# The Cybersecurity Overreach: A Few Harsh Words About the President's Cybersecurity Executive Order, Along with a Better Solution

*By Patricia Paoletta**

## Note from the Editor:

This article is a discussion about Executive Order 13636 on cybersecurity infrastructure. As always, the Federalist Society takes no position on particular legal or public policy initiatives. Any expressions of opinion are those of the author. The Federalist Society seeks to further discussion on cybersecurity. To this end, we offer links below to different perspectives on the issue, and we invite responses from our audience. To join this debate, please email us at info@fed-soc.org.

## Related Links:

- Exec. Order No. 13,636, 78 Fed. Reg. 11739 (2013): http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
- Jessica Vosgerchian, *Executive Order Promotes Public-Private Collaboration to Protect Critical Infrastructure from Cyber Threats*, Jolt digest, Harvard J.L. & Tech., Feb. 19, 2013: http://jolt.law.harvard.edu/digest/internet/executive-order-promotes-public-private-collaboration-to-protect-critical-infrastructure-from-cyber-threats
- Mike McConnell et al., The Cybersecurity Executive Order: Exploiting Emerging Technologies and Practices for Collaborative Success, Booz Allen Hamilton (2013): http://www.boozallen.com/media/file/BA13-

### Introduction

Few topics are worthier of public debate than enhancing U.S. cybersecurity. Former Secretary of Defense Leon Panetta stated that the collective result of attacks on our nation's critical infrastructure could be "a cyber Pearl Harbor."[1] At present, much of the U.S. fleet of critical infrastructure floats vast and unprotected. Almost every aspect of modern life intersects with or depends on the use of information and communications technology—transportation, defense, electricity, water, healthcare, and agriculture are just a few examples. Each is prey to the spies, terrorists, hackers, and hostile foreign governments that operate online.

All agree that the U.S. is vulnerable to cyberattack, but there is broad disagreement regarding how to mitigate this risk. The 112th Congress hotly debated this issue, weighing a number of legislative measures to improve cybersecurity. The debate divided Congress into two camps: one camp advocating for a regulatory approach, focused on top-down restrictions imposed on private industry by regulatory agencies; and the other camp advocating for a voluntary approach based on cooperation with the private sector, focused on information sharing between private industry and government. The parties' positions on the private sector's protection from liability—granted in wireless and wireline communications precedents—prevented agreement in legislation.

When the Senate defeated a bill that adopted the former approach, President Obama took matters into his own hands, issuing Executive Order ("EO") 13636 on improving critical infrastructure cybersecurity.[2] Though its aims were praiseworthy, the EO was ill-advised. The EO itself was a half-measure, attempting to fight sophisticated and rapidly evolving cybersecurity threats with the slow and cumbersome tools of regulation. Worse, the EO's issuance interrupted a productive and lively debate in Congress on how best to involve the private sector in cybersecurity. While the President has the authority to execute existing legislation, new obligations on the private sector and on interstate commerce must be passed by Congress.[3]

This article (1) examines how the White House may have used the EO to circumvent these limitations; (2) briefly discusses flaws with the EO's approach; and (3) endorses a non-regulatory approach based on information sharing with and liability protection for the private sector, such as that adopted by the Cyber Intelligence Sharing and Protect Act ("CISPA").[4]

### I. Cyber Pearl Harbor

The cybersecurity threat is looming and multifarious. Terrorist organizations use the internet as a tool to radicalize and recruit citizens, to distribute propaganda, to plan attacks, and to communicate.[5] Likewise, "cyberspies" use the internet to steal confidential or classified information to gain strategic or competitive advantages.[6] In one example cited in a 2011 FBI report, "one company that was recently the victim of an intrusion . . . lost 10 years worth of research and development—valued at $1 billion—virtually overnight."[7] "Cyberwarriors" conduct cyberattacks on behalf of nation-states; "cyberhacktivists" carry out cyberattacks for philosophical or policy reasons.[8] As a recent white paper noted, "[m]any 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."[9]

Cybersecurity attacks are increasing in frequency and severity. According to one report, "[o]ver the past 6 years, the

*Patricia Paoletta is a partner with the law firm of Wiltshire & Grannis LLP, where she specializes in telecommunications, trade and technology policy. Formerly, Ms. Paoletta served as senior advisor to the International Bureau Chief and Office Director at the Federal Communications Commission, Director of Telecommunications Trade Policy in the Office of the U.S. Trade Representative, and as Majority Counsel to the House Energy and Commerce Committee.

number of cyber incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team ("US-CERT") rose from 5,503 in fiscal year 2006 to 48,562 in fiscal year 2012, an increase of 782 percent.[10] Stories of these attacks are sobering. Recently, the *Washington Post* reported that "[d]esigns for many of the nation's most sensitive advanced weapons systems have been compromised by Chinese hackers."[11] Quoting a confidential report from the Defense Science Board, the *Post* reported that "[a]mong more than two dozen major weapons systems whose designs were breached were programs critical to U.S. missile defenses and combat aircraft and ships." While large defense contractors may have systems sufficiently immune to hackers, subcontractors several layers below the general contractor with whom a federal agency contracts may lack sufficiently secure firewalls or security procedures to prevent intrusion up the chain.

