**Robyn Greene**
**Policy Counsel and Government Affairs Lead**
**New America's Open Technology Institute**

**Hearing: The Current State of DHS Private Sector Engagement for Cybersecurity**
**Date: Thursday, March 9, 2017, at 10:00 a.m.**

Thank you for the opportunity to testify today on "The Current State of DHS Private Sector Engagement for Cybersecurity." I represent New America's Open Technology Institute (OTI), where I am a Policy Counsel and Government Affairs Lead on privacy, surveillance, and cybersecurity issues.

New America is a nonpartisan, nonprofit, civic enterprise dedicated to the renewal of American politics, prosperity, and purpose in the digital age through big ideas, technological innovation, next generation politics, and creative engagement with broad audiences. OTI is a program at New America that works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators. Our current focus areas include surveillance, privacy and security, net neutrality, broadband access, and consumer privacy.

In December 2015, Congress passed the Cybersecurity Information Sharing Act (CISA).[1] The law provides private sector entities with liability protection for sharing information about cybersecurity threats with one another and with the government. Throughout the debate over information sharing legislation, OTI voiced significant concerns about the scope of sharing permitted and the insufficient privacy protections for internet users both before and after information is shared. We also urged Congress to take a more holistic approach to cybersecurity policy, rather than focus solely on information sharing.[2]

My testimony will cover three topics: 1) OTI's outstanding privacy concerns related to how much information can be shared, with whom, and how it can be used under CISA; 2) the ways in which the Department of Homeland Security (DHS) has worked in its implementation of the law to protect privacy and simultaneously enhance cybersecurity, and 3) additional steps that the government could take to strengthen public-private partnerships related to cybersecurity, and to

[1] Cybersecurity Information Sharing Act, 6 U.S.C. 1501 et. seq., Public Law No: 114-113, H.R. 2029 Division N, Title I, 114th Cong. (2015), https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf.
[2] Robyn Greene, *Congress Must Focus on More Than Information Sharing*, The Hill, Jan. 30, 2015, http://thehill.com/blogs/congress-blog/technology/231190-congress-must-focus-on-more-than-information-sharing.

incentivize or encourage the private sector to adopt best practices, to meaningfully protect privacy and improve overall security.

Outstanding Concerns Regarding the Cybersecurity Information Sharing Act (CISA)

Information sharing legislation was extremely controversial for the entire time that Congress debated it, even up to the point that CISA became law. The most significant point of contention was always how to adequately protect privacy and civil liberties. CISA's predecessor, the Cyber Intelligence Sharing Protection Act (CISPA), contained no meaningful privacy protections when it was first introduced.[3] After years of advocacy by privacy and security experts, and several iterations of legislation, the final version of CISA included important improvements and protections. Nevertheless, certain privacy concerns were left unaddressed or inadequately addressed. Those shortfalls include imprecise definitions, a too-weak requirement to remove personal information before sharing cyber threat indicators, overbroad allowances for law enforcement to use shared data for purposes unrelated to cybersecurity, and the possibility that the President will undermine DHS's role as the lead information sharing portal by establishing a second authorized portal.[4]

CISA's overbroad definitions threaten privacy because they can result in over-sharing of personal or otherwise unnecessary information. This is the case for the definition of "cybersecurity threat," which triggers the authorization to share. The law defines a cybersecurity threat as anything that "may result in an unauthorized effort to adversely impact" a device or system.[5] It covers any potential threat and does not require that a company make a determination that the purported cyber threat is likely to cause harm before sharing their users' information.

This low threshold could spur sharing of unnecessary information, like that concerning false alarms, which would threaten privacy if the sharer transmits personal information as part of the cyber threat indicators shared. It could also undermine security. Unnecessary sharing of personal information can expose internet users to new threats should their information be successfully targeted and exfiltrated by malicious actors after being shared under CISA. Additionally, it can undermine security by creating "white noise" that distracts from imminent threats.[6]

---

[3] Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2011), https://www.congress.gov/112/bills/hr3523/BILLS-112hr3523ih.pdf; *see also* Letter from the ACLU to Hon. Mike Rogers & Hon. C.A. "Dutch" Ruppersberger, Dec. 1, 2011, https://www.aclu.org/other/aclu-opposition-hr-3523-cyber-intelligence-sharing-and-protection-act-2011.

