Calendar No. 707

111TH CONGRESS *2d Session*	SENATE	REPORT 111–384

CYBERSECURITY ACT OF 2010

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 773

DECEMBER 22, 2010.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
99–010 WASHINGTON : 2010

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUYE, Hawaii
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
MARK PRYOR, Arkansas
CLAIRE MCCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
TOM UDALL, New Mexico
MARK WARNER, Virginia
MARK BEGICH, Alaska

KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
JOHN ENSIGN, Nevada
JIM DEMINT, South Carolina
JOHN THUNE, South Dakota
ROGER F. WICKER, Mississippi
GEORGE S. LEMIEUX, Florida
JOHNNY ISAKSON, Georgia
DAVID VITTER, Louisiana
SAM BROWNBACK, Kansas
MIKE JOHANNS, Nebraska

ELLEN DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
BRUCE ANDREWS, *General Counsel*
ANN BEGEMAN, *Republican Staff Director*
BRIAN HENDRICKS, *Republican General Counsel*
TODD BERTOSON, *Republican Senior Counsel*

Calendar No. 707

111TH CONGRESS *2d Session* | SENATE | REPORT 111–384

CYBERSECURITY ACT OF 2010

DECEMBER 22, 2010.—Ordered to be printed

Mr. ROCKEFELLER, from the Committee on Commerce, Science, and Transportation, submitted the following

REPORT

[To accompany S. 773]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 773) to enhance the security of the information infrastructure of the United States, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends that the bill (as amended) do pass.

PURPOSE OF THE BILL

The purpose of S. 773, The Cybersecurity Act of 2010, is to strengthen the security of American information infrastructure by expanding the information security workforce, establishing authorities for the Federal government, and enhancing public-private collaboration.

BACKGROUND AND NEEDS

Information and communications technology (ICT) is essential for the day-to-day operations of companies, organizations, and government. Companies large and small increasingly rely on ICT to support diverse business processes, ranging from payroll and accounting to inventory tracking and management. Critical national infrastructure—such as energy, banking and finance, defense, law enforcement, water systems, and transportation systems—all depend on ICT to maintain daily operations. To allow for near real-time exchanges of information, money, goods, and services all across the globe, ICT systems are increasingly linked to each other through the Internet.

While open systems connected to the Internet provide great societal benefits, owners and operators place the confidentiality, integrity, and availability of their information and information systems at risk by connecting to the Internet. Every day, millions of attacks are launched against public and private sector computers. Attackers seek a variety of things, from money, to information, to destruction. The success of the attack depends on both the skill level of the attacker and the sophistication of the defender. Unfortunately for defenders, automated tools available online provide an added boost for lesser-skilled attackers.

As the most connected nation in the world, the United States is also the most vulnerable. Former Director of National Intelligence Michael McConnell testified at a Committee hearing in 2009 that, "If we [the U.S.] went to war today in a cyberwar, we would lose. We're the most vulnerable, we're the most connected, we have the most to lose."[1] Public and private sector computer networks within the U.S. are increasingly subject to attack. According to the U.S. Computer Emergency Readiness Team, Federal civilian agencies reported a total of 18,050 cyber incidents in Fiscal Year (FY) 2008, compared with 12,986 in FY 2007, and 5,144 in FY 2006.[2] During 2008, there were 54,640 identified attacks against the Department of Defense; in 2009, there were 71,661 incidents reported; and through June 30 of 2010, there were 60,026 incidents reported.[3]

Data theft and breaches from cyber crime may have cost businesses as much as $1 trillion globally in lost intellectual property and expenditures for repairing damage in 2008.[4] According to a group of 500 global information technology corporations, companies spend an average of $600,000 responding to each security breach leading to the loss of vital information.[5] Because of sophisticated tradecraft and inconsistent reporting, however, the total number of attacks is unknown.

The private sector owns a large percentage of the nation's critical infrastructure, including electricity generation and transmission, water and sewer treatment facilities, and financial markets and clearinghouses. The computers that run these systems are often interconnected and subject to the same potential attacks as other networks. Experts suggest that cyber attacks against critical infrastructure potentially could physically destroy infrastructure, depriving large populations of essential goods and services for extended periods of time and threatening lives.

