Congressional Research Service
Informing the legislative debate since 1914

The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress

Eric A. Fischer
Senior Specialist in Science and Technology

Edward C. Liu
Legislative Attorney

John W. Rollins
Specialist in Terrorism and National Security

Catherine A. Theohary
Specialist in National Security Policy and Information Operations

December 15, 2014

Congressional Research Service
7-5700
www.crs.gov
R42984

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The federal role in cybersecurity has been a topic of discussion and debate for over a decade. Despite significant legislative efforts in the 112th Congress on bills designed to improve the cybersecurity of U.S. critical infrastructure (CI), no legislation on that issue was enacted in that Congress. In an effort to address the issue in the absence of enacted legislation, the White House issued an executive order in February 2013. Citing repeated cyber-intrusions into critical infrastructure and growing cyberthreats, Executive Order 13636, *Improving Critical Infrastructure Cybersecurity,* was an attempt to enhance security and resiliency of CI through voluntary, collaborative efforts involving federal agencies and owners and operators of privately owned CI, as well as use of existing federal regulatory authorities.

Entities posing a significant threat to the cybersecurity of CI assets include cyberterrorists, cyberspies, cyberthieves, cyberwarriors, and cyberhacktivists. E.O. 13636 has attempted to address such threats by, among other things,

- expanding to other CI sectors an existing Department of Homeland Security (DHS) program for information sharing and collaboration between the government and the private sector;
- establishing a broadly consultative process for identifying CI with especially high priority for protection;
- requiring the National Institute of Standards and Technology (NIST) to lead in developing a cybersecurity framework of standards and best practices for protecting CI; and
- directing regulatory agencies to determine the adequacy of existing requirements and their authority to establish additional ones to address the risks.

Among the major issues covered by the unenacted legislative proposals in the 112th Congress, E.O. 13636 mainly addresses two: information sharing and protection of privately held critical infrastructure. It does not provide exemptions from liability stemming from information sharing, which would require changes to current law. Several of the legislative proposals included such changes. With respect to protection of critical infrastructure, the provisions on designation of CI and identification of relevant regulations are related to those in some legislative proposals.

In the 113th Congress, some bills would provide explicit statutory authority for information-sharing along the lines of some bills in the 112th Congress. Others would authorize activities on developing a cybersecurity framework similar to those in the executive order.

The issuance of E.O. 13636, as with many other executive orders, raises questions about whether the order exceeds the scope of the President's authority, in relation to the constitutional separation of powers and validly enacted legislation. While answers to those questions are complex, the executive order specifies that implementation will be consistent with applicable law and that nothing in the order provides regulatory authority to an agency beyond that under existing law.

Overall, response to the executive order has been optimistic. Given the absence of comprehensive cybersecurity legislation, some security observers contend that the order is a necessary step in securing vital assets against cyberthreats. Others have argued, in contrast, that it offers little more than do existing processes, that it could make enactment of a bill less likely, or that it could lead

to government intrusiveness into private-sector activities, for example through increased regulation under existing statutory authority. Despite considerable progress in meeting the specific objectives in the executive order, especially the NIST Framework, it still appears to be too early in the implementation of the order to determine whether such concerns will be addressed to the satisfaction of critics and skeptics.

Contents

Figures

Contacts

The federal legislative framework for cybersecurity is complex, with more than 50 statutes addressing various aspects of it either directly or indirectly. Many observers have expressed doubt that the current statutory framework is sufficient to address the growing concerns about the security of cyberspace in the United States, especially with respect to critical infrastructure (CI).[1] Several legislative proposals were made in recent Congresses to address those concerns. While a few cybersecurity bills were enacted in the 113th Congress, they addressed only the security of federal information systems (S. 2521) and workforce issues (H.R. 2952 and S. 1691) and information-sharing activities (S. 2519) at the Department of Homeland Security (DHS).

Within the executive branch, both the George W. Bush and Obama Administrations have focused on improving the cybersecurity of critical infrastructure. The Bush Administration created the classified Comprehensive National Cybersecurity Initiative (the CNCI) in 2008.[2] The Obama Administration performed an interagency review of federal cybersecurity initiatives in 2009, culminating in the release of its *Cyberspace Policy Review*[3] and the creation of the White House position of Cybersecurity Coordinator. In the absence of enacted legislation, the Obama Administration began drafting a cybersecurity executive order in 2012. The development involved input from both federal agencies and stakeholders in the private sector.[4]

On February 12, 2013, President Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*,[5] along with Presidential Policy Directive 21 (PPD 21),[6] *Critical Infrastructure Security and Resilience.* The issuance of the executive order in the absence of congressional action raises several questions that are addressed in this report:

- What are the kinds of threats to the national security and economic interests of the United States that the executive order is intended to address?
- What steps does it take to address those threats, what is the status of their implementation, and what issues do they raise?
- What is the legislative and constitutional authority for the executive order?

[1] CI is defined in 42 U.S.C. §5195c(e) as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." For more information on critical infrastructure, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff,. For a discussion of the legislative framework for cybersecurity, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

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

[3] 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/.

[4] Tony Romm, "White House Moves on Cybersecurity," *Politico*, November 27, 2012, http://www.politico.com/news/stories/1112/84247.html.

[5] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," *Federal Register* 78, no. 33 (February 19, 2013): 11737–11744. The information in this report is derived from unclassified sources, including this Executive Order, and does not reflect information that may be included in a classified Presidential Order or other classified documents addressing cyberthreats to the United States.

[6] 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.

- How do its provisions relate to those in legislative proposals in the 112th and 113th Congresses?
- What has been the reaction of stakeholders to the order and what issues does it raise?