[4] Robyn Greene, *The Knock-Down, Drag-Out Fight Over Cybersecurity Legislation*, Slate, Jan. 15, 2016, http://www.slate.com/articles/technology/future_tense/2016/01/how_the_privacy_community_made_cybersecurity_legislation_better.html.

[5] Supra note 1 *at* §1501(5).

[6] *See* Letter from security experts to Sen. Dianne Feinstein, et al concerning information sharing bills (Apr. 16, 2015), https://cyberlaw.stanford.edu/files/blogs/technologists_info_sharing_bills_letter_w_exhibit.pdf.

Over-sharing could also result from the insufficiently narrow definition for "cyber threat indicator" and the inadequate requirement to remove personal information before sharing. Cyber threat indicators include "information that is necessary to describe or identify…the actual or potential harm caused by an incident…[or any] attribute of a cybersecurity threat" so long as disclosure of the underlying attribute is not otherwise legally prohibited.[7]

A broad interpretation of this definition could include personal information or content of online communications that is not needed to detect or protect against a threat. This is because information that could be deemed necessary to describe a threat or potential harms caused by an incident could still be unnecessary to identify or protect against the threat. For example, while it might be reasonable to share an IP address that is associated with malicious activity, the breadth of this definition might also permit a company to share any information they might have associated with that IP address that identifies a particular account holder or location because they claim it is necessary to *describe* the IP address. In the case of botnets, this identifying information might not necessarily belong to the malicious actor; it could belong to a botnet victim.

Similarly, under the law, companies can share any personal information so long as it is "directly related to a cybersecurity threat."[8] This could be interpreted in a manner that undermines privacy by allowing a company to share victim information or other personal information unnecessary to identify or protect against a threat. For example, a broad interpretation of this requirement could allow for a company to share the personal information of the victim of a cyber incident, like information about the recipient of a phishing email, since that information could be deemed to be "directly related" to the threat, even though it may not be necessary to identify or protect against the threat.[9]

In addition to insufficiently narrow definitions and weak front-end privacy protections, CISA overbroadly authorizes law enforcement to use the shared information for non-cybersecurity investigations. Under the statute, any information that is shared with the government for a cybersecurity purpose may be used by law enforcement in investigations and prosecutions

---

[7] Supra note 1 *at* §1501(6).
[8] Supra note 1 *at* §1503(d)(2).
[9] As I discuss in the next section of this statement, DHS has done a good job of protecting privacy in its promulgation of guidance to companies on information sharing. It addresses this specific concern, making clear that companies should not share this kind of victim information. However, that guidance, and thus DHS's strict interpretation of the requirement to remove personal information, is subject to change. To better protect privacy, Congress should amend the law to address this concern. *See Dep't of Homeland Security & Dep't of Justice, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measure with Federal Entities under the Cybersecurity Information Sharing Act of 2015 5 (2016),* https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_(Sec%20105(a)).pdf *[hereinafter "Company Guidance"].*

entirely unrelated to cybersecurity or computer crimes. Authorized uses include investigations and prosecutions into Trade Secrets Act and Espionage Act violations, undefined "serious economic harms," and certain violent crimes irrespective of whether the threat is imminent.[10] This undermines Fourth Amendment protections because it allows law enforcement to use information in investigations and prosecutions that it would ordinarily only be able to obtain pursuant to a warrant issued by a judge based on a finding of probable cause. Information sharing is subject to no judicial oversight, and thus no judge ever makes a finding of probable cause before law enforcement uses the information it receives under CISA, even where investigations are unrelated to cybersecurity.

