

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 Rollins
Specialist in Terrorism and National Security

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

March 1, 2013

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

CRS Report for Congress
Prepared for Members and Committees of Congress
c11173008

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, no major legislation on this topic has been enacted since the Federal Information Security Management Act (FISMA) in 2002, which addressed the security of federal information systems. In February 2013, the White House issued an executive order designed to improve the cybersecurity of U.S. critical infrastructure (CI). Citing repeated cyber-intrusions into critical infrastructure and growing cyberthreats, Executive Order 13636, *Improving Critical Infrastructure Cybersecurity,* attempts 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.

Given the absence of comprehensive cybersecurity legislation, some security observers contend that E.O. 13636 is a necessary step in securing vital assets against cyberthreats. Others have expressed the view, in contrast, that the executive order could make enactment of a bill less likely or could lead to government intrusiveness into private-sector activities, for example through increased regulation under existing statutory authority.

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

- expanding to other CI sectors an existing Department of Homeland Security 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 to lead in developing a Cybersecurity Framework of standards and best practices for protecting CI; and
- requiring regulatory agencies to determine the adequacy of current requirements and their authority to establish requirements to address the risks.

Among the major issues covered by 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. 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. The role of NIST in developing the Cybersecurity Framework appears to be unique to E.O. 13636.

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.

Contents

Background: Threats and Consequences 1
Cyberthreats 2
Cyberterrorists 2
Cyberspies 2
Cyberthieves 3
Cyberwarriors 3
Cyberhacktivists 4
Cyberthreats and Implications for U.S. Policy 4
Overview of the Executive Order 5
Scope of Presidential Authority 8
Relationship to Legislative Proposals 10

Contacts

Author Contact Information 12

The federal legislative framework for cybersecurity is complex, with more than 50 statutes addressing various aspects of it either directly or indirectly. Many observers do not believe that the current framework is sufficient to address the growing concerns about the security of cyberspace in the United States.[1] However, no major cybersecurity legislation has been enacted since 2002. Several legislative proposals were made during the 112th Congress to close the gaps, but none were enacted.

On February 12, 2013, President Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*.[2] 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 legislative and constitutional authority for the executive order?
- How do its provisions relate to those in the major legislative proposals in the 112th and 113th Congresses?

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.[3]

Cyberthreats to U.S. infrastructure and other assets are a growing concern to policymakers. Information and communications technology (ICT)[4] 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.

[1] For a discussion of this legislative framework, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, by Eric A. Fischer.

[2] 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 the recently released National Intelligence Estimate addressing cyberthreats to the Nation.

[3] Ibid.

[4] 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.

Cyberthreats

Cyber-based technologies[5] 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.

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.[6] While no unclassified reports have been published regarding a terrorist-initiated cyberattack on U.S. critical infrastructure (CI),[7] 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.[8]

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

[5] 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.

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

[7] 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."

[8] 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 Rollins, and Catherine A. Theohary.

overnight."[9] 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."[10] 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."[11] 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."[12] A February 2013 report of an investigation by a private-sector security firm of intrusions 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.[13]

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.[14] 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.[15] 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

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

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

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

[12] Ibid.

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

[14] 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 M. Finklea.

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

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.[16] However, other observers suggest that the perpetrator of the attack was an employee of Saudi Aramco.[17]

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 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.[18] 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.[19] The threats posed by these aggressors, coupled with the United States' proclivity to be an early adopter of emerging technologies,[20] 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.

[16] 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.

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

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

[19] 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.

[20] 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 Global Trends 2030: Alternative Worlds, National Intelligence Council, Office of the Director of National Intelligence, December 10, 2012.

Overview of the Executive Order

The federal role in what is now called cybersecurity[21] has been debated for more than a decade, with much of the debate focusing on two issues: sharing of cybersecurity-related information within and across sectors, and the cybersecurity of CI sectors, including federal systems. 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,[22] protection of proprietary information, antitrust law, and misuse of shared information. A few sectors are subject to federal notification requirements,[23] but most such information sharing is voluntary, often through sector-specific Information Sharing and Analysis Centers (ISACs)[24] or programs under the auspices of the Department of Homeland Security (DHS) or sector-specific agencies.[25] 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.

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 way to protect those sectors, especially whether voluntary efforts are sufficient or additional federal regulation is required. Also, while some sectors are clearly subject to federal regulation with respect to cybersecurity, it is not clear how broadly federal authority applies in this area.[26]

One especially notable voluntary effort, established in May 2011, was a program known as the DIB[27] Cyber Pilot that involved several defense industry partners, the National Security Agency (NSA), and DOD,[28] to share classified threat-vector information among stakeholders. One aspect

[21] *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*.

[22] *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 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.

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

[24] See, e.g., ISAC Council, "National Council of ISACS," 2013, http://www.isaccouncil.org/.

[25] 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.

[26] 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.

[27] DIB refers to the Defense Industrial Base, one of the 18 CI sectors identified by DHS.