Background: Threats and Consequences

> Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats.[7]

Cyberthreats to U.S. infrastructure and other assets are a growing concern to policy makers. Information and communications technology (ICT)[8] is ubiquitous and relied upon for government services, corporate business processes, and individual professional and personal pursuits—almost every facet of modern life. Many ICT devices and other components are interdependent, and disruption of one component may have a negative, cascading effect on others. A denial of service, theft or manipulation of data, or damage to critical infrastructure through a cyber-based attack could have significant impacts on national security, the economy, and the livelihood and safety of individual citizens.

Cyberthreats

Cyber-based technologies[9] are now ubiquitous around the globe. The vast majority of users pursue lawful professional and personal objectives. However, criminals, terrorists, and spies also rely heavily on cyber-based technologies to support their objectives. These malefactors may access cyber-based technologies in order to deny service, steal or manipulate data, or use a device to launch an attack against itself or another piece of equipment. Entities using cyber-based technologies for illegal purposes take many forms and pursue a variety of actions counter to U.S. global security and economic interests. While E.O. 13636 discusses in general terms cyber-based threats directed at the nation's critical infrastructure, it does not identify the types of cyber-actors and possible consequences of a successful attack. Commonly recognized cyber-aggressors discussed below, along with representative examples of the harm they can inflict, include cyberterrorists, cyberspies, cyberthieves, cyberwarriors, and cyberhacktivists.

[7] E.O. 13636.

[8] The term ICT is increasingly used instead of IT (information technologies) because of the convergence of telecommunications and computer technology. However, the current federal legislative framework for cybersecurity does not reflect that convergence and generally treats IT and telecommunications as separate technologies.

[9] For purposes of this report, *cyber-based technologies* means electronic devices that access or rely on the transfer of bytes of data to perform a mechanical function. The devices can access cyberspace (including the Internet) through the use of physical connections or wireless signals.

Cyberterrorists

Cyberterrorists are state-sponsored and non-state actors who engage in cyberattacks as a form of warfare. Transnational terrorist organizations, insurgents, and jihadists have used the Internet as a tool for planning attacks, radicalization and recruitment, a method of propaganda distribution, and a means of communication.[10] While no unclassified reports have been published regarding a terrorist-initiated cyberattack on U.S. critical infrastructure (CI),[11] the vulnerability of essential components of that infrastructure to access and even destruction via the Internet has been demonstrated. In 2009, the Department of Homeland Security (DHS) conducted an experiment that revealed some of the vulnerabilities to the nation's control systems that manage power generators and grids. The experiment, known as the Aurora Project, entailed a computer-based attack on a power generator's control system that caused operations to cease and the equipment to be destroyed.[12]

Cyberspies

Cyberspies are individuals who steal classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage. These individuals often work at the behest of, and take direction from, foreign government entities. For example, a 2011 FBI report noted, "a company was the victim of an intrusion and had lost 10 years' worth of research and development data—valued at $1 billion—virtually overnight."[13] Likewise, in 2008 the Department of Defense's (DOD's) classified computer network system was unlawfully accessed and "the computer code, placed there by a foreign intelligence agency, uploaded itself undetected onto both classified and unclassified systems from which data could be transferred to servers under foreign control."[14] The U.S. intelligence community recently completed a classified National Intelligence Estimate (NIE) focused on cyberspying against U.S. targets. Reportedly, the NIE "concluded that the United States is the target of a massive, sustained cyber-espionage campaign that is threatening the country's economic competitiveness."[15] Media reports suggest that the NIE also assessed that Russia, Israel, and France also engage in illegal accessing of United States entities for economic intelligence purposes but notes that "cyber-espionage by those countries pales in comparison with China's effort."[16] A February 2013 report of an investigation by a private-sector security firm of intrusions

[10] For additional background information, see archived CRS Report RL33123, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, by John W. Rollins and Clay Wilson.

[11] The Executive Order uses the same definition of *critical infrastructure* as 42 U.S.C. 5195c(e): "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

[12] See "Challenges Remain in DHS' Efforts to Secure Control Systems," Department of Homeland Security, Office of Inspector General, August 2009. For a discussion of how computer code may have caused the halting of operations at an Iranian nuclear facility see CRS Report R41524, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, by Paul K. Kerr, John W. Rollins, and Catherine A. Theohary.

[13] Executive Assistant Director Shawn Henry, "Responding to the Cyber Threat," Federal Bureau of Investigation, Baltimore, MD, 2011.

[14] Department of Defense Deputy Secretary of Defense William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, October 2010.

[15] Ellen Nakashima, "U.S. Said to Be Target of Massive Cyber-Espionage Campaign," *Washington Post*, February 10, 2013.

[16] Ibid.

against more than 100 targets over the past seven years states that the attacks were performed by a single Chinese group that appears to be linked to the People's Liberation Army.[17]

Cyberthieves

Cyberthieves are individuals who engage in illegal cyberattacks for monetary gain. Examples include an organization or individual who illegally accesses a technology system to steal and use or sell credit card numbers and someone who deceives a victim into providing access to a financial account. Cybercrime is widely regarded as lucrative and relatively low-risk for criminals and costly for victims, with some estimates placing the annual global cost to individuals as high as hundreds of billions of dollars.[18] However, making accurate estimates of such aggregate costs is problematic, and there does not appear to be any publicly available, comprehensive, reliable assessment of the overall costs of cyberattacks.

