

Cybersecurity: A Briefing – Part I

R. Michael Senkowski
and Mimi W. Dawson

WILEY REIN LLP

This is Part I of a two-part story on cybersecurity.

Summary

On May 29, 2009, the Obama administration released the much-anticipated White House report and recommendations for federal cybersecurity strategy. This memorandum provides an overview of this report as well as recent cyber-related activities and pending cybersecurity-related legislation. The federal government has undertaken a major cybersecurity strategic review that includes reorganizing policy-making elements within the executive branch, prioritizing cybersecurity efforts across the federal government and improving public-private sector partnerships to promote cybersecurity. Congress has also established markers in this policy debate about executive branch organization and initiated possible regulatory and standard-setting efforts, new cybersecurity standards for IT procurement by the federal government and industry-specific legislation to address specific cybersecurity threats.

R. Michael Senkowski chairs Wiley Rein's Telecommunications Practice, which includes more than 40 lawyers and two engineers engaged in telephony, wireless, international and Internet issues. He can be reached at (202) 719-7249. Mimi W. Dawson is a noted public policy strategist and leads the firm's legislative and regulatory policy efforts. She served as a Commissioner at the Federal Communications Commission (FCC) and as Deputy Secretary of the U.S. Department of Transportation. She can be reached at (202) 719-7034. Mr. Senkowski and Ms. Dawson gratefully acknowledge the assistance of Julie A. Dunne, Scott Weaver and John B. Simpson on this article.

Cybersecurity Strategy In Executive Branch: Hathaway Report The Obama Administration's Cybersecurity Strategy

On May 29, 2009, the White House released the "Cyberspace Policy Review" (the Review) – often referred to as the Hathaway Report. Melissa Hathaway, acting senior director for Cyberspace for the National Security Council, led the Review. The Review was initiated by President Obama in February 2009 in order to do a "comprehensive 'clean-slate' review to assess U.S. policies and structures for cybersecurity." This Review – while light on specifics – sets the stage for high-level attention on all things related to cybersecurity and seeks to promote a comprehensive approach to securing digital infrastructure. The Review is a key indicator of this administration's approach to cybersecurity and will prompt continuing discussion of these issues in Congress.

With the release of the Review, the President announced he would appoint a White House cybersecurity policy official to lead cybersecurity-related policymaking and cyber-incident response efforts. This official would report to the National Security Council and the National Economic Council. The President is expected to name the person to fill this position during the week of June 1. Potential candidates for the position include Hathaway; Microsoft Corp. Vice President Scott Charney, who formerly ran the Justice Department's computer-crime unit, and Maureen Baginski, who has held senior National Security Council and FBI positions.

The Review addressed missions and activities associated with information and communications infrastructure, including computer network defense and other areas such as information assurance, counterintelligence, counterterrorism, telecommunications policies and general critical infrastructure protection. Key points in the report include the following:

I. Leading from the Top

- The President should appoint a cybersecurity official with clear presidential support and authority to participate in all appropriate

economic, counterterrorism and science and technology policy discussions to inform them of the cybersecurity perspectives.

- The cybersecurity policy official should not have operational responsibility or authority, nor the authority to make policy unilaterally, but using interagency coordination processes, the cybersecurity policy official should harmonize cybersecurity-related policy and technology efforts across the federal government.

- All federal departments and agencies should establish a point-of-contact in their respective executive suites who is authorized to interface with the White House on cybersecurity-related issues.

- The cybersecurity policy official should prepare for the President's consideration an updated national strategy to secure the information and communications infrastructure.

- The administration should work with Congress to update the Federal Information Security Management Act of 2002 (FISMA) to hold department and agency officials responsible for cybersecurity and secure systems.

II. Building Capacity for a Digital Nation

- The federal government, with the participation of all departments and agencies, should expand support for key education programs and research and development to ensure the nation's continued ability to compete in the information age economy.

- The President's cybersecurity policy official, in coordination with the ICI-IPC, should consider how to better attract cybersecurity expertise and to increase retention of employees with such expertise within the federal service.

III. Sharing Responsibility for Cybersecurity

- Industry and governments share the responsibility for the security and reliability of the infrastructure and the transactions that take place on it and should work closely together to address these interdependencies.

- Government can facilitate private sector engagement by considering incentive-based legislative or regulatory tools to enhance the value proposition and fostering an environment that facilitates and encourages partner-

Please email the authors at msenkowski@wileyrein.com or mdawson@wileyrein.com with questions about this article.

ship and information sharing.

- The President's cybersecurity policy official should work with relevant departments and agencies and the private sector to examine existing public-private partnership and information-sharing mechanisms to identify or build upon the most effective models.

- The federal government should develop a proactive engagement plan for use with international standards bodies (UN, Group of Eight, NATO, etc). Agreements, standards or practices promulgated in these organizations have global effects and cannot be ignored. The Review recommends further study on whether and in what ways elements of the information and communication infrastructure ought to be treated as a global commons.

IV. Creating Effective Information Sharing and Incident Response

- The newly created cybersecurity policy official is the White House action officer for cyber incident response.

- In order to improve situational awareness and response capability the federal government should explore long-term architectures for intrusion detection and prevention systems, leverage long-term investments in the development of cryptologic and information assurance technologies and supporting infrastructure.

- Develop options for cybersecurity-related information sharing – such as trusted third hosts – to enhance information sharing with the private sector to improve incident response.

V. Encouraging Innovation

- The federal government should provide a framework for research and development strategies that focus on game-changing technologies that will help meet infrastructure objectives, building on the existing Networking and Information Technology Research and Development (NITRD) strategies and other R&D-related work.

- The federal government – in collaboration with industry and the civil liberties and privacy communities – should build a cybersecurity-based identity management vision and strategy for the nation that considers an array of approaches, including privacy-enhancing technologies.

- The emergence of new centers for manufacturing, design and research across the globe raises concerns about the potential for easier subversion of computers and networks through subtle hardware or software manipulations. The best defense may be to ensure U.S. market leadership through continued innovation that enhances U.S. market leadership and the application of best practices in maintaining diverse, resilient supply chains and infrastructures.

- Federal policy must address national security requirements, protection of intellectual property and the availability and continuity of infrastructure, even when it is under

attack by sophisticated adversaries. The federal government also must be careful not to create policy and regulation that inhibits innovation or results in inefficiencies or less security.

The Review Team also recommended the following Action Plans:

Cyberspace Policy Review: Near-term Action Plan

- Appoint a cybersecurity policy official responsible for coordinating the nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.

- Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.

- Designate cybersecurity as one of the President's key management priorities and establish performance metrics.

- Designate a privacy and civil liberties official to the NSC cybersecurity directorate.

- Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the federal government.

- Initiate a national public awareness and education campaign to promote cybersecurity.

- Develop U.S. government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.

- Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement.

- In collaboration with other EOP entities, develop a framework for research and development strategies that focuses on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.

- Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the nation.

Cyberspace Policy Review: Mid-term Action Plan

- Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.

- Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.

- Expand support for key education programs and research and development to ensure the nation's continued ability to compete in the information age economy.

- Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the federal government.

- Determine the most efficient and effective mechanism to obtain strategic warning, maintain situational awareness and inform incident response capabilities.

- Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning and prioritization of R&D.

- Develop a process between the government and the private sector to assist in preventing, detecting and responding to cyber incidents.

- Develop mechanisms for cybersecurity-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.

- Develop solutions for emergency communications capabilities during a time of natural disaster, crisis or conflict while ensuring network neutrality.

- Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.

- Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.

- Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.

- Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.

- Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services.