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

was sharing by the NSA of threat signatures obtained through its computer monitoring activities.[29]

DOD established the DIB Cybersecurity/Information Assurance (CS/IA) Program[30] in May 2012, 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)—formerly known as the DIB Cyber Pilot[31]—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. In January 2013, the department named the program Enhanced Cybersecurity Services (ECS) and expanded it to all CI sectors, including the federal sector. In this program, DHS does not share threat indicators with CI entities directly but rather with participating CSPs. DOD still serves as the point of contact for participating DIB contractors.[32]

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;
- expand programs to place relevant private-sector experts in federal agencies on a temporary basis;
- establish a broad consultative process to coordinate improvements in CI cybersecurity;
- using consistent and objective criteria, the consultative process, and information from relevant stakeholders, identify and update annually a list of CI for which a cyberattack could have catastrophic regional or national impact, but not including commercial IT products or consumer IT services;
- confidentially notify owners and operators of identified CI of their designation and provide a process for them to request reconsideration; and

[29] 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 Update for the Joint Cybersecurity Services Program (JCSP), Defense Industrial Base (DIB – Enhanced Cybersecurity Services (DECS)*, July 18, 2012, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_livewave.pdf).

[30] 32 C.F.R. Part 236.

[31] 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.

[32] Ibid.

- coordinate technical assistance to CI regulatory agencies on development of their cybersecurity workforce and programs.

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; and
- coordination and assessment of privacy and civil liberties protections with respect to agency activities under the executive order, including protection of submitted information, with a report on the assessment and recommendations.

E.O. 13636 builds on the involvement of the National Institute of Standards and Technology (NIST) in the development of cybersecurity technical standards[33] by requiring 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.
- Secretary of Homeland Security—establish a voluntary program to support adoption of the framework 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.
- The Secretary of Defense and the Administrator of General Services—make recommendations to the President on incorporating security standards in acquisition and contracting processes, including harmonization of cybersecurity requirements.
- 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.

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.[34] That raises questions about what

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

[34] 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").

authority the President has to act on this matter through an executive order. That issue is discussed below.

Scope of Presidential Authority

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*.[35] 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 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.[36] For example,[37] 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.[38] 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.[39] 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[40] 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

[35] 343 U.S. 579, 634 (1952).

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

[37] 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.

[38] 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.

[39] 46 U.S.C. §§70102-70103.

[40] E.O. 13636, §10.

catastrophic effects.[41] While such identification is arguably authorized under the Homeland Security Act of 2002,[42] it might alternatively be justified under the President's constitutional authority to request written opinions from the heads of executive departments.[43]

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,[44] because the creation of a regulatory scheme can have an adverse effect on the exposure of regulated entities to civil liability.[45] 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.[46] 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.[47]

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

[41] E.O. 13636, §9(a).

[42] 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).

[43] 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").

[44] 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.

[45] 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").

[46] 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."

[47] 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).

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 Congress. A comparison of a selection of the issues covered by those proposals and the executive order is below.[48]

Several comprehensive legislative proposals on cybersecurity received considerable attention in the 112th Congress. They included

- The Cybersecurity Act of 2012 (CSA 2012, S. 2105), a comprehensive cybersecurity bill.
- A revised version of that bill, S. 3414, which was debated in the Senate but failed two cloture votes.
- The SECURE IT Act (S. 2151 and a refined version, S. 3342), an alternative to S. 3414.
- Recommendations from a House Republican task force,[49] which informed several House bills.
- A proposal by the Obama Administration (the White House Proposal).

While those proposals differed both in some of the issues addressed and in how they approached them, all addressed the following issues:

- Cybersecurity workforce authorities and programs.
- Cybersecurity R&D.
- FISMA reform.
- Information sharing.

All except S. 3342 (and S. 2151) addressed

- DHS authorities for protection of federal systems.
- Protection of privately held CI, including public/private sector collaboration and regulation of privately held CI.

[48] For more information on how legislative proposals in the 112th Congress would have addressed cybersecurity, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, by Eric A. Fischer.

[49] 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.

- Supply-chain vulnerabilities.
- Public awareness about cybersecurity.

Four narrower bills passed the House but were not considered by the Senate:

- Cybersecurity Enhancement Act of 2011 (H.R. 2096), which addressed federal cybersecurity R&D and the development of technical standards (H.R. 756 has been introduced in the 113th Congress).
- Cyber Intelligence Sharing and Protection Act (H.R. 3523, reintroduced in the 113th Congress as H.R. 624), which focused on information sharing and coordination, including sharing of classified information;
- Advancing America's Networking and Information Technology Research and Development Act of 2012 (H.R. 3834), which addressed R&D in networking and information technology, including but not limited to security; and
- Federal Information Security Amendments Act of 2012 (H.R. 4257), which addressed FISMA reform.

One was ordered reported out of the full committee but did not come to the floor:

- Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011 or PRECISE Act of 2011 (H.R. 3674), which addressed the role of the Department of Homeland Security in cybersecurity, including protection of federal systems, personnel, R&D, information sharing, and public/private sector collaboration in protecting critical infrastructure.

Some bills and the White House Proposal also addressed

- Data-breach notification.
- Penalties for cybercrime.

Among the 10 topics covered by legislative proposals in the last Congress, E.O. 13636 mainly addresses two: information sharing and protection of privately held critical infrastructure. 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. The role of NIST in developing the Cybersecurity Framework appears to be unique to the executive order. While NIST's role is expanded in several of the legislative proposals, provisions relating to the designation of the standards, practices, and so forth that comprise the framework focused on new entities such as the National Cybersecurity Council proposed in S. 3414 or the National Information Sharing Organization proposed in the introduced version of H.R. 3674.

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

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