Cyberwarriors

Cyberwarriors are agents or quasi-agents of nation-states who develop capabilities and undertake cyberattacks in support of a country's strategic objectives.[19] These entities may or may not be acting on behalf of the government with respect to target selection, timing of the attack, and type(s) of cyberattack and are often blamed by the host country when accusations are levied by the nation that has been attacked. Often, when a foreign government is provided evidence that a cyberattack is emanating from its country, the nation that has been attacked is informed that the perpetrators acted of their own volition and not at the behest of the government. In August 2012 a series of cyberattacks were directed against Saudi Aramco, the world's largest oil and gas producer and most valuable company. The attacks compromised 30,000 of the company's computers and the code was apparently designed to disrupt or halt the production oil. Some security officials have suggested that Iran may have supported this attack.[20] However, other observers suggest that the perpetrator of the attack was an employee of Saudi Aramco.[21]

Cyberhacktivists

Cyberhacktivists are individuals who perform cyberattacks for pleasure, or for philosophical or other nonmonetary reasons. Examples include someone who attacks a technology system as a personal challenge (who might be termed a "classic" hacker), and a "hacktivist" such as a

[17] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, February 18, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[18] For discussions of federal law and issues relating to cybercrime, see CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle; and CRS Report R41927, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, by Kristin Finklea.

[19] For additional information, see CRS Report RL31787, *Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues*, by Catherine A. Theohary.

[20] Wael Mahdi, "Saudi Arabia Says Aramco Cyberattack Came from Foreign States," *Bloomberg News*, December 9, 2012, http://www.bloomberg.com/news/2012-12-09/saudi-arabia-says-aramco-cyberattack-came-from-foreign-states.html.

[21] Michael Riley and Eric Engleman, "Code in Aramco Cyber Attack Indicates Lone Perpetrator," *Bloomberg Businessweek*, October 25, 2012.

member of the cyber-group Anonymous who undertakes an attack for political reasons. The activities of these groups can range from simple nuisance-related denial of service attacks to disrupting government and private corporation business processes.

Cyberthreats and Implications for U.S. Policy

These different kinds of cyber-aggressors and the types of attacks they can pursue are not mutually exclusive. For example, a hacker targeting the intellectual property of a corporation may be categorized as both a cyberthief and a cyberspy, and possibly a cyberwarrior if the activity is conducted by a military enterprise, as has been claimed for some such attacks.[22] A cyberterrorist and cyberwarrior may be employing different technological capabilities in support of a nation's security and political objectives. Ascertaining information about the aggressor and its capabilities and intentions is very difficult.[23] The threats posed by these aggressors, coupled with the United States' proclivity to be an early adopter of emerging technologies,[24] which often contain unrecognized vulnerabilities and are introduced into existing computer networks, make for a complex environment when considering operational responses, policies, and legislation designed to safeguard the nation's strategic economic and security interests. E.O. 13636 discusses the nation's reliance on cyber-based technologies and identifies activities and reporting requirements to be addressed by numerous federal government departments and agencies.

Overview of the Executive Order

The federal role in what is now called cybersecurity[25] has been debated for more than a decade. Much of the recent debate has focused on two issues: sharing of cybersecurity-related information within and across sectors, and the cybersecurity of CI sectors, including federal systems. E.O. 13636 attempts to address both of those issues, as well as others.

It uses existing statutory and constitutional authority to

[22] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, op. cit.

[23] The concept of attribution in the cybersecurity context entails an attempt to identify with some degree of specificity and confidence the geographic location, identity, capabilities, and intention of the cyber-aggressor. Mobile technologies and sophisticated data routing processes and techniques often make attribution difficult for U.S. intelligence and law enforcement communities.

[24] Emerging cyber-based technologies that may be vulnerable to the actions of a cyber-aggressor include items that are in use but not yet widely adopted or are currently being developed. For additional information on how the convergence of inexpensive, highly sophisticated, and easily accessible technology is providing opportunities for cyber-aggressors to exploit vulnerabilities found in a technologically laden society see Office of the Director of National Intelligence, "Global Trends 2030," 2013, http://www.dni.gov/index.php/about/organization/global-trends-2030.

[25] *Cybersecurity* is a convenient umbrella term that tends to defy precise consensus definition. Several different terms are in use that have related meanings. For example, *information security* is defined in some subsections of federal copyright law to mean "activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network" (17 U.S.C. 1201(e), 1202(d)), and, in the Federal Information Security Management Act (FISMA, 44 U.S.C. 3542) as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction" to provide integrity, confidentiality, and availability of the information. Other terms often used include *information assurance, computer security,* and *network security*.

- *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 CI sectors;
- *develop a voluntary framework of cybersecurity standards and best practices* for protecting CI, through a public/private effort;
- *establish a consultative process* for improving CI cybersecurity;
- *identify CI with especially high priority for protection,* using the consultative process;
- *establish a program with incentives for voluntary adoption of the framework* by CI 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

Improved sharing of information on cybersecurity threats, vulnerabilities, attacks, prevention, and response both within and across sectors, including government, is thought by most experts to be critical to improving cybersecurity but fraught with barriers and uncertainties, relating especially to privacy, liability, reputation costs,[26] protection of proprietary information, antitrust law, and misuse of shared information. A few sectors are subject to federal notification requirements,[27] but most such information sharing is voluntary, often through sector-specific Information Sharing and Analysis Centers (ISACs)[28] or programs under the auspices of the Department of Homeland Security (DHS) or sector-specific agencies.[29] A key question is how to balance the need for better, more timely cybersecurity information with other needs such as protection of privacy and civil rights as well as legitimate business and economic interests.