## II. The EO Cuts Short Congress's Debate on Cybersecurity

The Executive Order emerged from the *Sturm und Drang* of the 112th Congress, which saw a number of cybersecurity bills proposed and defeated. Though there was broad support for legislation addressing cybersecurity, the House, Senate, and White House all took a different view of the measures needed to address the problem.[12] Most of the bills proposed contained some combination of the following elements: reform of the Federal Information Security Management Act ("FISMA"), protection of critical infrastructure, information sharing, criminalization of cybercrime, privacy, and the cybersecurity workforce, among other topics.[13]

### *A. The Cybersecurity Debate*

A key difference between the House and Senate approaches to cybersecurity was the role of information sharing. One major House bill—the Cyber Intelligence Sharing and Protection Act ("CISPA")—focused on the sharing of cyberthreat information between private-sector entities and the intelligence community by, among other things, exempting private companies from liability for using cybersecurity systems to gain cyberthreat information and for making decisions based on the use of cyberthreat information gained under CISPA.[14] Critics of the bill claimed that it lacked necessary privacy, confidentiality, and civil liberties safeguards.[15]

The White House frequently waded into these legislative debates. In May 2011, the White House sent a comprehensive, seven-part legislative proposal to Congress.[16] Among other things, this proposal sought to strengthen the criminalization of cybercrimes, establish a national breach reporting system, create a system of cybersecurity information sharing, and mandate that regulatory steps be taken to protect critical infrastructure. The White House strongly disagreed with CISPA's information-sharing approach, particularly its shield of liability for companies that shared cybersecurity information.[17] In April 2012, the White House threatened to veto CISPA if passed, stating that CISPA "would inappropriately shield companies from any suits where a company's actions are based on cyberthreat information identified, obtained, or shared under this bill, regardless of whether that action otherwise violated Federal criminal law or results in damage or loss of life."[18]

Instead, President Obama favored a regulatory approach to cybersecurity that did not provide the private sector the incentive of liability protection.[19] Taking a rare step, he penned an editorial in the *Wall Street Journal* warning of the risks of a cyberattack and urging the Senate to pass the Cyber Security Act of 2012.[20] Among other things, this Act called for the creation of sector-by-sector risk-based cybersecurity performance requirements, which would require owners of critical infrastructure to mitigate cyber risks.

### *B. The Threatened EO*

"When Congress refuses to act . . . I have an obligation as president to do what I can without them," President Obama declared in 2012.[21] That is not a universally shared understanding of the executive power in our representative democracy. "It is a duty he has discharged with vigour and creativity," one commenter retorted.[22] The circumstances surrounding the issuance of EO 13636 put this view of presidential rulemaking on bold display, raising questions about the limits of the president's power under the Constitution.

During the 112th Congress, the White House indicated that it was considering issuing an executive order on cybersecurity that would implement some additional measures for information sharing and protection of critical infrastructure. Members of Congress opposed such action, arguing that an executive order would undermine Congress's effort to pass sorely needed cybersecurity legislation. In one example, a letter from Senators Susan Collins, Richard Lugar, and Olympia Snowe urged President Obama to refrain from issuing an Executive Order:

> The ramifications of a national cybersecurity policy for the public and private sectors are significant and deserve the transparency and legitimacy that can be achieved only though the legislative process. Moreover, an Executive Order could have the unintended consequence of undermining the need for Congress to act by lulling people into a false sense of security that the problem has been "solved" through executive action.
>
> Only the legislative process can provide all of the tools, including clear protections from liability, necessary to incentivize voluntary participation to meet best practices and to protect companies that share cyber threat information with the government. Only legislation can put in place the privacy protections that Americans expect from their government. Only legislation can ensure that the cybersecurity policy endures from one Administration to the next and provide the long-term solutions needed to address the cyber threat.[23]

On November 14, 2012, the Cyber Security Act of 2012 was defeated in the Senate by a 51-47 vote—with five Democrats voting against the bill and four Republicans voting for it.[24] Some predicted that President Obama would attempt to resurrect the dead Cyber Security Act with an Executive Order

that contained many of the same pieces.[25] They were right. In February 2013, as augured in his State of the Union address, President Obama issued Executive Order 13636 on improving critical infrastructure cybersecurity. The same day, he issued Presidential Policy Directive ("PPD") 21, which established new overall goals for protecting critical infrastructure from both physical threats and cyberthreats.[26]

This episode was typical of the President's approach to a Congress he reportedly views as obstructionist. President Obama has frequently wielded his executive power to circumvent Congress's wishes—for example, on immigration, gun control, climate change, and appointments. These actions approach—and possibly exceed—the limits of presidential power under the Constitution.

