THE COMMITTEE ON ENERGY AND COMMERCE

Memorandum

May 17, 2013

TO: Members, Committee on Energy and Commerce

FROM: Committee Majority Staff

RE: Hearing on "Cyber Threats and Security Solutions"

On May 21, 2013, at 10:00 a.m. in room 2123 of the Rayburn House Office Building, the Committee on Energy and Commerce will hold a hearing entitled "Cyber Threats and Security Solutions." This hearing will examine steps the Federal government and the private sector are taking to bolster the security of the nation's critical infrastructure and mitigate exposure to cyber-attacks. The hearing also will focus on the President's Executive Order to improve critical infrastructure cybersecurity, including the latest on its implementation and the Administration's development of a voluntary cybersecurity framework.

I. WITNESSES

Panel I

Dr. Patrick D. Gallagher
Under Secretary of Commerce for Standards and Technology
Director
National Institute of Standards and Technology

Panel II

The Honorable Dave McCurdy
President and CEO
American Gas Association
Former Chairman of the House Intelligence Committee

Mr. John M. (Mike) McConnell
Vice Chairman
Booz Allen Hamilton
Former Director of National Intelligence

Ambassador R. James Woolsey
Chairman, Woolsey Partners LLC
Former Director of Central Intelligence

Dr. Michael Papay
Vice President and Chief Information Security Officer
Northrop Grumman Information Systems

Dr. Phyllis Schneck
Vice President and Chief Technology Officer, Global Public Sector
McAfee, Inc.

Mr. Charles Blauner
Global Head of Information Security
Citigroup, Inc.
On behalf of the American Bankers Association

Mr. Duane Highley
President and CEO
Arkansas Electric Cooperative Corporation
On behalf of the National Rural Electric Cooperative Association

Mr. Robert Mayer
Vice President, Industry and State Affairs
United States Telecom Association

II. BACKGROUND

A. Cybersecurity Threats and Security Solutions

Over the last two decades, the United States has witnessed significant and rapid technological advancements in digital communications and information technology. Owners and operators of critical infrastructure have capitalized on these innovative technologies to operate their systems more efficiently and provide better service to customers. The increased utilization of digital technologies has resulted in untold operational, customer service, and cost efficiencies that have benefited consumers and the overall economy.

Despite the many benefits of an increasingly "wired" economy, the nation's exposure to cyber threats has also increased.[1] Combatting such threats requires a cybersecurity regime that provides ample flexibility to afford owners and operators of critical infrastructure the ability to protect against and respond to rapidly evolving threats. A one-size-fits-all approach to cybersecurity is ill-suited for the diverse range of critical infrastructure sectors, each of which has its own complex characteristics. Undertaking certain reasonable actions, however, could make a marked improvement in protecting critical assets, including enhanced information sharing between the Federal government and the private sector,[2] greater emphasis on public-private partnerships, and improved cross-sector collaboration.

B. Executive Order on Critical Infrastructure Cybersecurity

On February 12, 2013, President Obama issued an Executive Order, entitled "Improving Critical Infrastructure Cybersecurity."[3] Based on input from stakeholders, the final Executive Order differed dramatically from the draft cybersecurity Executive Order. The stated purpose of the Executive Order is to "enhance the security and resilience of the Nation's critical

[1] The number of reported and identified cybersecurity incidents impacting control systems associated with critical infrastructure increased by more than 2,000 percent between 2009 and 2011, according to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). *See* "ICS-CERT Incident Response Summary Report 2009-2011" (July 2012).
[2] On April 18, 2013, the House of Representatives passed H.R. 624, the "Cyber Intelligence Sharing and Protection Act", to provide greater sharing of cyber threat intelligence and information between the intelligence community and the private sector.
[3] Executive Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."[4] Such goals are to be achieved, according to the Executive Order, "through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards." [5]

The Executive Order directs the National Institute of Standards and Technology (NIST) to develop a "Cybersecurity Framework" that reduces cyber risks to critical infrastructure through a flexible, performance-based, and technology-neutral approach to managing cyber risks.[6] To address such risks, the Executive Order specifies that the Cybersecurity Framework must include "standards, methodologies, procedures, and processes that align policy, business, and technological approaches," as well as incorporate voluntary consensus standards and industry best practices.[7] Concurrently, the Executive Order directs the Department of Homeland Security (DHS) to develop a voluntary compliance program that incentivizes owners and operators of critical infrastructure to adopt the Cybersecurity Framework developed by NIST.[8]

Another stated objective of the Executive Order is improved sharing of cyber threat information between Federal agencies and private-sector entities. To this end, the Executive Order directs DHS to establish a process that rapidly disseminates unclassified reports of cyber threats to targeted entities.[9] It also expands the Enhanced Cybersecurity Services program, enabling sharing of cyber threat information to assist participating critical infrastructure companies in their cyber protection efforts. The Executive Order makes clear that this requirement is voluntary and "will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure."[10]

By July 2013, DHS also is required to apply a risk-based approach to identify critical infrastructure that, if subject to a cyber-attack, could have "catastrophic" effects on public health or safety, the economy, or national security.[11] This "at greatest risk" list is to be updated on an annual basis, and owners and operators of identified infrastructure are to be notified of the determination. Notably, the Executive Order specifies that commercial information technology products and consumer information technology services are not to be identified as critical infrastructure under this section.[12]

---

[4] *Id.* § 1.
[5] *Id.*
[6] *Id.* § 7.
[7] The Cybersecurity Framework is to be developed through a "consultative process" with relevant stakeholders, and NIST is required to "engage in an open public review and comment process." *Id.*
[8] *Id.* § 8.
[9] *Id.* § 4.
[10] *Id.* § 4(c).
[11] *Id.* § 9.
[12] *Id.* § 9(a).

III. ISSUES

The following issues will be examined at the hearing:

- the scope and nature of the cybersecurity threats to the nation's critical infrastructure and key resources;
- proposed solutions to better protect critical infrastructure from cyber threats, including best practices, enhanced information sharing, and public-private partnerships;
- current status and future outlook for implementation of the Executive Order and the Administration's development of a voluntary cybersecurity framework; and,
- private-sector perspectives on the Executive Order and the role of the private sector in protecting assets and mitigating exposure to cyber threats.

IV. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Patrick Currier at (202) 225-2927.