To improve information sharing, the order builds on a voluntary effort established in May 2011. That program, known as the DIB[30] Cyber Pilot, involved several defense industry partners, the National Security Agency (NSA), and DOD[31] in sharing classified threat-vector information

[26] *Reputation costs* refers to the various forms of economic and other harm that an entity may experience as a result of damage to its reputation with customers or others. For example, if a company experiences a cyberattack in which its customer records are stolen or compromised, and the attack is made public, customers may switch to other companies for which attacks have not been made public, whether or not they have occurred.

[27] Notable examples include the chemical industry, electricity, financial, and transportation sectors.

[28] See, e.g., ISAC Council, "National Council of ISACS," 2014, http://www.isaccouncil.org/.

[29] See, e.g., Department of Homeland Security, "Critical Infrastructure Protection Partnerships and Information Sharing," 2013, http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing.

[30] DIB refers to the Defense Industrial Base, one of the CI sectors identified by DHS.

[31] NSA is a DOD-led agency but has some government-wide responsibilities as a member of the intelligence community.

among stakeholders. One aspect was sharing by the NSA of threat signatures obtained through its computer monitoring activities.[32]

In May 2012, DOD established the DIB Cybersecurity/Information Assurance (CS/IA) Program,[33] making it broadly available to all eligible DIB partners. Under the program, DOD provides defense contractors with classified and unclassified cyberthreat information and cybersecurity best practices, while DIB participants report cyber-incidents, coordinate on mitigation strategies, and participate in cyber intrusion damage assessments if DOD information is compromised. Participating companies may also join an optional classified-information sharing subprogram, known as the DIB Cybersecurity Enhancement Program (DECS)—the former DIB Cyber Pilot[34]—by meeting specified security requirements.

To expand the program beyond the DIB sector, DHS established the Joint Cybersecurity Services Pilot (JCSP) in January 2012, the first phase of which focused on the DECS program and shifted operational relationships with participating commercial service providers (CSPs) to DHS. DHS made the program permanent in July 2012. In January 2013, the department named the program Enhanced Cybersecurity Services (ECS) and expanded it to all CI sectors, including the federal sector,[35] as well as nonfederal government entities.[36] In this program, DHS does not share threat indicators with CI entities directly but rather with participating CSPs (see **Figure 1**). DOD still serves as the point of contact for participating DIB contractors.[37]

The executive order builds on such established programs by requiring the Secretary of Homeland Security to

- expand ECS to all CI sectors;
- expedite processing of security clearances to appropriate CI personnel; and
- expand programs to place relevant private-sector experts in federal agencies on a temporary basis.

It also requires the Secretary of Homeland Security and the Attorney General to expedite collection of threat indicators and dissemination of them to targeted entities.

[32] The program may in some ways be considered a private-sector version of DHS's EINSTEIN 3 cybersecurity initiative for federal systems (see, for example, Department of Homeland Security, *Privacy Impact Assessment for the Enhanced Cybersecurity Services (ECS)*, January 16, 2013, http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf).

[33] 32 C.F.R. Part 236.

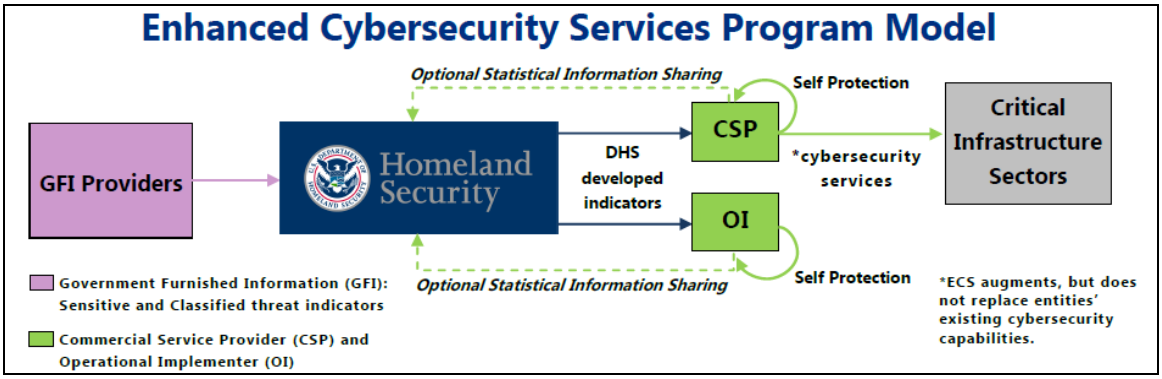
[34] John Reed, "DoD-DHS' Info Sharing Program on Cyber Threats Isn't Shrinking (Updated)," *Foreign Policy: Killer Apps*, October 9, 2012, http://killerapps.foreignpolicy.com/posts/2012/10/09/dod_dhs_cyber_threat_info_sharing_program_isnt_shrinking.

[35] Department of Homeland Security, *Privacy Impact Assessment for ECS*.

[36] Department of Homeland Security, "Enhanced Cybersecurity Services," September 8, 2014, http://www.dhs.gov/enhanced-cybersecurity-services.

[37] Ibid.

Figure 1. Schematic Description of ECS Information-Sharing Process



Source: Department of Homeland Security, "Enhanced Cybersecurity Services," November 14, 2014, http://www.dhs.gov/sites/default/files/publications/ECS-Fact-Sheet.pdf.

