ASA

Risk Consultants

Research Note

The Fight to Define U.S. Cybersecurity and Information Sharing Policy

By: Dan Arnaudo

Keywords: Congress, CISPA, Critical Infrastructure, Cybersecurity Act, Information Sharing, NSA

Abstract – This research note reviews the recent political battles over cybersecurity and information sharing policy in the past two years, particularly regarding critical infrastructure. Events covered include failed attempts by Congress to pass the Cyber Intelligence Sharing and Protection (CISPA) and the Cybersecurity Acts of 2012 and President Obama's signing of an executive order to improve critical infrastructure cybersecurity in February 2013. It identifies and reviews the key objectives of the bills, the debates over them and the interested stakeholders in the process.

> "America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."
> - President Barack Obama, State of the Union Address, February 11, 2013[1]

During his 2013 State of the Union Address, U.S. President Barack Obama highlighted the challenges to American cyberspace with these statements. Increasingly, corporations, the government, military and individual citizens have come to rely on the Internet for everything they do, and this has made them uniquely vulnerable to a wide range of threats that emanate online. Government and businesses are increasingly looking for ways to share information related to these problems so that they can become aware of problems as they occur

and coordinate better, both when dealing with attacks and preventing them before they occur.

In a much-anticipated action aimed at achieving these ends, he noted in the next lines of the speech that he had just signed an executive order earlier in the day that would attempt to encourage some information sharing along these lines.[2] Many in industry, government and the media have predicted this order since Congress failed to pass bills in 2012 that would address cybersecurity and information sharing for online threats and vulnerabilities, particularly towards critical infrastructure. However, an executive order is a limited instrument because it lacks the force of legislation and only encourages executive agencies such as the National Institute of Standards and Technology (NIST) to begin to coordinate their own policies. The history of these debates is helpful in understanding the challenges of passing cybersecurity and information sharing policy today. President Obama's executive order is only the latest in a series of attempts to balance privacy and security concerns to implement a solution to a problem that is growing rapidly in size, complexity and importance.

In April 2012, partly at the urging of the President and a significant number of private and public sector actors[3], the House passed the

"Cyber Intelligence Sharing and Protection Act" (CISPA) which would enable the kind of information sharing that President Obama is requesting today.[4] However, the president vowed to veto the act, citing both privacy concerns that the agreement would share too much of the citizens' private information and that it did not do enough to address serious threats to critical infrastructure. In a statement from the Office of Management and Budget, the administration laid out its case:

> "The sharing of information must be conducted in a manner that preserves Americans' privacy, data confidentiality, and civil liberties and recognizes the civilian nature of cyberspace. 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."[5]

Organizations such as the Electronic Frontier Foundation, the American Civil Liberties Union, The Sunlight Foundation, and Reporters Without Borders opposed the bill on privacy grounds as

well. The EFF in particular criticized the bill for being overly broad in terms of its information sharing and noted that parties to the agreement would not share information publicly. The bill contained a provision that would make any information shared under its framework irrecoverable by the public through Freedom of Information Act Requests. [6]

Alternatively, the American Chamber of Commerce opposed the bill because it would place overly onerous information sharing demands on U.S. businesses; a position that resonated with many conservatives. The result is that there were challenges from both a public concerned with civil liberties and a private sector concerned with a government overly interested in the affairs of a business, and enabled with the power of litigation if an enterprise did not share enough information. Obviously, there is a cost to set up any system, including both implementation and then managing compliance to ensure that firms are following the law, a subtext that many commentaries overlooked.