Finally, CISA includes a provision that could call into question DHS's important and proper role as the lead civilian portal for private sector information sharing with the government. Under CISA, if a company wants to receive liability protection for sharing cyber threat indicators with the federal government, it must share that information through an authorized portal.[11] Currently, DHS is the only authorized information sharing portal. However, CISA authorizes the president to establish a secondary portal at any federal entity except for the Department of Defense and the National Security Agency.[12]

If the president were to exercise this authority at a law enforcement or intelligence oversight agency like the Federal Bureau of Investigation or the Office of the Director of National Intelligence, it would significantly threaten privacy and undermine Americans' trust in the federal government's information sharing program. Additionally, it would introduce operational weakness by further decentralizing information sharing and undermining DHS's role and authority as the federal government lead on domestic cybersecurity and private sector engagement, which Congress just formally established in 2014.[13]

OTI believes that these outstanding flaws in CISA pose a clear threat to both privacy and effective cybersecurity practice, and hopes that Congress will consider amending it to address those concerns. However, despite those flaws, on the whole, DHS has done a good job of promulgating guidelines and procedures under CISA that protect privacy and strengthen cybersecurity. Congress should support DHS in this important work.

<u>DHS Implementation of CISA Has Been Effective and Privacy Protective, But More Should Be Done to Improve Information Sharing</u>

[10] Supra note 1 *at* §1504(d)(5)(A).
[11] Supra note 1*, at §1505(b).*
[12] *Id. at §1504(c)(2)(B).*
[13] Robyn Greene, *Dangerous for Cybersecurity and Privacy: Cotton Amendment No. 2581*, New America's Open Technology Institute (Aug. 25, 2015), https://www.newamerica.org/oti/blog/dangerous-for-cybersecurity-and-privacy-cotton-amendment-no-2581/ [analyzing a proposed amendment to CISA that would have authorized the FBI as an additional covered information sharing portal]; *and* National Cybersecurity Protection Act of 2014, 6 USC 148note, et seq., Public Law No: 113-282.

DHS has taken a reasonable and measured approach to implementing CISA that balances privacy and security. This is clear from how DHS set up its Automated Indicator Sharing system (AIS), and how its promulgation of procedures and guidelines clarified ill-defined terms and standards in the statute.

When DHS rolled out AIS, it leveraged Structured Threat Information eXchange (STIX) to establish standardized fields of information that can be shared and Trusted Automated eXchange of Indicator Information (TAXII) as the secure, automated method for sharing information.[14] This was an important step, because by setting out specific, standardized fields of information that can be shared, STIX limits the potential for sharing unnecessary personal information.

It is still possible for unnecessary personal information to be shared under CISA, because there are STIX fields that could include it or that allow a submitter to copy and paste communications content, and because a submitter could choose to send an email in lieu of submitting information via AIS. DHS mitigates this privacy risk by ensuring that any personal information included in one of those three types of submissions is subject to human review to determine if it is necessary to describe or identify the threat. The personal information is then either removed if it does not meet the standard or further disseminated if it does. DHS also discourages the use of e-mail to submit cyber threat indicators.[15]

Additionally, DHS guidance on how to determine if personal information must be removed is effective at protecting privacy, considering the requirements of the statute. DHS establishes a clear application of the test for removal of such information in its guidance to federal entities. It lays out the critical three-part test: 1) Do you know it is "personal information of a specific individual or information that identifies a specific individual"? 2) If yes, is it directly related to the threat? 3) If yes, then the entity may share it, and if no, then it must be removed prior to dissemination.[16]

Importantly, DHS also narrowly interprets the standard for removal of personal information in company guidance and in privacy guidelines for federal entities. It does so by offering a clear explanation of what is "directly related" to a cybersecurity threat. DHS provides that "Information is not directly related to a cybersecurity threat if it is not necessary to detect,

---

[14] *Company Guidance,* supra note 9 *at* 22.

[15] Dep't of Homeland Security & Dep't of Justice, *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government* 8, 10 (2016), https://www.us-cert.gov/sites/default/files/ais_files/Operational_Procedures_(105(a)).pdf [hereinafter "Final Proocedures"].