Voluntary Cybersecurity Framework

The increasing potential for attacks that might cripple components of CI or otherwise damage the national economy, as discussed above, has led to debate about the best ways to protect those sectors beyond improvements in information sharing. Some CI sectors are subject to federal regulation with respect to cybersecurity,[38] while the protection of others relies largely on voluntary efforts. The efficacy of that mix of voluntary and regulatory efforts has been a prominent issue in the ongoing debate about federal cybersecurity legislation. Proponents of additional regulation argue that the voluntary approach has not provided sufficient protection and that regulation has been effective in sectors such as electricity and financial services. Opponents argue that expanding federal requirements would be costly and ineffective and may impede innovation. Also, there has appeared to be some uncertainty about the extent to which existing statutory authority would permit new cybersecurity requirements in some sectors.

E.O. 13636 builds on the involvement of the National Institute of Standards and Technology (NIST) in the development of cybersecurity technical standards[39] and its statutory responsibilities to work with both government and private entities on various aspects of standards and technology.[40] The order requires the following:

- *NIST*—lead the development of the Cybersecurity Framework, an effort that uses an open, consultative process to reduce cybersecurity risks to CI; focuses on cross-sector, voluntary consensus standards and business best practices; is technology-neutral; identifies areas for improvement; and is reviewed and updated as necessary.

[38] For discussion of regulations on security of information systems for some CI sectors, see Government Accountability Office, *Information Technology: Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors,* GAO-08-1075R, September 16, 2008, http://www.gao.gov/assets/100/95747.pdf.

[39] See, e.g., National Institute of Standards and Technology, "Computer Security Resource Center," December 8, 2014, http://csrc.nist.gov/.

[40] 15 U.S.C. §272.

- *Secretary of Homeland Security*—set performance goals for the framework, establish a voluntary program to support its adoption, and coordinate establishment of incentives for adoption.
- *Sector-specific agencies*—coordinate review of the framework and development of sector-specific guidance, and report annually to the President on participation by CI sectors.
- *CI regulatory agencies*—engage in consultative review of the framework, determine whether existing cybersecurity requirements are adequate, and report to the President whether the agencies have authority to establish requirements that sufficiently address the risks (it does not state that the agencies must establish such requirements, however), propose additional authority where required, and identify and recommend remedies for ineffective, conflicting, or excessively burdensome cybersecurity requirements.

The executive order stipulates that it provides no authority for regulating critical infrastructure in addition to that under existing law, and it does not alter existing authority.

The development of the framework is arguably the most innovative and labor-intensive requirement in the executive order. 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 was envisioned by the executive order. Hundreds of entities have been involved in NIST's efforts, which led to release of the first version of the framework in February 2014.[41]

The framework is intended to provide broad guidance on cybersecurity using a risk-based approach that can be adapted to the needs of different CI sectors. It consists of three parts:

- The *core* is a common set of activities and outcomes applicable to all CI sectors It is organized into five functions—*identify, protect, detect, respond,* and *recover*—that are widely recognized components of any cybersecurity management lifecycle, along with associated programmatic and technical outcomes, for example, "access control" and "data-at-rest is protected."[42]
- The *profile* describes an entity's current and target cybersecurity postures, based on business needs identified by considering the relevant *core* components. It can be used to support prioritization of action and measurement of progress. The current profile lists outcomes that are being achieved, while the target profile lists the outcomes needed to achieve desired cybersecurity goals.
- The *implementation tiers* characterize an entity's current and intended practices, which can range from "informal, reactive responses" (Tier 1) to "agile and risk-informed" approaches (Tier 4).[43]

[41] National Institute of Standards and Technology, "Cybersecurity Framework," August 26, 2014, http://www.nist.gov/cyberframework/index.cfm.

[42] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. The core also includes relevant references, such as publications by NIST and other organizations, for each outcome.

[43] Ibid.

The framework is not intended to be static but will be updated as required. Areas that NIST has already identified for improvement include authentication, automated sharing of indicators, assessment of the degree of conformity to risk-management requirements, cybersecurity workforce needs, data analytics, supply-chain risk management, technical standards relating to privacy, alignment of the framework with federal agency cybersecurity requirements, and international aspects and implications.[44] Several of those are broadly recognized as key issues in cybersecurity.

To assist in adoption and implementation of the framework by CI entities, DHS has developed the Critical Infrastructure Cyber Community C³ Voluntary Program. Its goals are to help CI entities understand and use the framework and obtain feedback from them on improvements.[45]

Other Provisions

The executive order contains several additional provisions on CI cybersecurity:

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.

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.

[44] National Institute of Standards and Technology, "NIST Roadmap for Improving Critical Infrastructure Cybersecurity," February 12, 2014, http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

[45] Department of Homeland Security, "About the Critical Infrastructure Cyber Community C³ Voluntary Program," May 21, 2014, http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program.

E.O. 13636 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.[46] Several deliverables have 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)).[47]
- Recommendations to the President on incentives to participate in the framework (Secretaries of Homeland Security, Commerce, and the Treasury) (Sec. 8(d)).[48]
- Recommendations to the President on acquisitions and contracts (Secretary of Defense, Administrator of General Services) (Sec. 8(e)).[49]

July 12, 2013

- Designation of critical infrastructure at greatest risk (Secretary of Homeland Security) (Sec. 9(a)).[50]

October 10, 2013

- Publication of preliminary Cybersecurity Framework (Director of the National Institute of Standards and Technology) (Sec. 7(e)).[51]

---

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

[47] Department of Homeland Security, "Enhanced Cybersecurity Services."

[48] Department of Homeland Security Integrated Task Force, *Executive Order 13636: Improving Critical Infrastructure Cybersecurity: Incentives Study Analytic Report*, June 12, 2013, http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf; Department of Commerce, *Recommendations to the President on Incentives for Critical Infrastructure Owners and Operators to Join a Voluntary Cybersecurity Program*, August 6, 2013, http://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Recommendations_Final.pdf; Department of the Treasury, *Summary Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636*, August 6, 2013, http://www.treasury.gov/press-center/Documents/Treasury%20Report%20(Summary)%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf.

