Statement of Eric A. Fischer
Senior Specialist in Science and Technology
Congressional Research Service
before the
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security
U.S. House of Representatives

Hearing on

"Oversight of Executive Order 13636 and Development of the Cybersecurity Framework"

July 18, 2013

Chairman Meehan, Ranking Member Clarke, and distinguished Members of the Subcommittee:

Thank you for the opportunity to discuss Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, with you today. In my testimony, I will provide some background on the development of the order and describe its major provisions, including the roles it proposes for the private sector and reaction to it by those stakeholders, as well as its relationship to congressional legislation and the new Obama Administration policy directive on critical infrastructure.

Development of the Executive Order

Both the George W. Bush Administration and the Obama Administration have made improvements to the cybersecurity of critical infrastructure a priority. The Bush Administration created the Comprehensive National Cybersecurity Initiative (the CNCI) in 2008 via a classified presidential directive.[1] The Obama Administration performed an interagency review of federal cybersecurity initiatives in 2009, culminating in the release of its *Cyberspace Policy Review*[2] and the creation of the White House position of Cybersecurity Coordinator.

Both those efforts and a number of reports from agencies, think tanks, and other groups identified gaps in federal efforts. Both the 111th and 112th Congresses considered legislative proposals to close those gaps, but none were enacted. In the absence of enacted legislation, the Obama Administration began drafting a cybersecurity executive

---

[1] National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23).

[2] The White House, *Cyberspace Policy Review*, May 29, 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; The White House, "Cyberspace Policy Review [Supporting Documents]," May 2009, http://www.whitehouse.gov/cyberreview/documents/.

order in 2012. The development involved a lengthy interagency process, with both agencies and stakeholders in the private sector providing input.

The White House released Executive Order 13636 on February 12, 2013, along with a new policy directive on critical infrastructure. Relevant legislation is also being developed by the 113th Congress. Four bills with cybersecurity provisions (H.R. 624, H.R. 756, H.R. 967, and H.R. 1163) that were introduced in the month after the release of the executive order passed the House in April, and additional bills in the House and the Senate are reportedly being drafted.

Requirements in the Executive Order

The order uses existing statutory and constitutional authority to

- *expand information sharing and collaboration* between the government and the private sector, including sharing classified information by broadening a program developed for the defense industrial base to other critical-infrastructure sectors;
- *develop a voluntary framework of cybersecurity standards and best practices* for protecting critical infrastructure, through a public/private effort;
- *establish a consultative process* for improving critical-infrastructure cybersecurity;
- *identify critical infrastructure with especially high priority for protection*, using the consultative process;
- *establish a program with incentives for voluntary adoption of the framework* by critical-infrastructure owners and operators;
- *review cybersecurity regulatory requirements* to determine if they are sufficient and appropriate; and
- *incorporate privacy and civil liberties protections* in activities under the order.

The information-sharing and framework provisions in particular have received significant public attention.

Information Sharing

The order formalizes a previously existing program, now called Enhanced Cybersecurity Services, in the Department of Homeland Security (DHS), for providing classified threat information to eligible critical infrastructure companies and to their eligible Internet, network, communications, and cybersecurity service providers (known jointly as commercial service providers or CSPs). The program developed out of a pilot involving the Department of Defense and companies in the defense industrial base, which is one of the 16 recognized critical-infrastructure sectors.

The order also requires the Secretary of Homeland Security, the Attorney General, and the Director of National Intelligence to expedite dissemination to targeted entities of unclassified and, where authorized, classified threat indicators. Additionally, the Secretary of Homeland Security is to expedite processing of security clearances to

appropriate critical-infrastructure personnel and expand programs to place relevant private-sector experts in federal agencies on a temporary basis.

Cybersecurity Framework

Executive Order 13636 requires the National Institute of Standards and Technology (NIST) to lead the development of a Cybersecurity Framework that uses an open, consultative process to identify cross-sector, voluntary consensus standards and business best practices that can reduce cybersecurity risks to critical infrastructure. The framework is to be technology-neutral. It must identify areas for improvement and be reviewed and updated as necessary.