[16] Dep't of Homeland Security & Dep't of Justice, *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* 12 (2016), https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_(Sec%20105(b)).pdf [herinafter "Privacy Guidelines"].

prevent, or mitigate the cybersecurity threat."[17] It also offers examples to illustrate what kinds of personal information can and cannot be shared. Both documents highlight that personal information related to victims of cyber attacks, such as information that identifies the recipient of a phishing email, is not directly related to a cybersecurity threat, and must be removed before sharing or dissemination.[18]

The standard for removal of personal information before sharing or dissemination of cyber threat indicators was one of the most contentious aspect of the debate. Opponents of a strict removal requirement were concerned that a higher standard would slow down sharing and raise questions about when liability protections under the law are triggered. These concerns have been largely put to rest. In the vast majority of cases, speed of information sharing is not a determining factor in preventing an attack. The most recent Verizon data breach report concluded that 93% of successful attacks took minutes to breach a device or network, but organizations took weeks to discover them, leaving ample time for the attacker to have identified and stolen the sought after data in most cases.[19]

DHS's application of this standard for removal is also aligned with Congress' goal in passing CISA: to enhance security while simultaneously protecting privacy. Personal information is constantly targeted by hackers, as we have seen in countless data breaches, whether they be at government agencies like the Office of Personnel Management (OPM), healthcare providers like Anthem, retailers like Target and Home Depot, financial institutions like J.P. Morgan, or technology companies like Yahoo.[20] The more personal information is shared with more entities, the larger the target for malicious hackers and nation states seeking to breach our defenses.[21]

---

[17] *Company Guidance* supra note 9, *at* 5.
[18] Id. *See also Privacy Guidelines* supra note 16, *at* 12.
[19] Verizon, *2016 Data Breach Investigations Report: Executive Summary* 2 (2016), http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf. Full report available at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.
[20] *See* Brian Naylor, *One Year After OPM Data Breach, What Has The Government Learned?*, NPR, Jun. 6, 2016, http://www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned; Steve Ragan, *Anthem: How Does a Breach Like This Happen?* CSO, Feb. 9, 2015, http://www.csoonline.com/article/2881532/business-continuity/anthem-how-does-a-breach-like-this-happen.html; Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZD Net, Feb. 2, 2015, http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/; Julie Creswell & Nicole Perlroth, *Ex-Employees Say Home Depot Left Data Vulnerable*, NY Times, Sept. 19, 2014, https://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html?partner=rss&emc=rss&_r=2; Matthew Goldstein, Nicole Perlroth & Michael Corkery, *Neglected Server Provided Entry for JPMorgan Hackers*, NY Times, Dec. 22, 2014, https://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/?_r=1; *and* Asha McLean, *Yahoo Says 32m User Accounts Were Accessed via Cookie Forging Attack*, ZD Net, Mar. 2, 2017, http://www.zdnet.com/article/yahoo-says-32m-user-accounts-accessed-via-cookie-forging-attack/.
[21] Robyn Greene, *Is CISA Gift-wrapped for Hackers and Nation-state Actors?* The Hill, Aug. 3, 2015, http://thehill.com/blogs/pundits-blog/technology/250070-is-cisa-gift-wrapped-for-hackers-and-nation-state-actors.

Thus, by reducing the amount of personal information shared under CISA, DHS is serving a critical security function, as well as protecting privacy.

Privacy is not only essential to data security but also to trust. To the extent that information sharing is an important element of a holistic cybersecurity strategy, having adequate standards in the law and its application are essential to expanding its reach and impact. Companies will be uncomfortable sharing information if they worry their users will see it as harmful to their privacy. Indeed, two months before CISA's final passage, many leading technology companies and trade associations specifically cited its insufficient privacy protections as their grounds for opposition to the bill.[22]

Though DHS has done a good job implementing CISA in a manner that protects privacy and enhances security, Congress should address the outstanding concerns outlined above by codifying these sensible implementations in the law itself. This would provide the public and the private sector with the assurance that the protections as applied by the various guidelines and procedures will not be altered or reinterpreted in a manner harmful to privacy by this or any future administration.