[49] Department of Defense and General Services Administration, *Improving Cybersecurity and Resilience through Acquisition*, November 2013, http://www.gsa.gov/portal/mediaId/185367/fileName/IMPROVING_CYBERSECURITY_AND_RESILIENCE_THROUGH_ACQUISITION.action.

[50] See Statement of Robert Kolasky, Department of Homeland Security, *Oversight of Executive Order 13636 and Development of the Cybersecurity Framework*, Before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, July 18, 2013, http://docs.house.gov/meetings/HM/HM08/20130718/101151/HHRG-113-HM08-Wstate-KolaskyR-20130718.pdf.

[51] National Institute of Standards and Technology, *Preliminary Cybersecurity Framework*, October 22, 2013, http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

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)).[52]
- Publication of final Cybersecurity Framework (Director of the National Institute of Standards and Technology) (Sec. 7(e)).[53]

May 13, 2014

- Reports to the President on review of regulatory requirements (agencies with regulatory responsibilities for critical infrastructure) (Sec. 10(a)).[54]
- Proposed additional risk mitigation actions (agencies with regulatory responsibilities for critical infrastructure) (Sec. 10(b)).[55]

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. Some of the deliverables have been made publicly available, largely in accordance with the deadlines in the order, as noted above in the footnotes. Some provisions appeared to have had some effect soon after the order was issued. For example, the provision on expedited security clearances was apparently used to facilitate communication by the FBI with banks in response to a cyberattack in the spring of 2013 on several banks.[56]

The assessments of regulatory requirements and proposed actions focused on three agencies: DHS, the Environmental Protection Agency (EPA), and the Department of Health and Human Services (HHS). The Administration concluded that "existing regulatory requirements, when complemented with strong voluntary partnerships, are capable of mitigating cyber risks to our critical systems and information."[57]

[52] Department of Homeland Security, The Privacy Office and the Office for Civil Rights and Civil Liberties, *Executive Order 13636: Privacy and Civil Liberties Assessment Report*, April 2014, http://www.dhs.gov/sites/default/files/publications/2014-privacy-and-civil-liberties-assessment-report.pdf.

[53] National Institute of Standards and Technology, "Cybersecurity Framework."

[54] Michael Daniel, "Assessing Cybersecurity Regulations," *The White House Blog*, May 22, 2014, http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations.

[55] Ibid.

[56] 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.

[57] Daniel, "Assessing Cybersecurity Regulations." The document notes that the executive order does not apply to independent regulatory agencies.

Relationship of the Executive Order to Presidential Policy Directive 21

Presidential Policy Directive 21 (PPD 21),[58] *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 17, 2003. The PPD 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.

PPD 21 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).[59]

July 12, 2013

- Analysis of public-private partnership models with recommended improvements (Secretary of Homeland Security).[60]

August 11, 2013

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

[58] The White House, "PPD 21."

[59] Department of Homeland Security Integrated Task Force, "National Infrastructure Protection Plan Update – Public Slides for National Infrastructure Advisory Council," July 17, 2013, http://www.dhs.gov/sites/default/files/publications/final-niac-brief-2013-07-11-v2-expanded.pdf.

[60] Ibid.

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).[61]

February 12, 2015

- First quadrennial National Critical Infrastructure Security and Resilience R&D Plan (Secretary of Homeland Security).[62]

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.[63]

Scope of Presidential Authority

E.O. 13636 was issued in the wake of the lack of enactment of cybersecurity legislation in the 112th Congress, apparently at least in part as a response to that.[64] That raises questions about what authority the President has to act on this matter through an executive order. That issue is discussed below.

The issuance of an executive order frequently raises questions about whether the order exceeds the scope of the President's authority, in relation to the constitutional separation of powers and validly enacted legislation. Since the latter half of the 20th century, these questions have typically been evaluated using the tripartite framework set forth by U.S. Supreme Court Justice Jackson in his concurring opinion in the case of *Youngstown Sheet & Tube Company v. Sawyer*.[65] First, if the President has acted according to an express or implied grant of congressional authority, presidential "authority is at its maximum." Second, in situations where Congress has neither granted nor denied authority to the President, the President acts in reliance only "upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain." Third, in instances where presidential action is "incompatible with the express or implied will of Congress," the power of

[61] This document was not released on October 10, with a draft version reportedly criticized by industry representatives (see Jason Miller, "Industry, DHS at Odds Over Draft Plan to Secure Critical Infrastructure," *Federal News Radio*, November 4, 2013, http://www.federalnewsradio.com/473/3497578/Industry-DHS-at-odds-over-draft-plan-to-secure-critical-infrastructure).

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

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

[64] The White House, "Executive Order on Improving Critical Infrastructure Cybersecurity" Press Release, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0 (describing Executive Order as a "down-payment on expected further legislative action").

[65] 343 U.S. 579, 634 (1952).

the President is at its minimum. In such a circumstance, presidential action must rest upon an exclusive Article II power.

As an example of the first category, Congress has previously provided explicit statutory authority for the executive to regulate the security of private entities.[66] For example,[67] chemical facilities are subject to chemical facility anti-terrorism standards (CFATS) promulgated by the Department of Homeland Security (DHS), which include provisions requiring chemical facilities to take measures to protect against cyberthreats.[68] Similarly, the Maritime Transportation Security Act (MTSA) gives the Coast Guard the authority to regulate the security of maritime facilities and vessels, including requiring security plans that contain provisions for the security of communications systems used in those facilities.[69] In these and other situations where Congress has provided explicit regulatory authority to the executive branch related to cybersecurity, the President's authority to direct sector-specific agencies to coordinate, evaluate, develop, or implement appropriate cybersecurity standards pursuant to the executive order[70] would appear to be at its maximum.