In general, the Constitution vests the President with the power to execute and Congress with the power to legislate.[27] Presidents use executive orders to manage the operations of the federal government under legislated authority or authority expressly granted in Article II of the Constitution. It is worth noting that the Founders dedicated the First Article to Congress, as more closely representative of the voting public. In one exposition of the President's power to issue executive orders, the Office of Legal Counsel ("OLC") explained:

> The President's authority to issue the proposed executive order derives from his constitutional power to 'take Care that the Laws be faithfully executed.' It is well established that this provision authorizes the President, as head of the Executive Branch, to 'supervise and guide' executive officers in 'their construction of the statutes under which they act in order to secure that unitary and uniform execution of the laws which Article II of the Constitution evidently contemplated in vesting general executive power in the President alone.'[28]

But executive orders cannot impose novel obligations or restrictions on the public unless Congress has authorized the President to do so—whether expressly or implicitly.[29] Further, questions arise where—as here—a President issues an executive order to do that which Congress has expressly rejected.

Both Republicans and Democrats have harshly criticized presidents for usurping legislative authority with executive orders.[30] But such constitutional arguments rarely seem sincere; views on the scope of executive power often turn on an author's agreement with the policy being promoted.[31] In any case, the EO effectively created a set of obligations on private industry in a manner that bypassed the deliberation and accountability of Congress.

## III. The EO Is Well-Intentioned, But Flawed

With EO 13636 and PPD-21, President Obama forced into law the pieces of the Cyber Security Act that the Senate had rejected. The EO and PPD direct the Department of Homeland Security ("DHS") and the National Institute for Standards and Technology ("NIST") to, among other things: (1) create policies and procedures to increase information sharing about cyberthreats; (2) develop a "Cybersecurity Framework" to reduce risk to critical infrastructure; and (3) create an incentives-driven cybersecurity program for critical infrastructure to share threat information with the U.S. Government. As of the writing of this article, implementation of the EO is well underway. On February 26, 2013, NIST published a request for information, initiating its development of the Cybersecurity Framework.[32] In July 2013, NIST released a draft outline of its Cybersecurity Framework.[33] NIST is continuing to hold events and workshops as it develops and gathers additional input on the framework.

The exact scope of the EO is unclear, but ultimately it will be extremely broad. The EO and PPD contemplate regulation of "critical infrastructure." Both adopt the definition of "critical infrastructure" employed by section 1016(e) of the USA PATRIOT Act of 2001; namely, "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." [34]

Industry sectors that fall under this broad tent will likely be subject to myriad regulations, all of which may fail to adequately address cybersecurity concerns. The EO's primary shortcoming is this: it does not incent information sharing, but rather adopts a regulatory approach that is unlikely to enhance cybersecurity.

*First, the EO fails to provide for information sharing.* The EO does not facilitate information sharing among industry stakeholders and with the federal government. Section 4 of the EO declares that "[i]t is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats."[35] Among other things, the EO (1) calls for the federal government to quickly move unclassified information to the private sector[36]; (2) increases the number of security clearances given to owners of covered infrastructure[37]; and (3) expands existing information-sharing systems.[38]

At bottom, this directive simply commands agencies to be more vigorous in their information sharing. It does not create any new authority for information sharing, nor does it protect private companies that choose to use and share cybersecurity information from legal action—companies that may be reluctant to share information because of FOIA, regulatory enforcement, and lack of liability protections. (Nor could it, since such an exemption could only be accomplished through legislative action.) Without these protections, private industry will be cautious in sharing information or using shared information.

And rightly so: a FOIA request could reveal proprietary information; shared information among businesses could raise antitrust concerns; and sharing sensitive information could result in a lawsuit alleging violation of privacy. A business will only voluntarily share information if the benefits of sharing outweigh its risks; without protection, a company may well decide to opt out of the voluntary information-sharing systems created by the EO. The EO's failure to adequately protect companies seeking to share cybersecurity information was a theme of comments in the NIST docket regarding the Cybersecurity Framework.[39]

*Second, the EO does not sufficiently allow for industry*

*participation.* Though NIST has solicited input from private industry in crafting a Cybersecurity Framework, its rulemaking procedures lack the procedural protections of typical notice-and-comment rulemaking. Notice-and-comment rulemaking proceedings require agencies to issue a notice of proposed rulemaking that references the legal authority and substance of the rule,[40] to disclose the scientific basis for the rule in order to allow adequate opportunity to comment,[41] to provide an opportunity for comment, and to issue a statement of basis and purpose.[42] The point of these procedures is to publicize an agency's development of its position, allow interested parties to comment on a proposed rule and, if necessary, allow the agency to revise the proposed rules.[43]

The EO directs NIST to publish a preliminary version of comments within 240 days, and a final version within a year. That provides NIST only four months to allow comment on its preliminary framework, to adjust for new technological changes as required by Section 7(f) of the EO, and to modify the final Cybersecurity Framework consistent with these comments. Given the broad scope of the EO and the technical, changing complexity of the issue, this timeline is challenging for substantive and broad public participation. Further, as explained more fully below, the threat of liability and antitrust concerns may chill stakeholder participation in this rulemaking process.