Finally, more must still be done to increase information sharing by the government with the private sector. Throughout the debate on information sharing security experts were clear that CISA would likely have only a modest impact on security, if it had any impact at all, because it focuses on increasing information sharing from the private sector to the government or to other private sector entities. These experts argued that in order to enhance cybersecurity by increasing information sharing, the government needs to improve its system for sharing actionable information with the private sector. Specifically, experts called on the government to declassify more information and share it with a broader set of stakeholders, to speed up its declassification process, and to expand the pool of stakeholders that are cleared to receive classified indicators.[23] Congress should look to how it can help DHS address these concerns.

While improving information sharing can be an important element to cybersecurity, it is just one of many steps that must be taken overall. Ultimately, the only effective approach to cybersecurity will be a holistic approach.

Additional Steps to Strengthen Private Sector-Public Sector Partnerships to Improve Cybersecurity and Protect Privacy

[22] Robyn Greene, *Tech Industry Leaders Oppose CISA as Dangerous to Privacy and Security*, The Hill, Oct. 21, 2015, http://thehill.com/blogs/pundits-blog/technology/257601-tech-industry-leaders-oppose-cisa-as-dangerous-to-privacy-and.

[23] Sara Sorcher, *Security Pros: Cyberthreat Info-sharing Won't Be as Effective as Congress Thinks*, Christian Sci. Monitor, Jun. 12, 2015, http://www.csmonitor.com/World/Passcode/2015/0612/Security-pros-Cyberthreat-info-sharing-won-t-be-as-effective-as-Congress-thinks.

OTI has long argued that while information sharing can have value, it is only a part of the more holistic approach to cybersecurity that Congress, the federal government, and the private sector must take. That approach necessitates more resources for the federal government, as well as more public education about cybersecurity threats and how to defend against them. The federal government also needs to take a "whole-of-government" approach to cybersecurity issues. This is especially needed in two areas: the establishment of policies on vulnerabilities management, and identifying ways to encourage users and private companies to adopt security best practices, like increasing the use of multi-factor authentication and encryption.

Ensuring that all agencies have sufficient resources to buy newer, more secure hardware and software systems, and to recruit and retain a robust staff of skilled security and technology policy experts, has been a longstanding problem. This was one of the problems that led to the OPM breach that resulted in the exfiltration of over 20 million records. Ann Barron-DiCamillo, DHS lead on the team that investigated the breach, stressed that "[OPM] had older systems, that needed to be modernized...They had neglected networks from the perspective of putting in the cybersecurity sensors and technologies that they need to find adversaries in the network."[24]

Less than a year after the OPM breach became public, the previous administration announced the establishment of the President's Commission on Enhancing National Cybersecurity.[25] The commission concluded its work with the issuance of the Cybersecurity National Action Plan (CNAP). Many of the Commission's recommendations focused on adequately resourcing the federal government. They recommended increasing the cybersecurity budget to $19 billion in fiscal year 2017, including investing $3.1 billion in information technology modernization to ensure that federal devices and networks would be compatible with modern security tools; and allocating an additional $62 million to training and hiring new cybersecurity personnel.[26]

These recommendations to significantly increase federal spending related to cybersecurity are well taken, considering the scale of attacks on federal government networks in recent years and the difficulty the federal government has hiring and retaining cybersecurity experts.[27] As Congress drafts the budget for fiscal year 2017, it should allocate whatever resources will be

---

[24] *One Year After the Government Data Breach,* supra note 20.

[25] Michael Daniel, Ed Felten, & Tony Scott, *Announcing the President's Commission on Enhancing National Cybersecurity*, The White House, Apr. 13, 2016, https://obamawhitehouse.archives.gov/blog/2016/04/13/announcing-presidents-commission-enhancing-national-cybersecurity.

[26] Press Release, Office of the Press Secretary, White House, Fact Sheet: Cybersecurity National Action Plan (Feb. 9, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[27] Dustin Volz & Warren Strobel, *NSA Risks Talent Exodus Amid Morale Slump*, Trump fears, Reuters, Feb. 28, 2017, http://www.reuters.com/article/us-usa-cyber-nsa-idUSKBN1672ML.

necessary to hire a skilled workforce, and to modernize federal government networks and harden them against attacks.