The Secretary of Homeland Security is required to set performance goals for the framework, establish a voluntary program to support its adoption, and coordinate establishment of incentives for adoption. The sector-specific agencies must coordinate review of the framework and development of sector-specific guidance, and report annually to the President on participation by critical-infrastructure sectors. Agencies with regulatory responsibilities for critical infrastructure are required to engage in consultative review of the framework, determine whether existing cybersecurity requirements are adequate, report to the President whether the agencies have authority to establish requirements that sufficiently address the risks, propose additional authority where required, and identify and recommend remedies for ineffective, conflicting, or excessively burdensome cybersecurity requirements.

The development of the framework is arguably the most innovative and labor-intensive requirement in the executive order. It builds on the involvement of NIST in the development of cybersecurity technical standards[3] and its statutory responsibilities to work with both government and private entities on various aspects of standards and technology.[4]

None of the major legislative proposals in the 111th and 112th Congresses had proposed using NIST to coordinate an effort led by the private sector to develop a framework for cybersecurity, such as is envisioned by the executive order. Hundreds of entities have been involved in NIST's efforts to date, beginning with a Request for Information in February and including public workshops in April, May, and July of 2013.[5] An additional workshop is planned for September.

Other Requirements

Acquisition and Contracting. The Secretary of Defense and the Administrator of General Services must make recommendations to the President on incorporating security standards in acquisition and contracting processes, including harmonization of cybersecurity requirements.

---

[3] See, e.g., National Institute of Standards and Technology, "Computer Security Resource Center," February 20, 2013, http://csrc.nist.gov/.

[4] 15 U.S.C. §272.

[5] National Institute of Standards and Technology, "Cybersecurity Framework," July 2, 2013, http://www.nist.gov/itl/cyberframework.cfm.

Consultative Process. The Secretary of Homeland Security is required to establish a broad consultative process to coordinate improvements in the cybersecurity of critical infrastructure.

Cybersecurity Workforce. The Secretary of Homeland Security is required to coordinate technical assistance to critical-infrastructure regulatory agencies on development of their cybersecurity workforce and programs.

High-Risk Critical Infrastructure. The order requires the Secretary of Homeland Security to use consistent and objective criteria, the consultative process established under the order, and information from relevant stakeholders to identify and update annually a list of critical infrastructure for which a cyberattack could have catastrophic regional or national impact, but not including commercial information technology products or consumer information technology services. The Secretary must confidentially notify owners and operators of critical infrastructure that is so identified of its designation and provide a process to request reconsideration.

Privacy and Civil Liberties. The order requires agencies to ensure incorporation of privacy and civil liberties protections in agency activities under the order, including protection from disclosure of information submitted by private entities, as permitted by law. The DHS Chief Privacy Officer and Officer for Civil Rights and Civil Liberties must assess risks to privacy and civil liberties of DHS activities under the order and recommend methods of mitigation to the Secretary in a public report. Agency privacy and civil liberties officials must provide assessments of agency activities to DHS.

Implementation Deliverables and Deadlines

The order contains several requirements with deadlines, and other requirements with no associated dates. In March 2013, DHS announced that it had formed a task force with eight working groups focused on the various deliverables for which it is responsible.[6] There are 12 deliverables with specific associated dates:

June 12, 2013:

- Instructions for producing unclassified threat reports (Secretary of Homeland Security, Attorney General, Director of National Intelligence) (Sec. 4(a)).
- Procedures for expansion of the Enhanced Cybersecurity Services Program (Secretary of Homeland Security) (Sec. 4(c)).
- Recommendations to the President on incentives to participate in the framework (Secretaries of Homeland Security, Commerce, and theTreasury) (Sec. 8(d)).
- Recommendations to the President on acquisitions and contracts (Secretary of Defense, Administrator of General Services) (Sec 8(e)).

[6] Department of Homeland Security, "Integrated Task Force," March 18, 2013, http://www.dhs.gov/sites/default/files/publications/EO-PPD%20Fact%20Sheet%2018 March13.pdf.