*A mandatory regulatory approach is not well-suited to this task.* Section 8 directs DHS and sector-specific agencies to establish a program under which owners and operators of critical infrastructure will voluntarily adopt the directives of the Cybersecurity Framework.[44] Though the EO purports to create a voluntary, incentive-driven framework, Section 10 strongly suggests that the Cybersecurity Framework will ultimately drift from voluntary to mandatory. That section directs agencies responsible for regulating critical infrastructure to "determine if current cybersecurity regulatory requirements are sufficient given current and projected risks."[45] If an agency determines that "current regulatory requirements are deemed to be insufficient,"[46] then that agency has 90 days to propose additional actions to mitigate cyber risk.

Such a regulatory approach is ill-suited to this task. The primary problem is speed: the pace of innovation is fast; the pace of regulatory rulemaking slow. According to a phenomenon commonly called Moore's law, personal-computer performance doubles every 18 to 24 months.[47] By contrast, the average time it takes to write and implement major regulations is at least 24 to 36 months.[48] As one commenter in the NIST proceedings noted, "[t]he current cyber-threat environment evolves in real time and requires a continuous, complex, and layered approach to security that varies greatly across industry sectors. Many of the cyber issues faced by our clients differ greatly, change daily, and cannot be solved by an externally-imposed set of common responses."[49] Regulations will always trail technology; as a result, the efforts of regulators to stop hackers will resemble Wile E. Coyote's efforts to catch the Road Runner—a step behind, no matter how sophisticated or expensive the Acme contrivance.

The regulatory approach has other shortcomings. Apart from being slow, it is inflexible, costly, and diverts resources from innovative problem-solving towards compliance, regardless of the efficacy of regulation by those in private industry who own critical infrastructure. As a recent Government Accountability Office ("GAO") report noted, regulations can often be overly rigid or precise, mandating the use of particular technical standards or even a specific product or technology.[50] Compliance with regulations is also costly; the regulatory burdens imposed by reporting requirements could divert resources that businesses would otherwise use to protect infrastructure.[51] Finally, a regulatory environment may "create[] a culture within the utility industry of focusing on compliance with cybersecurity requirements, instead of a culture focused on achieving comprehensive and effective cybersecurity."[52]

## IV. A Better Approach: Non-Regulatory Solutions to the Cybersecurity Problem

Since the EO's issuance, Congress has continued to propose bills aimed to protect cybersecurity. In July 2013, Senators Rockefeller and Thune introduced the Cybersecurity Act of 2013,[53] which, among other things, proposed to codify the EO's mandate to NIST, direct the Office of Science and Technology Policy to build on existing programs and plans to develop a national cybersecurity research and development plan, task various authorities with supporting competitions to develop and recruit cybersecurity employees, and direct NIST to continue coordination of national cybersecurity awareness and preparedness. Crucially, the bill omits any discussion of information sharing and explicitly states that it does not "confer any regulatory authority on any Federal, State, tribal, or local department or agency." [54]

It would be wiser to adopt a flexible and non-regulatory approach focused on cooperation with the private sector. With Congress's help, the private sector—nimbler and more innovative—can protect its infrastructure more effectively than federal regulators can.[55] As the Defense Science Board Report shows, a performance mandate for effective protection may be needed. Commenters have raised a number of non-regulatory solutions to improving the nation's cybersecurity, including (1) revising liability rules to ensure that the full cost of data breaches is borne by the companies responsible, an innovation that could also lead to the development of a "cyber insurance" system to guard against liability; (2) improving supply chain security by establishing an accreditation system for technology companies; and (3) better educating the "cyber workforce." [56] This Article examines two such non-regulatory approaches: (1) permitting "hacking back" and (2) facilitating information sharing among private corporations and the federal government.

### *A. Hacking Back: An Interesting Idea in Need of Refinement*

To foil robbers, many banks have turned to "dye packs," exploding devices that stain both the money and thief with red ink, and then emit tear gas and release a foul odor.[57] Designed to be indistinguishable from a stack of bills, these dye packs act as a kind of Trojan horse. After a robbery, the robber hurries away from the scene of the crime with the dye pack buried among the rest of his stolen cash. Moments later, the dye pack detonates—destroying the money and covering the robber in ink. Not only does the dye pack lessen a prospective robber's

incentive to steal by decreasing the value of his expected gain, but it also makes robbers easier to catch by literally painting them red.

The Georgian government recently employed a similar tactic to catch a cyber spy. In March 2011, the Georgian government began to investigate a hacker who was stealing sensitive information from government officials by planting malicious software on Georgian news websites.[58] Later, the hacker began attacking the computers of Georgian government officials directly, by sending emails purporting to be from the president of Georgia. Each email contained a PDF attachment that delivered malware to the recipient's computer. Throughout 2011, the government continued to fight the hacker, whose attacks became increasingly sophisticated, with limited success.

