The National Cybersecurity Advisor Act of 2009

Sec. 1 – Office of the National Cybersecurity Advisor.

This section establishes the Office of the National Cybersecurity Advisor within the Executive Office of the President. The National Cybersecurity Advisor will lead this office and shall report directly to the President. This section also outlines a number of important functions and authority of the National Cybersecurity Advisor.

Analysis—This section is a major component of the bill. Many experts have recommended the creation of a high-ranking official that will coordinate cyber efforts across the government and with the private sector. Per their recommendations, we've modeled the office after the Office of the United States Trade Representative, which is within the Executive Office of the President. This is important because the office and the Advisor need to have the authority to compel other agencies to comply. The Advisor will serve as the lead official on all cyber matters, coordinating with the intelligence community, as well as the civilian agencies.

The Cybersecurity Act of 2009

Section by Section and Analysis

Sec. 1 – Short Title; Table of Contents.

This section includes the short title and a table of contents.

Sec. 2 – Findings.

This section includes findings guiding the development of this legislation.

Sec. 3 – Cybersecurity Advisory Panel

This section would require the President to establish or designate a Cybersecurity Advisory Panel. This panel shall consist of outside experts in cybersecurity from industry, academia, and non-profit advocacy organizations who will advise the President on cybersecurity related matters.

Analysis—This Advisory Panel provides industry, academia, and civil liberty groups an opportunity to review the federal cybersecurity

effort and provide advise on its direction and progress. The Panel reports to the President every two years, providing recommendations on how the program can be improved.

Sec. 4 – Real-Time Cybersecurity Dashboard

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

Analysis—The lack of real-time visibility into the state of an information system or network is a key limitation of improving cybersecurity. This visual tool will aid major decision makers, such as the Secretary, in identify which resources and determine how much to dedicate to address specific cybersecurity issues, as they arise. This will lead to a more efficient allocation of limited resources. The DOC may be seen as the pilot in a larger effort that the Federal government may attempt to roll out at a future date.

Sec. 5 – State and regional cybersecurity enhancement program

This provision would create state and regional cybersecurity centers to assist small and medium sized companies address cybersecurity issues.

Analysis—This program is modeled off of the Hollings Manufacturing Extension Partnership (MEP). Large companies have the resources and expertise to address cybersecurity issues, but small- and medium-sized companies often do not. This program would help address that gap.

Sec. 6 – NIST standards development and compliance

This section would require NIST to establish measureable and auditable cybersecurity standards for all federal government, government contractor, or grantee critical infrastructure information systems and networks. The section also requires the agency to establish standards and research in cybersecurity metrics, security controls, software security, and configurations. This section would also increase the agency's authorization of appropriations to accomplish this task.

Sec. 7 – Licensing and certification of cybersecurity professionals

This section would require the President, through the appropriate federal department or agency, to develop and integrate a national licensing and certification program for cybersecurity professionals. This section would also require all federal cybersecurity professionals to obtain this license.

Analysis—All major professions (doctors, lawyers, plumbers, electricians, etc.) are required to have a license to demonstrate they are qualified; cybersecurity professionals should not be exempt from this. There are a number of different cybersecurity certifications available currently, but there isn't a common standard among them.

Sec. 8 – Review of NTIA domain name contracts

This section would require the Advisory Panel to review and approve the renewal or modification of the Internet Assigned Number Authority contract to ensure that U.S. national security is not compromised.

Analysis—This provision relates to the contract that the Department of Commerce has with the International Corporation for Assigned Names and Numbers (ICANN) to manage and administer the domain name system, which is at the heart of the Internet. This provision is to make sure that ICANN does not succumb to foreign pressure to unilaterally release itself of its relationship with the U.S. government.

Sec. 9 – Secure domain name addressing system

This section requires the Assistant Secretary of Commerce for Communications and Information to develop a strategy to implement a secure domain name addressing system.

Analysis—There has been widespread disagreement as to how we should implement DNSSEC, a secure version of the domain name system. This is presumably something that ICANN should lead on, but since the organization has failed in this regard, it would be appropriate for the federal government to step in and improve the security of the Internet.