The Department of Homeland Security (DHS) is responsible for securing cyberspace and critical infrastructure under Homeland Security Presidential Directive 7. Specifically, DHS is responsible for: developing a comprehensive national plan for critical infrastructure protection; developing and enhancing national cyber analysis and warning capabilities; providing and coordinating incident response

---

[1] McConnell, Michael (former Director of National Intelligence). Quote from Hearing of the Senate Committee on Commerce, Science, and Transportation. "Cybersecurity: Next Steps to Protect Our Critical Infrastructure." 23 Feb. 2010.

[2] Bain, Ben. "Number of Reported Cyber Incidents Jumps." Federal Computer Week. 17 Feb. 2009. Web. http://fcw.com/Articles/2009/02/17/CERT-cyber-incidents.

[3] Report to Congress. U.S.-China Economic and Security Review Commission. 29 Oct. 2010. Web. http://www.uscc.gov/annual—report/2010/annual—report—full—10.pdf

[4] Study: Cybercrime cost firms $1 trillion globally, Elinor Mills, 28 Jan. 2009. Web. http://news.csnet.com. While S. 773 is focused on the cybersecurity of critical infrastructure information systems, rather than cybercrime, these statistics underscore the vulnerability of ICT systems to cyber attacks.

[5] Unsecured Economies: Protecting Vital Information, McAfee, Inc., Jan. 2009, page 3.

and recovery planning, including conducting incident response exercises; identifying, assessing, and supporting efforts to reduce cyber threats and vulnerabilities, including those associated with infrastructure control systems; and strengthening international cyberspace security. However, a number of reports demonstrate that DHS has not been fully effective in improving cybersecurity throughout the private sector. For example, in 2006, DHS issued guidance for agencies to develop sector-specific plans for protecting cyber and physical critical infrastructure. Agencies issued plans in 2007, but the Government Accountability Office (GAO) found that none fully addressed all cyber-related criteria. DHS asked for the plans to be updated in 2008, but a September 2009 GAO report found limited progress.[6]

The U.S. cybersecurity workforce—comprised significantly of students who excel at science and engineering—is insufficient to meet the cyber threat. For nearly five decades, the domestic science and engineering workforce has grown faster than the total civilian workforce, reaching about 5.5 million in 2007. However, undergraduate and graduate degrees in computer sciences have declined since 2004, back to the levels observed in 2000.[7] In addition, an increasing proportion of computer science degrees granted in this country are awarded to foreign nationals, often from China and India. Competitiveness aside, many are concerned with the limited pool of properly educated U.S. citizens who maintain an ability to obtain security clearances at the highest levels.

When it comes to specializations in cybersecurity, the situation worsens. According to the President's Information Technology Advisory Committee (PITAC), there currently are fewer than 250 active cybersecurity specialists at U.S. academic institutions, and the nation's cybersecurity research community is too small to adequately support the cybersecurity research and education programs necessary to protect the country. The PITAC thus recommended an intense effort to promote the recruitment and retention of cybersecurity researchers and students at research universities with a goal of at least doubling the size of the civilian cybersecurity fundamental research community by the end of the decade.[8]

Though technology has changed significantly in the last decade, America's fundamental policies and strategies for addressing the cyber threat have not. The "National Strategy to Secure Cyberspace" was drafted in 2002, and has not been updated or revised since. Many people, including independent commissions, independent oversight bodies, and knowledgeable observers, have suggested that the time for a new strategy, vision, and plan for national cybersecurity is past due. This legislation seeks to address these and other information security issues in a comprehensive format.

---

[6] GAO-09-969, Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment. Sept. 2009.

[7] Science and Engineering Indicators 2010. National Science Board.

[8] Report to President. President's Information Technology Advisory Committee. Cyber Security: A Crisis of Prioritization. Virginia: The Commission. Web. 7 December 2010. http://www.nitrd.gov/pitac/reports/20050301—cybersecurity/cybersecurity.pdf

SUMMARY OF PROVISIONS

The primary goal of the Cybersecurity Act of 2010 is to modernize the public-private sector relationship on cybersecurity. As vast majority of our Nation's networks are owned and operated by the private sector, securing cyberspace must be a collaborative effort between our Government and the private sector. Reactive, ad hoc responses to the cyber threat leave our country, our businesses, and our civil liberties at risk. The Cybersecurity Act of 2010 would provide a framework for proactive engagement, collaboration, and teamwork between the government and the private sector on cybersecurity.