Then Georgian officials came up with a better idea. They allowed the hacker to infect one of their computers. On the computer, they planted a file that they knew would be irresistible to the hacker: a ZIP archive entitled "Georgian-NATO Agreement." The file was the cyber equivalent of a dye pack: once downloaded, it installed spyware on the *hacker*'s computer, mining it for documents that officials could use to identify the hacker. The file also activated the hacker's webcam and took two photos of the very surprised looking hacker—which the Georgian government then published online.[59]

Some urge Congress to allow U.S. companies to take similar measures. There is growing support for allowing the private sector to retaliate against hackers by "hacking back"—in other words, taking retaliatory measures to investigate or attack parties believed to be involved in a cyberattack.[60] While hacking back may be structured in a way not to damage the hacker's property, without legislation it could be found in a court to be trespass. But the approach nevertheless has a number of advantages: to begin with, it would harness private companies' unique abilities and incentives to fight those who attempt to steal or destroy their data. Further, it would allow companies to aid intelligence and law enforcement officials in their efforts to catch hackers.[61]

To minimize legal challenges, legislators should allow self-help that does not permanently damage hackers' or innocent third-parties' property. One can imagine a number of scenarios where an overzealous company punishes a relatively innocent server from which it detected a hacker—for example, a school in which a student has misused a school computer. Nevertheless, milder forms of self-help—temporary measures similar to the dye pack—could be beneficial.

Further, companies require more clarity on what defensive measures the law currently permits. The Computer Fraud and Abuse Act ("CFAA"), which prohibits accessing a computer "without authorization," seems to bar hacking back. [62] The CFAA operates similar to an anti-trespassing law, allowing computer owners the right to control what happens on their machines. There is some disagreement on whether the CFAA permits hacking back.[63] Is burying code on one's own computer in an enticing file that a hacker inadvertently carries with him after an intrusion "accessing" the hacker's computer? The Department of Justice takes the view that the CFAA prohibits hacking back. According to the Department of Justice's manual *Prosecuting Computer Crimes*,

> Although it may be tempting to do so (especially if the attack is ongoing), the company should not take any offensive measures on its own, such as "hacking back" into the attacker's computer—even if such measures could in theory be characterized as "defensive." Doing so may be illegal, regardless of the motive. Further, as most attacks are launched from compromised systems of unwitting third parties, "hacking back" can damage the system of another innocent party.[64]

So what defensive measures are permitted? Even the above-quoted passage says only that hacking back "*may*" be illegal, and the CFAA does not explicitly define what constitutes "authorization." It seems clear that the CFAA prohibits a hacked party from breaking into a computer to retrieve hacked data. It is less clear whether the CFAA prohibits planting malware in your own computer as a trap for an unwary hacker, as the Georgian government did. Better-defined rules about permissible defensive measures will help responsible companies defend themselves against hackers and could foster their cooperation with law enforcement.

As policymakers struggle with the balance between security and privacy in the wake of the PRISM disclosure by Edward Snowden and oversight of the Foreign Intelligence Surveillance Act ("FISA") court, so too should they balance rights of companies to defend their data and the property rights of innocent third parties..

*B. Information Sharing: A Long-Overdue Solution*

One badly needed measure to improve cybersecurity is a law fostering information sharing among private companies and the government. According to a recent GAO report, "[d]ifficulties in sharing information and the lack of a centralized information-sharing system continue to hinder progress [in coordinating the federal response to cyber incidents.]"[65] Information sharing would allow private and government actors to share risk information, cooperate in law enforcement efforts, and create patches for vulnerable software, among other benefits.

Such information sharing will not take place until private companies are given legal protection. Sharing information risks the exposure of proprietary information, antitrust concerns, and the filing of lawsuits based on alleged invasions of privacy or tortious interference. Potential liability makes businesses cautious about sharing information between themselves or with the government, and therefore makes the process of information sharing both slow and expensive. With millions of intrusion attempts daily, sharing delayed is security denied. One commenter illustrates what could happen to the sorry company that decides to share information with the government:

> Government prosecutors, law enforcement agencies, or civil attorneys use this information as the basis for establishing a violation of civil or criminal law against Company A [or a] customer, partner, or unaffiliated entity harmed by the incident sues Company A for not informing them of the incident as soon as they were aware of it. Company A's disclosure can be seen as a "smoking gun" or "paper trail" of when Company A knew about

a risk event though Company A did not yet have a legal duty to report the incident. Such allegation could lead to costly litigation or settlement regardless of its validity.[66]

A solution to this problem has percolated in the House, which recently passed CISPA.[67] CISPA provides for the sharing of cyberthreat information between private-sector entities and the intelligence community.[68] The proposed bill facilitates information sharing by making both private industry and the government comfortable sharing and using cyberthreat information. For information that the government shares with private entities, cyberthreat information is only shared with certified entities or those with a security clearance, and CISPA restricts how such information can be used.[69]

For information that private entities share with the government, CISPA (1) exempts such information from disclosure under FOIA; (2) prohibits the government from sharing the information with other entities; and (3) prohibits the government from using the information for regulatory purposes.[70] Perhaps most importantly—and most controversially—CISPA protects private companies from liability for using cybersecurity systems to gain cyberthreat information and for making decisions based on the use of cyberthreat information gained under CISPA.[71] The bill facilitates sharing, but does not require it. CISPA is voluntary, and private entities are not subject to liability for "choosing not to engage in the voluntary activities" authorized under CISPA.[72]

**Conclusion**

In his Executive Order, President Obama warns that "[t]he 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."[73] Elsewhere, he has noted that "[o]ur national security depends on sharing the right information with the right people at the right time."[74] He is right on both counts.