In other cases, where there may only be congressional silence regarding the President's authority to direct action on cybersecurity issues, an argument could be made that the issuance of such an executive order falls within the "zone of twilight," assuming that the action could be concurrently justified under some explicit or implied power granted to the President by the Constitution. For example, Section 9 of E.O. 13636 directs the Secretary of Homeland Security to use a risk-based approach to identify critical infrastructure where a cybersecurity incident could result in catastrophic effects.[71] While such identification is arguably authorized under the Homeland Security Act of 2002,[72] it might alternatively be justified under the President's constitutional authority to request written opinions from the heads of executive departments.[73]

However, some past legislative proposals may be beyond the reach of unilateral executive action. For example, prior proposals to regulate the cybersecurity of critical infrastructure have also proposed limits on liability or safe harbors for regulated entities that comply with the regulatory schemes,[74] because the creation of a regulatory scheme can have an adverse effect on the

---

[66] See also Government Accountability Office, *Federal Laws, Regulations, and Mandatory Standards*.

[67] The existing regulatory frameworks discussed here do not constitute an exhaustive list of all regulations applicable to critical infrastructure, but are only intended to provide some context for the following discussions.

[68] P.L. 109-295, §550 (codified at 6 U.S.C. §121 note). For a more detailed discussion of CFATS, see CRS Report R41642, *Chemical Facility Security: Issues and Options for the 112th Congress*, by Dana A. Shea.

[69] 46 U.S.C. §§70102-70103.

[70] E.O. 13636, §10.

[71] E.O. 13636, §9(a).

[72] See, e.g., 6 U.S.C. §121(d)(2) (directing the Secretary to carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States to determine the risks posed by particular types of terrorist attacks).

[73] U.S. Constitution, article I, §2, clause 1 ("[the President] may require the Opinion, in writing, of the principal Officer in each of the executive Departments, upon any Subject relating to the Duties of their respective Office").

[74] See, e.g., S. 3414 §104(c)(1) (112th Cong.) (barring the award of punitive damages against any regulated entity arising out of a cyber-incident if the entity is in substantial compliance with voluntary cybersecurity practices established under the bill). Exposure to civil liability may also be increased if an entity receives information about a cyberthreat (as under §4 of the Executive Order) and fails to take reasonable measures to defend against or mitigate that threat.

exposure of regulated entities to civil liability.[75] The scope of such proposed limits has ranged from complete immunity, to lesser restrictions such as prohibitions against the awarding of punitive damages. Such limits on liability may also be made dependent upon an entity's satisfaction of its regulatory obligations, in order to create a further incentive for compliance.

The abrogation of civil claims under common law or contract law without explicit congressional authorization may be difficult to justify on the executive's constitutional powers alone. Notably, the executive order does not purport to provide any similar liability safe harbors for private entities that comply with cybersecurity standards developed pursuant to the executive order. While it does direct the Secretary of Homeland Security to coordinate the establishment of a set of incentives to promote voluntary participation in the critical infrastructure program, it also acknowledges that some incentives may require legislation affirmatively authorizing such limitations.[76] This is not to say that the executive order will have no impact on liability. The publication of recommendations or risk assessments, as provided under the executive order, may be used by litigants as evidence of the appropriate standard of care to apply in tort litigation resulting from a cybersecurity incident, even if such standards are not controlling.[77]

Similarly, it may not be possible for an executive order to authorize telecommunications providers to engage in more aggressive monitoring of communications networks to help identify cyber threats or attacks in real-time. Such an executive action would contravene current federal laws protecting electronic communications, and would be evaluated in the third category of Justice Jackson's *Youngstown* framework, where the President's power is at its minimum. Such an executive order would not be effective, unless such action fell within a power exclusively granted to the executive by the Constitution. Consistent with this analysis, E.O. 13636 does not purport to provide any authority for private telecommunications providers to engage in monitoring of their networks.

Relationship to Legislative Proposals

While E.O. 13636 does not purport to create new authorities, there are commonalities between some of its provisions and some of the cybersecurity proposals from the 112th and 113th Congresses. A comparison of a selection of the issues covered by those proposals and the executive order is below.[78]

Several comprehensive legislative proposals on cybersecurity in the 112th Congress received considerable attention, including a Senate bill, a set of bill proposals by the Obama

[75] See Restatement (Third) of Torts: Product Liability §4 (b) ("[a] product's compliance with an applicable product safety statute or administrative regulation is properly considered in determining whether the product is defective with respect to the risks sought to be reduced by the statute or regulation").

[76] E.O. 13636, §8(d) (Feb. 12, 2013). When developing the incentives, the Secretary is required to note "whether the incentives would require legislation or can be provided under existing law and authorities."

[77] See, e.g., *Burmaster v. Gravity Drainage Dist. No. 2*, 448 So. 2d 162, 164 (La. Ct. App. 1984) (Occupational Safety and Health Act regulations and standards published by industry groups warrant consideration as evidence of standard of care, even if they are not controlling).