The bill would raise the priority of cybersecurity throughout the Federal government and streamline cybersecurity-related government functions, authorities, and laws. The bill would protect civil liberties, intellectual property, and businesses' proprietary information, while promoting cybersecurity public awareness, education, and research and development. The bill would foster market-driven cybersecurity innovation and creativity to develop long-term technology solutions and train the next generation of cybersecurity professionals.

Sections 101 and 204 would bolster market incentives for innovation and excellence in cybersecurity professional training and cybersecurity products and services by encouraging, coordinating, and building on private sector initiatives. They are intended to create a dynamic, ever-improving cycle of market-driven innovation—not a static checklist administered by a slow-moving bureaucracy. Section 208 would place the purchasing power of the Federal government behind these innovations by requiring them to be part of every Federal contract for information technology (IT) products and services. These sections would require the President to collaborate with private sector critical infrastructure companies to identify the world's best private sector training programs and industry best practices for IT products and services. Then, they would require those same companies to report the results of independent audits of their compliance with these standards—their own standards. These sections also call for collaborative remediation of persistent vulnerabilities. In practice, this would effectively be a government-coordinated, private sector intervention to prevent a company that has failed consecutive audits from damaging the entire industry sector—and the country's security along with it.

Sections 201 and 403 would require a collaborative effort to promote effective, well-coordinated, government-private sector teamwork—and protect civil liberties, proprietary rights, and confidential and classified information—before, during, and after a cybersecurity emergency. Section 201 would require the President to collaborate with owners and operators of critical infrastructure information systems, through existing partnerships, to develop and rehearse detailed cybersecurity emergency response and restoration plans. The explicit purpose of this section is to clarify roles, responsibilities, and authorities of government and private sector actors in the event of a cybersecurity emergency that threatens strategic national interests. The President's declaration of a cybersecurity emergency would trigger the implementation of the collaborative emergency response and restoration plans. Section 201 states ex-

plicitly that nothing in the section authorizes new or expanded Presidential authorities—it simply seeks to avoid the type of dangerous bureaucratic confusion witnessed in the aftermath of Hurricane Katrina. To establish greater accountability for the President's actions during a declared emergency, the section would also require the President to report to Congress in writing, within 48 hours of the declaration, regarding the circumstances necessitating the declaration, and the estimated scope and duration of the emergency.

Section 403 would complement this emergency response provision by creating a public-private information sharing clearinghouse in which government and private officials would share classified and/or confidential cybersecurity threat and vulnerability information. This would allow incidents to be handled in real-time, or prevent them from occurring altogether.

LEGISLATIVE HISTORY

Senators Rockefeller and Snowe introduced S. 773 on April 1, 2009. The legislation was referred to the Committee, and included Senator Nelson (of Florida) as an original cosponsor. The bill is also cosponsored by Senators Bayh and Mikulski.

Chairman Rockefeller held two hearings on cybersecurity at the full committee level. The first, held on March 19, 2009, was titled "Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response," and the Committee heard from: Dr. James A. Lewis, Director and Senior Fellow, Center for Strategic and International Studies (CSIS); Dr. Joseph Weiss, Managing Partner, Applied Control Solutions, LLC; Dr. Edward G. Amoroso, Chief Security Officer, AT&T; and Dr. Eugene H. Spafford, Professor and Executive Director of the Center for Education and Research in Information Assurance and Security, Purdue University.

The second hearing was held on February 23, 2010, and was titled "Cybersecurity: Next Steps to Protect Our Critical Infrastructure." At this hearing, witnesses included: Vice Admiral Michael McConnell (USN, Ret.), Executive Vice President, Booz Allen Hamilton and former Director of National Intelligence; Dr. James A. Lewis, Director and Senior Fellow, CSIS; Dr. Scott Borg, Director and Chief Economist, U.S. Cyber Consequences Unit; Rear Admiral James Arden Barnett Jr. (USN, Ret.), Chief, Public Safety and Homeland Security Bureau, Federal Communications Commission (FCC); and Ms. Mary Ann Davidson, Chief Security Officer, Oracle Corporation.