President Obama's EO is a well-intentioned attempt to address U.S. vulnerability to cyberattack, but it is also a misguided one. Mandated solutions will inevitably be too slow to effectively respond. Such regulation can divert resources to compliance rather than innovation and cooperation on anticipating threats. The better approach is to cooperate with private industry by—among other things—sharing information to help coordinate efforts to enhance cybersecurity and providing liability protection.

The debate on PRISM has shown that there is more tolerance in the electorate for decreased privacy in exchange for enhanced security than opponents of liability protection in cybersecurity legislation would have us believe. Regardless of the long-term wisdom of that perceived trade-off, if PRISM is allowed to continue, certainly the private sector—which does not have the power to incarcerate or execute other forms of state violence—should be allowed to share information that, while revealing certain users' data, will enhance cybersecurity for all users.

Endnotes

1 U.S. Gov't Accountability Office, GAO-13-462T, Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges 3 (2013) (quoting the remarks of Secretary of Defense Leon E. Panetta) ("GAO-13-462T").

2 Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013) ("EO").

3 Where authority to regulate existed, new obligations on the private sector can only be imposed after notice and comment rulemaking, under the Administrative Procedures Act. *See* Administrative Procedures Act, 5 U.S.C. § 553.

4 H.R. 3523, 112th Cong. (2012); H.R. 624, 113th Cong. (2013) ("CISPA").

5 *See* Eric A. Fischer et al., Cong. Research. Serv., R42984, The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress 2 (2013), *available at* https://www.fas.org/sgp/crs/misc/R42984.pdf ("Fischer Report").

6 *Id.*

7 Remarks by Shawn Henry, Executive Assistant Director, Federal Bureau of Investigation, in Baltimore, MD (Oct. 20, 2011), *available at* http://www.fbi.gov/news/speeches/responding-to-the-cyber-threat.

8 *See* Fischer Report at 3-4.

9 *Id.* at 1.

10 U.S. Gov't Accountability Office, GAO-13-283, High-Risk Series: An Update 184 (2013).

11 Ellen Nakashima, *Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies*, Wash. Post, May 27, 2013, http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html (last accessed Aug. 2, 2013).

12 For more detail about the various bills proposed in the 112th Congress, *see generally* Eric A. Fischer, Cong. Research Serv., R42114, Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions (2013), *available at* http://www.fas.org/sgp/crs/natsec/R42114.pdf.

13 *Id.* at 4-5.

14 CISPA § 3 (2013) (proposed to be codified at 50 U.S.C. § 1104).

15 The White House was among these critics. *See* Office of Mgmt. & Budget, Exec. Office of the President, Statement of Administrative Policy: H.R. 3523—Cyber Intelligence Sharing and Protection Act (Apr. 25, 2012) ("OMB Statement of Policy").

16 *See, e.g.,* Memorandum from the Office of Mgmt. & Budget, Exec. Office of the President, on Law Enforcement Provisions Related to Computer Security to Congress (May 12, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf.

17 *See* OMB Statement of Policy at 1 ("Cybersecurity and privacy are not mutually exclusive. Moreover, information sharing, while an essential component of comprehensive legislation, is not alone enough to protect the Nation's core critical infrastructure from cyber threats. Accordingly, the Administration strongly opposes H.R. 3523, the Cyber Intelligence Sharing and Protection Act, in its current form.").

18 *Id.*

19 In light of the PRISM revelations, the Administration's concerns about users' privacy in the context of information sharing between commercial communications operators ring a little hollow.

20 Barack Obama, *Taking the Cyberattack Threat Seriously*, Wall St. J., July 19, 2012, http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html?KEYWORDS=Obama+cybersecurity (last accessed Aug. 2, 2013).

21 *W's Apprentice*, The Economist, May 18, 2013, http://www.economist.com/news/united-states/21578047-presidents-use-executive-orders-many-them-praiseworthy-aims-will-end (quoting President Obama) (last accessed Aug. 2, 2013).

22 *Id.*

23 Press Release, Senate Committee on Homeland Security and Governmental Affairs, Senators Collins, Snowe, and Lugar to White House: Refrain from Executive Order on Cybersecurity (October 10, 2012), *available at* http://www.hsgac.senate.gov/media/minority-media/senators-collins-snowe-and-lugar-to-white-house-refrain-from-executive-order-on-cybersecurity; *see also* Letter from the Honorable Fred Upton et al. to President Barack Obama (October 11, 2012), *available at* http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/letters/20121011Cybersecurity.pdf ("[W]e urge you to rethink the wisdom of an executive order.").