In addition to proper resourcing, the federal government, including DHS, should continue its efforts to educate industry and the public about how to better protect themselves online. Increased education on how to identify social engineering attacks is particularly needed. Internet users' susceptibility to these kinds of threats has proven to be a somewhat intractable problem over the years. The most recent Verizon data breach report found that 30% of recipients of phishing emails opened them (a 23% increase from the prior year), and 12% of those people downloaded the malicious attachment or clicked on the malicious link.[28] Nonetheless, raising awareness of these threats via campaigns like "Stop. Think. Connect." may be the first step to reducing the threats' effectiveness.[29]

While resourcing and education are important, DHS must also be part of a whole-of-government approach to cybersecurity and engagement with the private sector. Two areas that could most positively impact our nation's cybersecurity are vulnerability management and widespread adoption of security best practices.

One key aspect of vulnerability management is incentivizing the private sector and individuals to protect themselves against known vulnerabilities by regularly updating their software so that known vulnerabilities are patched. Yet for eight years, Congress focused almost entirely on how to increase information sharing about those vulnerabilities, without doing anything to help ensure that they are patched. Indeed, CISA explicitly states that a company is not required to act on the threat information it receives.[30]

Unsurprisingly, the private sector often only takes action to update their systems after a massive breach, but maintaining updated software would protect against the vast majority of threats. Approximately 85% of successful exploits used the same 10 vulnerabilities, all of which have patches available.[31] In order for CISA to have its intended impact, the government and the private sector must turn information sharing into action by encouraging more and more regular patching of known vulnerabilities.

Another critical aspect to vulnerabilities management concerns how the federal government and Congress approach laws and policies impacting vulnerability research and disclosure, and government participation in the market for previously undiscovered vulnerabilities, called "zero-days." Last year, OTI published a research paper called "Bugs in the System" that serves as a

---

[28] Supra note 19, *at 3.*
[29] *Stop. Think. Connect.*, Dep't of Homeland Security, https://www.dhs.gov/stopthinkconnect (*last visited* Mar. 5, 2017).
[30] Supra note 1 *at* §1505(c)(1)(B)
[31] Supra note 19 *at* 10.

primer on the vulnerabilities ecosystem. We concluded that the leading factors hindering effective vulnerabilities management were a lack of clarity about how best to disclose newly discovered vulnerabilities in order to see them patched; the chilling effect that out-of-date technology laws have on security researchers; and the existence of and U.S. government participation in the zero-day market.[32]

We made five recommendations as to how Congress and the federal government could most effectively address these issues:

1. The U.S. government should minimize its participation in the zero-day market: The zero-day market incentivizes selling vulnerability information to the highest bidder rather than disclosing it to the vendor so it can be fixed, and it caters to the intelligence and law enforcement arms of democratic governments and repressive regimes alike, as well as spies and criminals. The U.S. government can significantly shrink this market simply by abstaining from it and instead relying on and growing resources and technical expertise at agencies like the NSA;[33]

2. The U.S. government should establish strong, clear procedures for government disclosure of the vulnerabilities it buys or discovers: When the government discovers or purchases vulnerabilities that put American internet users and companies at risk, it should ensure that they are disclosed and patched as soon as possible. While there is a process, called the Vulnerabilities Equities Process (VEP), to decide when the government should disclose vulnerabilities, little is known about how that process works, how often it is used, and how effective it is at ensuring vulnerabilities are disclosed. Congress should investigate this issue, and then codify a process that agencies would be required to follow, and that heavily favors disclosure;[34]

3. Congress should establish clear rules of the road for government hacking in order to protect cybersecurity in addition to civil liberties: Government hacking is as privacy-invasive as wiretapping, and it introduces a set of unique risks to security and to civil liberties, such as government malware spreading to innocent people's computers, or resulting in unintended damage or the creation of new vulnerabilities. Yet, Congress has not established a clear legal framework for government hacking, with rules and constraints that address these unique concerns, as it did to address concerns associated with wiretapping;[35]

---

[32] Andi Wilson, Ross Schulman, Kevin Bankston & Trey Herr, *Bugs in the System,* New America's Open Tech. Institute (July 2016), https://na-production.s3.amazonaws.com/documents/Bugs-in-the-System-Final.pdf.
[33] Id. *at* 21.
[34] Id. *at* 21-22.
[35] Id. *at* 23.