On March 24, 2010, the Committee met in Executive Session, during which S. 773 was considered with an amendment in the nature of a substitute. The committee adopted amendments offered by Senators Hutchison, Cantwell, Klobuchar, Udall, and Warner. The bill, as amended, was ordered reported by voice vote.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

S. 773—Cybersecurity Act of 2010

Summary: S. 773 would authorize several National Science Foundation (NSF) grant and scholarship programs aimed at enhancing cybersecurity (the protection of computers and computer networks from unauthorized access) through expanded research and workforce development. The bill also would authorize the National Institute of Standards and Technology (NIST) to carry out certain activities to promote the development of new cybersecurity technologies and to enhance public awareness of cybersecurity issues. In addition, the bill would direct the President to develop and implement a comprehensive cybersecurity strategy for the federal government. Finally, the legislation would codify certain ongoing activities related to cybersecurity.

Assuming appropriation of the necessary amounts, CBO estimates that implementing S. 773 would cost $1.4 billion over the 2011–2015 period. Pay-as-you-go procedures do not apply to this legislation because it would not affect direct spending or revenues.

S. 773 would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), on owners and operators of information systems designated as critical infrastructure by the President. Owners and operators of such systems would have to comply with new security standards and procedures. Because the number of entities subject to the mandates would be large, and the costs of complying with some of the mandates in the bill would be substantial, CBO estimates that the costs to comply would well exceed the annual thresholds established in UMRA for intergovernmental and private-sector mandates ($70 million and $141 million in 2010, respectively, adjusted annually for inflation).

CBO has not reviewed section 201(b) of the bill for mandates. Section 4 of UMRA excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that the provisions of section 201(b) fall within that exclusion because they would allow the President to declare a cybersecurity emergency and implement emergency-response and restoration plans.

Estimated cost to the Federal Government: The estimated budgetary impact of S. 773 is shown in the following table. The costs of this legislation fall within budget functions 250 (general science, space, and technology), 370 (commerce and housing credit), and 800 (general government).

	By fiscal year, in millions of dollars—					
	2011	2012	2013	2014	2015	2011–2015
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
National Science Foundation Activities:						
Authorization Level	339	356	371	388	0	1,454
Estimated Outlays	61	210	295	338	297	1,201
Department of Commerce Activities:						
Estimated Authorization Level	38	48	58	68	8	220
Estimated Outlays	20	34	44	55	45	198
Other Activities:						
Estimated Authorization Level	7	6	6	6	6	31
Estimated Outlays	6	6	6	6	6	30
Total Spending Under S. 773:						
Estimated Authorization Level	384	410	435	462	14	1,705

	By fiscal year, in millions of dollars—					
	2011	2012	2013	2014	2015	2011–2015
Estimated Outlays	87	250	345	399	348	1,429

Basis of estimate: For this estimate, CBO assumes that the legislation will be enacted in 2010 and that the necessary amounts will be appropriated for each fiscal year. Estimated outlays are based on historical spending patterns for similar programs.

National Science Foundation activities

S. 773 would authorize appropriations totaling about $1.2 billion over the 2011–2014 period for several existing NSF programs related to cybersecurity research. The bill also would authorize the appropriation of $250 million over that period for the agency to provide scholarships to students who pursue higher education in fields related to cybersecurity. Finally, the bill would authorize the appropriation of $2 million a year over the 2011–2012 period to provide grants for higher education institutions to develop cybersecurity curricula. Based on information from NSF and assuming appropriation of the authorized amounts, CBO estimates that implementing the NSF programs authorized under the bill would cost $1.2 billion over the 2011–2015 period.

Department of Commerce activities

S. 773 would authorize the appropriation of $15 million a year over the 2011–2014 period for NIST to award cash prizes to individuals who develop innovative cybersecurity technologies. The bill also would require the agency to establish regional cybersecurity centers that would assist businesses in implementing cybersecurity best practices. In addition, the legislation would require NIST to establish a program to promote cybersecurity awareness and education. Finally, the bill would require the Secretary of Commerce to develop a tracking system to provide the real-time cybersecurity status of all federal agencies within the Department of Commerce. Based on information regarding the cost of implementing similar programs, CBO estimates that carrying out the provisions affecting the Department of Commerce would cost $198 million over the 2011–2015 period, assuming appropriation of the authorized and necessary amounts.