[78] For more information on the current legislative framework for cybersecurity, including discussion of provisions in legislative proposals in the 112th and 113th Congresses, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

Administration, and a report with recommendations from a House Republican task force,[79] which informed several House bills. The various proposals differed both in some of the issues they addressed and in how they approached them. Among the issues addressed were the following:

- Cybersecurity workforce authorities and programs,
- Cybersecurity R&D,
- Data-breach notification,
- DHS authorities for protection of federal systems,
- FISMA reform,
- Information sharing,
- Penalties for cybercrime,
- Protection of privately held CI, including public/private sector collaboration and regulation of privately held CI,
- Public awareness about cybersecurity, and
- Supply-chain vulnerabilities.

E.O. 13636 mainly addresses two of those topics: information sharing and protection of privately held CI. With respect to information sharing, the executive order does not provide exemptions from liability stemming from information sharing, which would require changes to current law. Several of the legislative proposals included such changes. Also, some proposals included the creation of new entities for information sharing, whereas the executive order uses existing mechanisms.

With respect to protection of critical infrastructure, the provisions on designation of CI and identification of relevant regulations are related to those in some legislative proposals in the 112th Congress. The role of NIST in developing the Cybersecurity Framework was not in the legislative proposals from that Congress, although several would have expanded the agency's role in cybersecurity.

In the 113th Congress, H.R. 624 and S. 2588 would address information sharing, and H.R. 3696 and S. 1353 would require NIST to lead a public/private effort similar to the process by which the Cybersecurity Framework is being developed. Both House bills passed in the House, H.R. 694 in April 2013 and H.R. 3696 in July 2014, but some provisions in each were controversial.[80]

Reactions to the Executive Order

Given the absence of enacted comprehensive cybersecurity legislation, some security observers have contended that the executive order is a necessary step in securing vital assets against

[79] House Republican Cybersecurity Task Force, *Recommendations of the House Republican Cybersecurity Task Force*, October 5, 2011, http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf.

[80] See, for example, The White House, "H.R. 624—Cyber Intelligence Sharing and Protection Act," Statement of Administration Policy, April 16, 2013, http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr624r_20130416.pdf.

cyberthreats. Proponents of the framework point to its ability to alleviate the problems created by a lack of understanding about cybersecurity issues and practices among different classes of stakeholders. They claim that the framework provides a common, nontechnical basis for developing consensus on how best to approach cybersecurity needs.[81]

Other observers, however, have raised concerns.[82] Common themes by such critics have included 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 have delayed implementation of needed security measures,[83] creating 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 may be insufficient, given that the process for developing and updating consensus standards often takes several years. In fact, some CI entities have reportedly delayed implementation while waiting for additional federal guidance.[84] Some also state that the framework process does not preclude entities from adopting established security measures immediately.

[81] See, for example, Jack Whitsitt, "Framing the Future," *CForum*, December 5, 2014, http://cyber.securityframework.org/blog/11/entry-10-framing-the-future/.

[82] 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/.

[83] 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).

[84] John Reosti, "Feds Leaning Toward Incentives to Boost Cyber Security Framework," *Credit Union Journal*, November 14, 2014, http://www.cujournal.com/news/feds-leaning-toward-incentives-to-boost-cyber-security-framework-1023493-1.html.

- 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 the executive order could lead to government intrusiveness into private-sector activities, for example through increased regulation under existing statutory authority,[85] 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.[86]
- 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.[87] This might be particularly a problem if the criteria are not sufficiently validated.[88]

It appears to be too early in the implementation of the executive order to determine how effectively 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 largely positive. Some organizations and experts have urged adoption of the framework by CI entities.[89]

---

[85] 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). See also Homeland Security News Wire, "Cybersecurity Business Cyberwarfare Critical Infrastructure," March 3, 2014, http://www.homelandsecuritynewswire.com/dr20140303-nist-s-voluntary-cybersecurity-framework-may-be-regarded-as-de-facto-mandatory.

[86] Mike McConnell et al., *The Cybersecurity Executive Order* (Booz Allen Hamilton, April 26, 2013), http://www.boozallen.com/media/file/BA13-051CybersecurityEOVP.pdf.

[87] 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.

[88] 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).

[89] See, for example, PricewaterhouseCoopers, "Why You Should Adopt the NIST Cybersecurity Framework," May 9, 2014, http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf; Luis A. Aguilar, "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus" (presented at the Cyber Risks and the Boardroom, New York Stock Exchange, New York, NY: Securities and Exchange Commission, 2014), http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.VI8v-8kXMo0; Paul A. Ferrillo and Tom Conkle, "Guest Post: Cybersecurity and Cyber Governance: Understanding and Implementing the NIST Cybersecurity Framework," *The D&O Diary*, August 13, 2014, http://www.dandodiary.com/2014/08/articles/uncategorized/guest-(continued...)

In August 2014, NIST requested public comments on implementation of the framework and posted more than 60 it received from various companies, trade associations, and other organizations.[90] The responses demonstrate a range of understanding and implementation both across and within sectors and generally support the contention that additional experience will be necessary before the success of the framework at improving CI cybersecurity can be adequately assessed.

Author Contact Information

Eric A. Fischer
Senior Specialist in Science and Technology
efischer@crs.loc.gov, 7-7071

Edward C. Liu
Legislative Attorney
eliu@crs.loc.gov, 7-9166

John W. Rollins
Specialist in Terrorism and National Security
jrollins@crs.loc.gov, 7-5529

Catherine A. Theohary
Specialist in National Security Policy and Information Operations
ctheohary@crs.loc.gov, 7-0844

(...continued)

post-cybersecurity-and-cyber-governance-understanding-and-implementing-the-nist-cybersecurity-framework/.

[90] National Institute of Standards and Technology, "RFI—Framework for Reducing Cyber Risks to Critical Infrastructure," October 23, 2014, http://csrc.nist.gov/cyberframework/rfi_comments_10_2014.html.