Because of this opposition and the president's veto threat, the bill didn't proceed to the Senate, but elements of it were picked up in when the Senate attempted to pass the

Cybersecurity Act of 2012, which incorporated provisions of CISPA but failed on a largely party line vote when it was voted on in August and November.[7] That failure led to the beginning of speculation that President Obama would make an executive order to implement many of its provisions, fulfilled on the day of his State of the Union. Two days after the President's executive order, the cosponsors of CISPA last year, Congressmen Mike Rogers (R-MI), chairman of the House Intelligence Committee, and ranking member Dutch Ruppersberger (D-MD), announced that they were reintroducing the measure with some amendments that would limit the scope of the information shared. They also noted in a press conference that they were working with the administration to address its privacy concerns and avoid a veto.[8]

The authors' positions point to one of the chief reasons that many detractors of these bills are concerned about privacy, namely that they represent the intelligence community and that institutions like the National Security Agency will benefit the most from these kinds of information sharing initiatives with little oversight.[9] Intelligence committees in Congress are supposed to

provide this function but it is unclear to many observers how, once Congress has vested this power, its members or the public can really verify what kind of data is being exchanged.

The concerns that members of Congress, the public, their related interest groups and the private sector raised in the course of the debate over CISPA and the Cybersecurity Act will continue to be the locus of the debate over the resurrected bill. Ultimately, government and industry need to address these issues and come to some kind of agreement on how they can coordinate both their information and the policies that govern them to protect critical infrastructure better. It is a good thing that this argument is so vociferous, including through State of the Union Addresses and from heavyweights in the public and private sectors participating and encouraging wider debate. There is a justified urgency to these calls for political and technical reform. Whether or not the various parties can come to agreement on a strong, coherent policy is difficult to predict, but any decision will form a major component of how the U.S. will be able to protect its banking, power and utility systems in future. The security of critical infrastructure is linked inextricably with the privacy and civil rights

of its users, and the balancing act to ensure both of these objectives forms the core of the challenge that any sound policy will have to address. However, failure to pass laws regarding cooperation between private and public sectors will have severe consequences for all concerned.

ASA

Risk Consultants

References

[1] Obama, Barack. "Transcript: State of the Union 2013." 13 Feb. 2013. Web. 14 Feb. 2013. <http://abcnews.go.com/Politics/OTUS/transcript-president-barack-obamas-2013-state-union-address/story?id=18480069>

[2] Obama, Barack. "Executive Order -- Improving Critical Infrastructure Cybersecurity." Web. 15 Feb. 2013. <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

[3] "Facebook Backs Cyber-threat Bill." *BBC* 16 Apr. 2012. Web. 15 Feb. 2013. <http://www.bbc.co.uk/news/technology-17730266>

[4] "Cyber-security Bill Past US House." *BBC* 27 Apr. 2012. Web. 15 Feb. 2013. <http://www.bbc.co.uk/news/world-us-canada-17864539>

[5] Franzen, Carl. "Obama Will Veto CISPA Unless Changes Are Made." *Talking Points Memo*. 25 Apr. 2013. Web. 15 Feb. 2013. <http://livewire.talkingpointsmemo.com/entry/obama-will-veto-cispa-unless-changes-are-made>

[6] Timm, Trevor. "Cybersecurity Bill FAQ: The Disturbing Privacy Dangers in CISPA and How To Stop It." *Electronic Frontier Foundation* 15 Apr. 2012. Web. 15 Feb. 2013. <https://www.eff.org/deeplinks/2012/04/cybersecurity-bill-faq-disturbing-privacy-dangers-cispa-and-how-you-stop-it>

[7] Smith, Josh. "Cybersecurity Bill Fails To Advance in Senate, Again." *National Journal* 14 Nov. 2012. Web. 15 Feb. 2013. <http://www.nationaljournal.com/tech/cybersecurity-bill-fails-to-advance-in-senate-again-20121114>

[8] Franzen, Carl. "Controversial Cyber Bill CISPA Returns to Congress for Debate, Same as Before." *The Verge* 13 Feb. 2013. Web. 15 Feb. 2013. <http://www.theverge.com/2013/2/13/3984442/cispa-back-in-congress>

[9] Schwartz, Matthew. "CISPA Bill: 5 Main Privacy Worries." *Information Week* 17 Apr. 2013. Web. 16 Feb. 2013. <http://www.informationweek.com/news/security/privacy/232900418>