Other activities

S. 773 would direct the President to establish a national cybersecurity strategy and to conduct biennial reviews to assess the nation's cybersecurity posture. The legislation also would require the President to appoint a panel of academic and industry experts to advise the Office of Science and Technology Policy on issues related to cybersecurity. Finally, the bill would require a study by the National Academies to assess workforce development efforts related to cybersecurity. Based on information regarding the cost of similar activities, CBO estimates that implementing those provisions would cost $30 million over the 2011–2015 period.

Pay-as-you-go considerations: None.

Mandates that apply to both intergovernmental and private-sector entities

Intergovernmental and private-sector impact: S. 773 would impose intergovernmental and private-sector mandates, as defined in UMRA, on owners and operators of information systems designated as critical infrastructure by the President. Critical infrastructure could include information systems for public and private transportation systems, police and fire departments, airports, hospitals, electric utilities, health departments, water systems, and financial companies.

The bill would require those entities to:

- Train employees working in cybersecurity to meet new certification requirements;
- Comply with risk-management techniques and best practices to be established for cybersecurity; and
- Audit their compliance with those requirements on a semiannual basis and report the results of those audits to the federal government.

The costs of complying with the mandates would depend on future regulations, the extent to which the regulations would impose requirements that differ from current practice, and which entities would be subject to those requirements. Based on information from industry sources, the cost of conducting a cybersecurity audit could range from $30,000 to millions of dollars per entity, depending on the size of the entity and the nature and scope of the audit. For example, such an audit could involve ensuring compliance with firewall, encryption, and data storage and transfer requirements, among other risk-management techniques. Based on information from government and industry sources, more than 50,000 public entities could be subject to the mandates. Further, according to a study by the Government Accountability Office, the private sector owns more than 85 percent of the nation's critical infrastructure. Because the number of entities subject to the mandates could be large and the costs of complying with some of the mandates in the bill would be substantial, CBO estimates that the aggregate costs to comply would well exceed the annual thresholds established in UMRA for intergovernmental and private-sector mandates ($70 million and $141 million in 2010, respectively, adjusted annually for inflation).

Provisions excluded under UMRA

CBO has not reviewed section 201(b) of the bill for mandates. Section 4 of UMRA excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined the provisions of section 201(b) fall within that exclusion because they would allow the President to declare a cybersecurity emergency and implement emergency-response and restoration plans.

Other impacts on State and local governments

The bill would benefit public institutions of higher education by authorizing grants for cybersecurity programs. Any costs that those entities incur would result from complying with conditions of federal assistance.

Previous CBO estimate: On December 10, 2009, CBO transmitted a cost estimate for H.R. 4061, the Cybersecurity Enhancement Act of 2009, as ordered reported by the House Committee on Science and Technology on November 18, 2009. S. 773 contains several provisions that were included in H.R. 4061; however, the authorization levels for those provisions are different. In addition, S. 773 contains additional provisions that were not included in H.R. 4061. The CBO cost estimates reflect those differences.

Estimate prepared by: Federal Costs: Jeff LaFave; Impact on State, Local, and Tribal Governments: Elizabeth Cove Delisle; Impact on the Private Sector: Samuel Wice.

Estimate approved by: Peter H. Fontaine, Assistant Director for Budget Analysis.

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

Private entities designated as CIIS under section 4 of the bill would be covered by the requirements of sections 101, 201, and 204. CBO has estimated that the number of covered entities could be large, but the number is difficult to calculate in advance of the rulemaking required by section 4.

ECONOMIC IMPACT

S.773 would authorize $384 million in FY 2011, $410 million in FY 2012, $435 million in FY 2013, $462 million in FY 2014, and $14 million for FY 2015 in appropriations to the National Science Foundation, Department of Commerce, and the President. These funding levels are not expected to have a significant impact on the nation's economy. Owners and operators of CIIS would face compliance costs with new cyber security standards and related audits; however, the impact of these costs could vary, as some entities may already be acting consistently with the standards. Moreover, compliance with the new standards should help to prevent or mitigate economic losses from cyber attacks. The bill's investments in research and education should also have a positive impact on the nation's competitiveness.

PRIVACY

The bill would have little, if any, impact on the personal privacy of individuals.

