive status to individuals previously appointed to an excepted service position; the authority, with the direct approval of the Director of the NCCC, to pay up to 20 employees a salary up to level I of the Executive Schedule and, with the direct approval of the Secretary of Homeland Security, up to 5 employees a salary up to that of the Vice President; the authority to offer retention bonuses to cybersecurity specialists likely to leave the Department for another federal agency; and the authority to pay entry-level employees a salary higher than currently designated for their position on the General Schedule. These authorities will sunset after 3 years.

Title V – Additional DHS Provisions

Section 238: This section directs the DHS Under Secretary for Science and Technology to carry out a research and development program to improve the security of the nation's information infrastructure.

Section 239: This section directs the Secretary of Homeland Security to establish a private sector advisory committee which will be known as the National Cybersecurity Advisory Council. The Council will advise the Director of the Center on the implementation of cybersecurity provisions affecting the private sector. Members of the Council will be appointed by the Director and include representatives of the covered critical infrastructure; academic institutions with expertise in cybersecurity; federal, state, and local government agencies with expertise in cybersecurity; and a representative of the National Security Telecommunications Advisory Council, the Information Technology Sector Coordinating Council, and the Communications Sector Coordinating Council.

Section 503: The Secretary of Homeland Security will be required to consider cyber vulnerabilities and consequences, including interdependencies between components of the covered critical infrastructure, when establishing and maintaining a list of the covered critical infrastructure. The Secretary may add covered critical infrastructure to, or delete covered critical infrastructure from, the list based on the consideration of cybersecurity. The Secretary will notify the owner or operator of the system or asset added to the list as soon as practicable and afford it the opportunity to provide information pertaining to its addition to the list.

Section 504: The NCCC will have additional procurement authorities to execute its cybersecurity mission. Specifically, NCCC will be granted the same flexibilities already available to the Department of Defense, NASA and the Coast Guard for procurements that may be satisfied by only a limited number of responsible sources, or for follow-on contracts for the continued provision of highly specialized services. The authorities granted under this section will terminate three years after the date of enactment of this Act. The Director is required to report on a semiannual basis to Congress on the use of the authority granted under this section.