Sec. 10 – Promoting cybersecurity awareness

This section would authorize the Advisor to initiate a cybersecurity awareness campaign to educate the general public about cybersecurity risks and countermeasures they can implement to better protect themselves.

Sec. 11 – Federal cybersecurity research and development

This section would increase federal support for cybersecurity research and development at the National Science Foundation. This section would also highlight important areas of research that needs to be conducted, as recommended by the President's Information Technology Advisory Committee's 2005 report.

Sec. 12 – Scholarship-for-service program

This section would create in statute the Scholarship-For-Service program at the National Science Foundation, 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've learned. This section would also increase the number of students, from 300 to 1,000, annually.

Analysis—The Scholarship-For-Service was created through Executive Order and this would codify it. Additionally, the language clarifies the authority for hiring officials to bring Scholarship-For-Service graduates into the Federal workforce without having to go through competitive hiring procedures.

Sec. 13 – Cybersecurity competition and challenge

This section would authorize the NIST Director to establish cybersecurity competitions and challenges to attract, identify, and recruit talented individuals to the cybersecurity field.

Sec. 14 – Public–private clearinghouse

This section would allow the National Cybersecurity Advisor to designate a federal agency to serve as the public-private clearinghouse for cybersecurity threat and vulnerability data. The clearinghouse would responsible for the management and sharing of data between the federal government and private sector critical infrastructure operators.

Analysis—One major weakness of existing federal cybersecurity efforts is the sharing of information, both within the federal government and with industry. Agencies are not willing to share data with each other. The federal government has access to threat data and does not share it with industry (who may be the target of an attack). The CSIS Commission explicitly called for the government to recast its relationship with the private sector and promote information sharing in order to improve cybersecurity overall. The legislation would require the government to come up with a way by which it will share information with the private sector. By exempting the data managed by the clearinghouse from FOIA requests, we hope to encourage industry to share their data.

Sec. 15 – Cybersecurity risk management report

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

Sec. 16 – Legal framework review and report

This section would require the President, through the appropriate entity, to complete a comprehensive review of the federal statutory and legal framework applicable to cybersecurity.

Sec. 17 – Authentication and civil liberties report

This section would require the President to review the feasibility of an identity management and authentication program.

Analysis—Many experts believe that the anonymous nature of the Internet is one of it major vulnerabilities. Experts believe that incorporating identity management and authentication will improve overall security. This can be controversial with regards to civil liberties, which is why we start with a study.

Sec. 18 – Cybersecurity Responsibilities and Authorities

The President would be responsible for developing a comprehensive national strategy for cybersecurity. The President would also be able to disconnect a federal department or agency from the Internet if they are found to at risk and unwilling to take corrective action.

Sec. 19 – Quadrennial cyber review

This section directs the President to conduct a quadrennial review of the U.S. cyber program. The review shall examine cyber strategy, budget, plans, and policies.

Analysis—This review is modeled off of the Department of Defense's Quadrennial Defense Review to provide periodic review and analysis of the country's cyber program.

Sec. 20 – Joint intelligence threat assessment

This section requires the Director of National Intelligence and the Secretary of Commerce to provide assessment on threats and vulnerabilities to critical national information, communication, and data network infrastructure.

Sec. 21 – International norms and cybersecurity deterrence measures

This section would require the President to develop international standards and techniques for improving cybersecurity.

Analysis—Since the Internet is not limited to geographic boundaries it is necessary to coordinate cybersecurity efforts on a global basis.

Sec. 22 – Federal Secure Products and Services Acquisitions Board

This section would establish a Secure Products and Services Acquisitions Board responsible for certifying that products the federal government purchases will have met standards for security as established by the Board.

Analysis—Many critics have encouraged the federal government to use its acquisition authority as a way to compel software and product vendors to improve the security of their goods and services. Many contracting officers do not incorporate security provisions into acquisition contracts (either because it is not considered a performance requirement or they lack the knowledge and understanding to make it a requirement), and this Board would eliminate that problem by requiring all information and communication technologies are reviewed and approved.

Sec. 23 – Definitions

This section defines terms used in this legislation.