PAPERWORK

The bill would create paperwork requirements for owners and operators of CIIS through the semi-annual audits established in sections 101 and 204. The owners and operators of CIIS would also be required to develop and annually update guidance for the identification of cybersecurity personnel and requirements for their certification. The bill would also require several plans, strategies, and reports from the Federal government. Section 104 would require the head of each Federal agency to complete an annual cybersecu-

rity workforce plan, with hiring projections available on the agency's website. Section 105 would require each Federal agency to measure the effectiveness of its cybersecurity hiring efforts, with the results reported annually to Congress and the public. Section 201 would require the President to develop and implement a national cybersecurity strategy in collaboration with relevant stakeholders. Should the President declare a cybersecurity emergency as defined in the national strategy, the President would then be required to report to Congress in writing, within 48 hours of the declaration, regarding the circumstances necessitating the declaration and its estimated scope and duration. Section 202 would require a biennial review of the U.S. cyber program, modeled after the DoD's Quadrennial Defense Review. Section 204 would require NIST to review and update cyber audit plans on at least a semi-annual basis. The section would also require the FCC to report to Congress on effective and efficient means to ensure the cybersecurity of commercial broadband networks with an additional supplement to its National Broadband Plan. Section 205 would require the GAO to complete a comprehensive review of the Federal statutory and legal framework applicable to cybersecurity, with recommendations regarding changes needed to advance cybersecurity and protect civil liberties. Section 210 would require the President to report to Congress on the feasibility of an identity management and authentication program with appropriate civil liberties and privacy protections. Section 211 would require NIST to issue a public report assessing the strategies and best practices for identity authentication, with specific attention paid to health information applications. Section 401 would require the President to establish or designate a Cybersecurity Advisory Panel, which would then provide a report to the President every two years with recommendations on how the Federal cybersecurity effort should be improved. Section 404 would require the President to report to Congress on the feasibility of a cybersecurity risk management market, including the potential role of civil liability and insurance. The bill would also establish or enhance several grant programs, for which applicants would have to file documents to apply. Key owners and operators of CIIS, as identified in section 209, could be required to file documents in the security clearance process.

CONGRESSIONALLY DIRECTED SPENDING

In compliance with paragraph 4(b) of rule XLIV of the Standing Rules of the Senate, the Committee provides that no provisions contained in the bill, as reported, met the definition of congressionally directed spending items under the rule.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title; table of contents.

This section would cite the short title as the "Cybersecurity Act of 2010" and provide a table of contents.

Section 2. Findings.

This section includes findings guiding the development of this legislation.

Section 3. Definitions.

This section would provide definitions for the terms Advisory Panel, cybersecurity, cybersecurity professional, information system, internet, and United States critical infrastructure information system.

Section 4. Procedure for designation of critical infrastructure information systems.

This section would initiate a rulemaking in which the President, in consultation with sector coordinating councils, relevant government agencies, and regulatory entities, would establish a procedure for the designation of critical infrastructure information systems (CIIS). The infiltration, incapacitation, or disruption of these systems would have a debilitating impact on national security, including national economic security and national public health or safety. The process would be governed by the Administrative Procedure Act and would, at a minimum, set forth objective criteria for designation, provide for emergency and temporary designations, ensure protection of privacy and proprietary information, and establish an appeal process.

Section 101. Certification and training of cybersecurity professionals.

This section would direct the President to request a National Academies report on cybersecurity accreditation, training, and certification programs. This section would direct the President to develop and annually update guidance for the identification of cybersecurity personnel within the Federal Government and requirements for their certification. Department of Defense (DoD) Directive 8570, which specifies guidance and procedures for the training, certification, and management of all people performing security functions on DoD information systems, may provide a valuable reference for understanding the challenges and potential solutions to cybersecurity certification and training.

This section would also direct the President to require owners and operators of Unites States CIIS to develop and annually update guidance for the identification of relevant cybersecurity personnel and requirements for their certification. The Committee believes that this guidance should take into account whether the owners or operators are small businesses, as small businesses have unique operational requirements and constraints.

This section would require the President to convene sector-specific working groups to establish auditable, private sector developed, accreditation, training, and certification programs for critical infrastructure cybersecurity personnel. The President would recognize and promote these programs. The President would require owners and operators of CIIS to conduct semiannual audits of compliance with the accreditation, training, and certification programs. Companies demonstrating compliance may receive positive recognition. Companies who fail to demonstrate substantial compliance through two semiannual independent audits would be required to collaborate with sector coordinating councils, relevant government agencies, and regulatory entities to develop and implement a remediation plan. This provision would leverage the existing structure

of the sector coordinating councils, but would not imbue them with any Federal authority.