4. Government and industry should support bug bounty programs as an alternative to the zero-day market and investigate other innovative ways to foster the disclosure and prompt patching of vulnerabilities: We can improve security by creating more avenues through which security experts can disclose vulnerabilities and diverse incentives for disclosing them, like through Vulnerability Reward Programs, often referred to as bug bounty programs. These programs also provide an outlet for researchers who do not want to participate in the zero-day market; and[36]

5. Congress should reform computer crime and copyright laws, and agencies should modify their application of such laws, to reduce the legal chill on legitimate security research: Out-of-date laws like the Electronic Communications Privacy Act (ECPA), the Computer Fraud and Abuse Act (CFAA), and the Digital Millennium Copyright Act (DMCA), chill security research. This is because under these laws, security researchers are threatened with criminal and civil penalties for their efforts to identify vulnerabilities and fix them.[37]

Finally, in addition to improving vulnerabilities management, the federal government must work with the private sector to help drive a cultural shift in government and industry that embraces privacy by design, and that fuels widespread adoption of security best practices. OTI recently launched a project called "Do the Right Thing" in which we studied the factors that led to the widespread industry adoption of now common, though not yet ubiquitous, security tools like transit encryption by default and offering two-factor authentication. We found that government was often influential in spurring increased adoption of these tools.[38]

DHS and other relevant federal agencies should champion the use of multi-factor authentication and of encryption to protect stored data and communications in transit.[39] DHS should also work with relevant federal entities and industry leaders to encourage a "privacy by design" approach to

---

[36] Id.
[37] Id. *at* 24.
[38] Kevin Bankston, Ross Schulman & Liz Woolery, *Getting Internet Companies To Do The Right Thing*, https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/ (last visited Mar. 5, 2017). For a summary of all of the most common factors spurring the spread of three privacy and security best practices, *see* Kevin Bankston, Ross Schulman & Liz Woolery, *Key Lessons*, https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/key-lessons/ (last visited Mar. 5, 2017).
[39] The question of how to address law enforcement access to encrypted communications has been the subject of intense controversy for several years. OTI strongly opposes any policy proposal that would amount to a mandate for exceptional access to encrypted communications, commonly referred to as encryption backdoors. For a detailed explanation of OTI's position on exceptional access for law enforcement, *see* Kevin Bankston, Written statement to the House Committee on Oversight & Gov't Reform Subcommittee on Information Technology. *Encryption Technology and Possible U.S. Policy Responses*, Hearing, Apr. 29, 2015, http://oversight.house.gov/wp-content/uploads/2015/04/4-29-2015-IT-Subcommittee-Hearing-on-Encryption-Bankston.pdf. For more materials on OTI's position on encryption, *see Read this Before You Rail Against Encryption*, New America's Open Tech. Institute (Nov. 19, 2015), https://www.newamerica.org/weekly/101/read-this-before-you-rail-against-encryption/.

product development, including employing security mechanisms like automatic software updates and offering multi-factor authentication and encryption services by default. Thinking about security holistically and from the ground up will be especially important as more devices become connected and the Internet of Things morphs into simply "the internet."

In conclusion, while CISA improved in some areas over the course of the congressional debate, the final law left certain privacy concerns unresolved and in need of reform. CISA also addresses only a fraction of what Congress and industry should be thinking about as they work to enhance cybersecurity. The focus must now turn to an outcomes-based approach. Congress must ensure that all federal agencies, including DHS, have the resources necessary to hire robust teams of security and technology policy experts, and maintain modern and up-to-date systems and equipment. It will also be essential to find ways to incentivize the private sector and individuals to take action based on new information, such as patching known and newly discovered vulnerabilities and clarifying the government's approach to vulnerabilities management in general. Finally, the relevant federal agencies should take advantage of their bully pulpit to encourage broader adoption of security best practices like the use of encryption and two-factor authentication.