24 Eric Engleman, *Cybersecurity Bill Killed, Paving Way for Executive Order*, Bloomberg, Nov. 14, 2012, *available at* http://www.bloomberg.com/news/2012-11-15/cybersecurity-bill-killed-paving-way-for-executive-order.html (last accessed Aug. 2, 2013).

25 *See id.*; *see also* Taylor Armerding, *Demise of Cybersecurity Bill Means Executive Order on the Way*, NetworkWorld, Nov. 20, 2012, http://www.networkworld.com/news/2012/112012-demise-of-cybersecurity-bill-means-264432.html (last accessed Aug. 2, 2013).

26 Presidential Policy Directive-21, The White House, Critical Infrastructure Security and Resilience (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

27 *Compare* U.S. Const. art. I, § 1 ("All legislative Powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives."), *with* U.S. Const. art. II, § 1, cl. 1 (""The executive Power shall be vested in a President of the United States of America.").

28 *See* Proposed Executive Order Entitled "Federal Regulation," 5 U.S. Op. Off. Legal Counsel 59 (1981) (citations omitted).

29 5 U.S.C. § 553.

30 *See, e.g.*, Todd F. Gaziano, *The Use and Abuse of Executive Orders and Other Presidential Directives* (2001), 5 Tex. Rev. of L. & Pol. 267, 269 (2001) (calling President Clinton's executive orders "[a] driving force" behind "a renewed interest in the proper use and possible abuse of executive orders and other presidential directives"); Neal K. Kaytal & Laurence H. Tribe, *Waging War, Deciding Guilt: Trying the Military Tribunals*, 111 Yale L.J. 1259, 1277 (2002) (challenging the constitutionality of the President's executive order establishing military tribunals for enemy combatants on the ground that the President had "usurped the legislative powers vested by the Constitution exclusively in Congress and threatened the Constitution's rights-protecting asymmetry").

31 For example, the *New York Times* has treated President Obama gently on this issue, pointing out that "[g]overnment by executive order is not sustainable in the long-term," but excusing President Obama's orders on the grounds that "in this particular case, there may be no alternative." Andrew Rosenthal, *Government by Executive Order*, N.Y. Times, Apr. 23, 2012, http://takingnote.blogs.nytimes.com/2012/04/23/executive-overreach/?_r=0 (last accessed Aug. 2, 2013).

32 Developing a Framework To Improve Critical Infrastructure Cybersecurity, 78 Fed. Reg. 13,024 (Feb. 26, 2013), *available at* https://www.federalregister.gov/articles/2013/02/. The period for comment closed on April 8. NIST has published these comments online. *See* NIST, RFI—Framework for Reducing Cyber Risks to Critical Infrastructure (Apr. 29, 2013), *available at* http://csrc.nist.gov/cyberframework/rfi_comments.html.

33 NIST, *NIST Releases Draft Outline of Cybersecurity Framework for Critical Infrastructure*, http://www.nist.gov/itl/csd/cybersecurity-070213.cfm (last accessed August 2, 2013).

34 42 U.S.C. § 5195c(e); EO § 2.

35 EO § 4.

36 *Id.* § 4(b).

37 *Id.* § 4(d).

38 *Id.* § 4(e).

39 Comments of IBM at 5, No. 130208119-3119-01, (Apr. 12, 2013) *available at* http://csrc.nist.gov/cyberframework/rfi_comments/041213_ibm.pdf ("IBM Comments") ("[M]ore needs to be done by Congress to address legal impediments and liability risks that are hindering the robust sharing of information by private sector organizations. The sooner actionable information about cybersecurity threats is shared, the faster it can be used to help protect the public. Today, however, even the most security-conscientious businesses may hesitate to bring forward that information in a timely way due to liability concerns, even when they, too, are being victimized. Treating such organizations as allies rather than accomplices will help them step forward – in the interests of their clients, employees, the nation, and themselves."); Comments of VISA at 4-5 (Apr. 8, 2013), *available at* http://csrc.nist.gov/cyberframework/rfi_comments/040813_visa.pdf ("We . . . support a legislative solution that affords appropriate legal and privacy protections for information sharing between government and the private sector. These protections will allow government and businesses to exchange specific threat information and defense strategies, secure the nation's cyber assets and mitigate emerging threats in real time, all with appropriate liability, antitrust and freedom of information protections.").

40 *See* 5 U.S.C. § 553(b).

41 *See United States v. N.S. Food Prods. Corp.*, 568 F.2d 240, 251 (2d Cir. 1977).

42 *See* 5 U.S.C. § 553(c).

43 *See* Kevin M. Stack, *The Constitutional Foundations of Chenery*, 116 Yale L.J. 952, 995 (2007).

44 EO § 8.

45 *Id.* § 10(a).

46 *Id.* § 10(b).

47 *A Law Deeper than Moore's? The Energy Efficiency of Computing Is Doubling Every 18 Months*, The Economist, Oct. 10, 2011, http://www.economist.com/blogs/dailychart/2011/10/computing-power (last accessed Aug. 2, 2013).