This section would require the President to publish a reference list of cybersecurity accreditation, training, and certification programs whose rigor and effectiveness are beneficial to cybersecurity. The Committee believes that the general public would benefit from this list.

Section 102. Federal Cyber Scholarship-for-Service Program.

This section would authorize the Scholarship-For-Service program at the National Science Foundation (NSF), which is focused on recruiting students into a cybersecurity curriculum program. Upon graduation, these students would enter public service, joining an agency or department and leveraging the skills they have learned. This section would increase the number of students from 300 to 1000 annually. The Committee supports the Scholarship-For-Service program and believes that the program can help to close the talent gap to meet the nation's demand for cybersecurity experts.

Section 103. Cybersecurity competition and challenge.

This section would authorize the Director of the National Institute of Standards and Technology (NIST) to establish cybersecurity competitions and challenges to attract, identify, and recruit talented individuals to the cybersecurity field.

Section 104. Cybersecurity workforce plan.

This section would require the head of each Federal agency to annually complete a cybersecurity workforce plan that details recruitment, hiring, and training of cybersecurity employees and contractors. Each agency would make its hiring projections publicly available on the agency's website.

Section 105. Measures of cybersecurity hiring effectiveness.

This section would require each Federal agency to measure the effectiveness of its cybersecurity recruiting and hiring efforts, from the perspective of hiring managers, applicants, and new hires. This information would be reported annually to Congress and the public.

Section 201. Cybersecurity responsibilities and authorities.

This section would require the President to develop and implement a national cybersecurity strategy. This section would also require the President to collaborate with stakeholders to develop and rehearse detailed response and restoration plans for cybersecurity emergencies, and to define the types of events and incidents that would constitute a cybersecurity emergency. The section would authorize the President to declare a cybersecurity emergency and implement the plans. The Committee recognizes that this does not expand any existing Presidential authorities, and does not provide an exception to the procedures of Title 18, United States Code, sections 119, 121, and 206, or of Title 50, United States Code, sections 1801 et seq. The President would be required to report to Congress in writing, within 48 hours of declaring an emergency, regarding the circumstances necessitating the declaration and the estimated scope and duration of the emergency.

The Committee recognizes that it is virtually impossible to prevent each and every cybersecurity incident. Accordingly, this section would require the development of strategies and plans to quickly and effectively respond and restore all capabilities after an incident. The Committee believes it is vital that these plans and activities be rehearsed on a regular basis to ensure that, in the case of an emergency, the public and private sector participants will already be familiar with their roles and responsibilities and prepared to act appropriately.

Section 202. Biennial cyber review.

This section would direct the President to conduct a biennial review of the U.S. cyber program. The review would examine cyber strategy, budget, plans, and policies, and is modeled after the DoD's Quadrennial Defense Review. Although the Defense Review occurs every four years, the Internet and cyberspace are evolving so rapidly that a biennial review is appropriate.

Section 203. Cybersecurity dashboard pilot project.

This section would require the Secretary of Commerce to plan and implement a system to provide the real-time cybersecurity status of all Federal information systems and networks within the Department of Commerce.

Section 204. NIST cybersecurity guidance.

This section requires NIST to recognize and promote auditable, private sector developed, cybersecurity risk management techniques, risk management measures, and best practices, and to review and update these recognitions not less frequently than semiannually. The Committee believes that NIST should act transparently and provide relevant stakeholders with a meaningful opportunity to participate as it implements this section.

The President would require all Federal departments, agencies, and United States CIIS to meet or exceed these standards. Critical infrastructure owners and operators who meet these standards may be positively recognized by the President, and those who fail to demonstrate substantial compliance through two semiannual independent audits would be required to collaborate with sector coordinating councils, relevant government agencies, and regulatory entities to develop and implement a remediation plan. This section would leverage the existing structure of the sector coordinating councils, but would not imbue them with any Federal authority.

This section directs NIST to engage with international standards bodies regarding cybersecurity and to adopt a risk-based approach to cybersecurity. The Committee believes that it is vitally important that NIST adopt a risk-based approach to Federal cybersecurity guidance that recognizes techniques and best practices without prescribing specific hardware or software products.