July 12, 2013:

- Designation of critical infrastructure at greatest risk (Secretary of Homeland Security) (Sec. 9(a)).

October 10, 2013:

- Publication of preliminary Cybersecurity Framework (Director of the National Institute of Standards and Technology) (Sec. 7(e)).

February 12, 2014:

- Report on privacy and civil liberties, preceded by consultations (Chief Privacy Officer and Officer for Civil Rights and Civil Liberties of DHS) (Sec. 5(b)).
- Publication of final Cybersecurity Framework (Director of the National Institute of Standards and Technology) (Sec. 7(e)).

May 13, 2014:

- Reports to the President on review of regulatory requirements (agencies with regulatory responsibilities for critical infrastructure) (Sec. 10(a)).
- Proposed additional risk mitigation actions (agencies with regulatory responsibilities for critical infrastructure) (Sec. 10(b)).

February 12, 2016:

- Reports to the Office of Management and Budget on ineffective, conflicting, or burdensome requirements (agencies with regulatory responsibilities for critical infrastructure) (Sec. 10(c)).

The order also includes more than 20 actions for which no specific date is provided. While many of the activities under the order are in the process of development, some provisions may already have had some effect. For example, the provision on expedited security clearances was apparently used in responses to a cyberattack this past spring on several banks, to facilitate communication by the FBI with the banks.[7]

Relationship of the Executive Order to the Presidential Policy Directive

Presidential Policy Directive 21 (PPD 21),[8] *Critical Infrastructure Security and Resilience*, on protection of critical infrastructure, was released in tandem with Executive Order 13636. PPD 21 supersedes Homeland Security Presidential Directive 7 (HSPD 7), *Critical Infrastructure Identification, Prioritization, and Protection*, released December

---

[7] Joseph Menn, "FBI Says More Cooperation with Banks Key to Probe of Cyber Attacks," *Reuters*, May 13, 2013, http://www.reuters.com/article/2013/05/13/us-cyber-summit-fbi-banks-idUSBRE94C0XH20130513.

[8] The White House, "Critical Infrastructure Security and Resilience," Presidential Policy Directive 21, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

17, 2003. PPD 21 includes cybersecurity broadly as a need to be addressed along with physical security. It seeks to strengthen both the cyber- and physical security and resilience of critical infrastructure by

- clarifying functional relationships among federal agencies, including the establishment of separate DHS operational centers for physical and cyber-infrastructure;
- identifying baseline requirements for information sharing, to facilitate timely and efficient information exchange between government and critical-infrastructure entities while respecting privacy and civil liberties;
- applying integration and analysis capabilities in DHS to prioritize and manage risks and impacts, recommend preventive and responsive actions, and support incident management and restoration efforts for critical infrastructure; and
- organizing research and development (R&D) to enable secure and resilient critical infrastructure, enhance impact-modeling capabilities, and support strategic DHS guidance.

Implementation Deliverables and Deadlines

June 12, 2013:

- Description of functional relationships within DHS and across other federal agencies relating to critical infrastructure security and resilience (Secretary of Homeland Security).

July 12, 2013:

- Analysis of public-private partnership models with recommended improvements (Secretary of Homeland Security).

August 11, 2013:

- Convening of experts to identify baseline information and intelligence exchange requirements (Secretary of Homeland Security).

October 10, 2013:

- Demonstration of "near real-time" situational-awareness capability for critical infrastructure (Secretary of Homeland Security).
- Updated National Infrastructure Protection Plan that addresses implementation of the directive (Secretary of Homeland Security).

February 12, 2015:

- First quadrennial National Critical Infrastructure Security and Resilience R&D Plan (Secretary of Homeland Security).[9]

[9] PPD 7 gave primary responsibility for coordinating R&D to the Office of Science and Technology Policy.