48 *See* Steven P. Bucci et al., *A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace*, 2785 Backgrounder, Mar. 28, 2013, at 3 ("Bucci").

49 IBM Comments at 1; *see also* Comments of Microsoft at 16, No. 130208119-3119-01 (Apr. 8, 2013), *available at* http://csrc.nist.gov/cyberframework/rfi_comments/040713_microsoft.pdf ("Specific systems and technologies change regularly, as do the threats facing them. Many traditional critical infrastructure approaches such as assets lists, specific mandated controls, and compliance checklists, are not well suited for such a dynamic risk landscape.").

50 U.S. Gov't Accountability Office, GAO-12-926T, Cybersecurity: Challenges in Securing the Electricity Grid (2012) ("GAO-12-926T").

51 Comments of Level 3 at 4, No. 130208119-3119-01 (Apr. 8, 2013), *available at* http://csrc.nist.gov/cyberframework/rfi_comments/040613_level3_communications.pdf ("In practice, far more resources are put into Program Managing these reporting relationships, than we spend in protecting the actual infrastructure; taking valuable capability away from the ability to better protect infrastructure.").

52 GAO-12-926T at 16.

53 S. 1353, 113th Cong. (2013).

54 *Id.* § 3.

55 *See, e.g.*, Marc Maiffret, *Closing the Door on Hackers*, N.Y. Times, Apr. 4, 2013, http://www.nytimes.com/2013/04/05/opinion/closing-the-door-on-hackers.html ("A lot of the talk around cybersecurity has centered on the role of government. But investing in software security and cooperating across the software industry shouldn't take an act of Congress. It will, however, take a new mind-set on the part of developers. They should no longer see security as an add-on feature, nor should they regard holes in their competitors' security efforts as merely a competitive advantage.") (last accessed Aug. 2, 2013).

56 For an excellent discussion of non-regulatory approaches to cybersecurity from which this article draws much useful information, *see* Bucci at 5-12.

57 Jim Di Paola, *Dye Packs Foil Bank Robbers' Clean Getaways*, Sun Sentinel, Nov. 19, 1989, http://articles.sun-sentinel.com/1989-11-19/news/8902100716_1_dye-packs-bank-robbers-robbery (last accessed Aug. 2, 2013).

58 Jeremy Kirk, *Irked by Cyberspying, Georgia Outs Russia-based Hacker—with Photos*, PC World, Oct. 30, 2012, http://www.pcworld.idg.com.au/article/440484/irked_by_cyberspying_georgia_outs_russia-based_hacker_--_photos/ (last accessed Aug. 2, 2013).

59 *Id.*

60 Christopher M. Matthews, *Support Grows to Let Cybertheft Victims 'Hack Back,'* Wall St. J., June 2, 2013, http://online.wsj.com/article/SB10001424127887324682204578517374103394466.html (last accessed Aug. 2, 2013).

61 For a discussion of the policy benefits of "hacking back," *see* Bucci at 10.

62 18 U.S.C. § 1030(a).

63 *Compare* Stewart Baker, *RATs and Poison II—the Legal Case for Counterhacking*, Volokh Conspiracy, Oct. 14, 2012, http://www.volokh.com/2012/10/14/rats-and-poison-ii-the-legal-case-for-counterhacking/ (arguing that it is legal to hack into the computer of someone who has hacked into your computer under the CFAA) (last accessed Aug. 2, 2013), *with* Orin Kerr, *The Legal Case Against Hack-Back: A Response to Stewart Baker,* Volokh Conspiracy, Oct. 15, 2012, http://www.volokh.com/2012/10/15/the-legal-case-against-hack-back-a-response-to-stewart-baker/ (attacking Baker's argument) (last accessed Aug. 2, 2013).

64 H. Marshall Jarrett et al., Comp. Crime and Intellectual Prop. Section, Crim. Div., Dep't of Justice, Prosecuting Computer Crimes at 180, *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

65 GAO-13-462T at 15.

66 Information Technology Industry Council, *ITI Recommendation: Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing*, January 2012, *available at* http://www.itic.org/dotAsset/fae2feab-7b0e-45f4-9e74-64e4c9ece132.pdf.

67 CISPA § 3 (2013) (proposed to be codified at 50 U.S.C. § 1104).

68 *See Id.* § 3(a) (amending 50 U.S.C. § 1104(a)(1)) ("The Director of National Intelligence shall establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private-sector entities and utilities and to encourage the sharing of such intelligence.").

69 *Id.* (amending 50 U.S.C. § 1104(b)).

70 *Id.* (amending 50 U.S.C. § 1104(b)(2)(D)).

71 *Id.* (amending 50 U.S.C. § 1104(b)(3)).

72 *Id.* (amending 50 U.S.C. § 1104(f)(5)).

73 EO at 11,739.

74 President Barack Obama, Introduction to *National Strategy for Information Sharing and Safeguarding*, *available at* http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.