This section also requires the FCC to report to Congress on effective and efficient means to ensure the cybersecurity of commercial broadband networks. The Committee recognizes that the FCC has introduced the National Broadband Plan which largely meets this requirement, and the FCC may provide an additional supplement on cybersecurity.

Section 205. Legal framework review and report.

This section would require GAO to complete a comprehensive review of the Federal statutory and legal framework applicable to cybersecurity and to make recommendations regarding changes needed to advance cybersecurity and protect civil liberties.

Section 206. Joint intelligence threat and vulnerability assessment.

This section would require the Director of National Intelligence, the Attorney General, and the Secretaries of Commerce, Homeland Security, Defense, and State to provide assessments on threats to and vulnerabilities of Federal information systems and CIIS.

Section 207. International norms and cybersecurity deterrence measures.

This section would require the President to promote the development of international norms, standards and techniques for improving cybersecurity.

Section 208. Federal secure products and services acquisitions.

This section would require that information systems, products, and services purchased by the Federal government comply with the cybersecurity standards recognized under section 204 and the cybersecurity professional certifications recognized under section 101.

Section 209. Private sector access to classified information.

This section would require the President to provide security clearances to key private sector operators of CIIS to facilitate the sharing of classified threat information with these officials. The Committee believes that this provision addresses the lack of coordination between civilian and national security information system protection efforts described in recommendation 23 of the CSIS report titled, Securing Cyberspace for the 44th Presidency.

Section 210. Authentication and civil liberties report.

This section would require the President to report to Congress on the feasibility of an identity management and authentication program with appropriate civil liberties and privacy protections.

Section 211. Report on evaluation of certain identity authentication functionalities.

This section would require NIST to issue a public report assessing the strategies and best practices for identity authentication, and to specifically address the application of this technology to health information.

Section 301. Promoting cybersecurity awareness and education.

This section would authorize a cybersecurity awareness campaign to educate the general public about cybersecurity risks and countermeasures people can implement to better protect themselves. It would also direct the Secretary of Education to consult with State authorities, private sector companies, and nongovernmental organizations to identify and promote age appropriate information and programs for grades K-12 regarding cyber safety, security, and ethics.

Section 302. Federal cybersecurity research and development.

This section would increase Federal support for cybersecurity research and development at the NSF. This section would also highlight important areas of research that need to be conducted, including secure coding and design.

Section 303. Development of curricula for incorporating cybersecurity into educational programs for future industrial control system designers.

This section would establish a grant program through the NSF to fund the development of undergraduate and graduate level curricula that address cybersecurity in modern industrial control systems.

Section 401. Cybersecurity Advisory Panel.

This section would require the President to establish or designate a Cybersecurity Advisory Panel consisting of outside experts in cybersecurity from industry, academia, and nonprofit advocacy organizations who will advise the President on cybersecurity related matters. This Panel would review Federal cybersecurity efforts and provide advice and direction. The Panel would provide a report to the President every two years with recommendations on how the Federal cybersecurity effort should be improved. The Committee believes that, while there is no shortage of advisory panels throughout the Federal government, none is specifically focused on cybersecurity. Furthermore, the Committee recognizes that the CSIS Securing Cyberspace report specifically recommends the creation of a Federal Advisory Committee with membership from key cyber infrastructures.

Section 402. State and regional cybersecurity enhancement program.

This section would create State and regional cybersecurity centers to assist small- and medium-sized companies in addressing cybersecurity issues. This program is modeled on the Manufacturing Extension Partnership (MEP). Large companies generally have the resources and access to expertise that would allow them to properly defend themselves against potential cyber intrusions. However, the Committee is particularly concerned about the small- and medium-sized businesses that often do not have the understanding or expertise to recognize that they are at risk, much less the resources to deal with this problem. The Committee believes that this program would help address such a knowledge gap. At the same time, the Committee believes these centers must operate in a manner that supplements or coordinates with, and does not compete with or duplicate, private sector activities.

Section 403. Public-private clearinghouse.

This section would create a public-private information sharing clearinghouse in which government and private officials would share classified and/or confidential cybersecurity threat and vulnerability information.

Section 404. Cybersecurity risk management report.

This section would require the President to report on how to create a market for cybersecurity risk management, including the potential role of civil liability and insurance.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, the Committee states that the bill as reported would make no change to existing law.

○