In addition to DHS, the directive describes specific responsibilities for the Departments of Commerce, Interior, Justice, and State, the Intelligence Community, the General Services Administration, the Federal Communications Commission, the sector-specific agencies, and all federal departments and agencies.[10]

Relationship of the Executive Order to the Cyber Intelligence Sharing and Protection Act (CISPA, H.R. 624) and Other Legislation

A number of observers, both in the federal government and the private sector, have stated that Executive Order 13636 is not sufficient to protect U.S. critical infrastructure from cyberthreats, and that legislation is needed. In 2011, the White House proposed legislation with provisions on personnel authorities, criminal penalties, data breach notification, authorities of the Department of Homeland Security (DHS), a regulatory framework for cybersecurity of critical infrastructure, and reform of the Federal Information Security Management Act (FISMA). Related provisions also appeared in bills introduced in recent congresses. Both the White House proposal and several bills have contained incentives for information sharing by the private sector with the federal government and other private entities, including protection from legal liability and exemption from provisions in the Freedom of Information Act.

At a hearing before the Senate Committee on Homeland Security and Governmental Affairs in September 2012, Secretary of Homeland Security Janet Napolitano stated that in addition to the executive order, there were at least three things for which legislation would be necessary: personnel authorities, liability protections, and criminal penalties (S.Hrg. 112-639, p. 23). A number of private-sector entities have also stated that liability and disclosure protections are needed to encourage private-sector information sharing.

Among the cybersecurity bills that have been introduced in the 113th Congress, H.R. 624, the Cyber Intelligence Sharing and Protection Act (CISPA), which passed the House in April, addresses information sharing. Some provisions in CISPA, as in the executive order, would provide for expedited security clearances and sharing of classified information by the federal government with the private sector. The bill would additionally permit entities providing cybersecurity services to themselves or others (which the bill calls cybersecurity providers) to obtain and share threat information for purposes of protection, notwithstanding any other provision of law.

CISPA would also make such entities and those they protect exempt from liability for good-faith use of cybersecurity systems to obtain or share threat information and decisions based on such information.

In the Senate, the Committee on Commerce, Science, and Transportation is reportedly drafting a bill that would provide a legislative basis for NIST's role in developing and

[10] PPD 7 did not describe specific responsibilities of the Intelligence Community, the General Services Administration, or the Federal Communications Commission.

updating the framework in the executive order.[11] The draft bill would also reportedly require a federal cybersecurity research and development plan, as would H.R. 756, the Cybersecurity Enhancement Act of 2013, which passed the House in April. PPD-21 requires an R&D plan that addresses security and resiliency for critical infrastructure, including cybersecurity.

Private-Sector Reactions to the Executive Order

Given the absence of enacted comprehensive cybersecurity legislation, some security observers contend that the executive order is a necessary step in securing vital assets against cyberthreats. Some observers, however, have raised concerns.[12] Common themes by such critics include the following claims:

- *The order offers little more than do existing processes.* Such critics point out that, for example, the Enhanced Cybersecurity Services program was in place before the release of the order, and that a variety of efforts have been underway to develop and adopt voluntary standards and best practices in cybersecurity for many years. Proponents of the order argue that it lays out and clarifies Obama Administration goals, requires specific deliverables and timelines, and that the framework and other provisions are in fact new with the executive order.
- *The order could make enactment of legislation less likely.* These critics express concern that Congress might decide to wait until the major provisions of the order have been fully implemented before considering legislation. Proponents state that immediate action was necessary in the absence of legislation, and that changes in current law are necessary no matter how successful the executive order might be, to provide liability protections for information sharing and to meet other needs.
- *The process for developing the framework is either too slow or too rushed.* Some observers believe that some actions to protect critical infrastructure are well-established and should be taken immediately, given the nature and extent of the current threat. They state that the year-long process to develop the framework may delay implementation of needed security measures[13] and creates unnecessary and unacceptable risks. Others counter that widespread adoption of the framework requires consensus, which takes time to achieve, and that the one-year timeframe

---

[11] John Eggerton, "Rockefeller, Thune Circulate Cybersecurity Draft," *Broadcasting & Cable*, July 12, 2013, http://www.broadcastingcable.com/article/494447-Rockefeller_Thune_Circulate_Cybersecurity_Draft.php.

[12] See, for example, Paul Rosenzweig and David Inserra, *Obama's Cybersecurity Executive Order Falls Short*, Issue Brief #3852, February 14, 2013, http://www.heritage.org/research/reports/2013/02/obama-s-cybersecurity-executive-order-falls-short; Dave Frymier, "The Cyber Security Executive Order Is Not Enough," *Innovation Insights: Wired.com*, March 1, 2013, http://www.wired.com/insights/2013/03/the-cyber-security-executive-order-is-not-enough/.

[13] For example, some suppliers to the federal government have reportedly called for suspension of procurement rulemaking relating to cybersecurity until the framework has been published (Aliya Sternstein, "Contractors Ask GSA to Freeze Cyber-Related Regulations," *Nextgov*, May 17, 2013, http://www.nextgov.com/cybersecurity/2013/05/contractors-ask-gsa-freeze-cyber-related-regulations/63244/?oref=nextgov_cybersecurity).

may be insufficient, given that the process for developing and updating consensus standards often takes several years. Some also state that the framework process does not preclude entities from adopting established security measures immediately.

- *The framework risks becoming a form of de facto regulation, or alternatively, its voluntary nature makes it insufficiently enforceable.* Another concern of some is that it could lead to government intrusiveness into private-sector activities, for example through increased regulation under existing statutory authority,[14] while others contend that voluntary measures have a poor history of success. Some others, however, have argued that changes in the business environment—such as the advent of continuous monitoring, more powerful analytical tools, and a better prepared workforce—improve the likelihood that a voluntary approach can be successful.[15]
- *The order could lead to overclassification or underclassification of high-risk critical infrastructure by DHS.* Some observers have expressed concern that the requirement in the order for DHS to designate high-risk critical infrastructure may be insufficiently clear and could lead to either harmfully expansive designations or inappropriate exclusions of entities.[16] This might be particularly a problem if the criteria are not sufficiently validated.[17]

---

[14] For example, some believe that the framework, while voluntary, "could develop in such a way that companies will be forced to adopt prescriptive standards due to the fact that information on program adoption for 'high risk' industries may be made public. More concerning, this could be done without a review process and could be used to leverage [*sic*] in ways that may not be beneficial to lowering overall risk" (Testimony of David E. Kepler, Senate Committee on Homeland Security and Governmental Affairs and Senate Committee on Commerce, Science, and Transportation, "The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security," hearing, March 7, 2013, http://www.hsgac.senate.gov/hearings/the-cybersecurity-partnership-between-the-private-sector-and-our-government-protecting-our-national-and-economic-security).

[15] CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.; Mike McConnell et al., *The Cybersecurity Executive Order* (Booz Allen Hamilton, April 26, 2013), http://www.boozallen.com/media/file/BA13-051CybersecurityEOVP.pdf.

[16] Testimony of Roger Mayer, House Committee on Energy and Commerce, "Cyber Threats and Security Solutions," hearing, May 21, 2013, http://energycommerce.house.gov/hearing/cyber-threats-and-security-solutions.

[17] The Government Accountability Office (GAO) expressed similar concerns about DHS's National Critical Infrastructure Prioritization Program (NCIPP) list of highest-priority U.S. infrastructure (Government Accountability Office, *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, GAO-13-296, March 2013, http://www.gao.gov/assets/660/653300.pdf). The relationship between the NCIPP list and that under the executive order has raised some concerns. There appear to be some differences between the lists that have resulted in some disagreements with the private sector (see, for example, Testimony of Dave McCurdy, House Committee on Energy and Commerce, Cyber Threats and Security Solutions, hearing, May 21, 2013, http://energycommerce.house.gov/hearing/cyber-threats-and-security-solutions).

It appears to be too early in the development of the components of the executive order to determine how the concerns described above will be addressed and whether the responses will satisfy critics and skeptics. Overall, however, response to the order from the private sector—including critical-infrastructure entities, trade associations, and cybersecurity practitioners—appears to be cautiously optimistic.