Cybersecurity Information Sharing Act of 2015 Is Cyber-Surveillance, Not Cybersecurity

By Robyn Greene, Policy Counsel

This month, Congress is expected begin consideration of the Cybersecurity Information Sharing Act of 2015 (CISA, S. 754). CISA continues to raise the same significant concerns as when it originated last year in the Senate Select Committee on Intelligence (SSCI). This bill was originally the Senate's answer to the notorious Cyber Intelligence Sharing and Protection Act (CISPA, H.R. 234), the primary information sharing legislation in the House of Representatives, which had been introduced and re-introduced three times over in the last three sessions of Congress (the Administration issued two veto threats in advance of both House votes so far).

Despite increasing doubts about whether information-sharing legislation could have prevented an Anthem, Sony, or Home Depot-style hack, CISA's proponents insist that passing cybersecurity information sharing legislation is the single most important way to enhance cybersecurity. However, the bill's primary effect will be to increase cyber-*surveillance*.

As this analysis will explain, this year's version of CISA would not just increase the sharing of impersonal technical data that indicates a cyber threat but would also significantly increase National Security Agency (NSA) access – in fact, all of government's access – to Americans' personal information. Further, it would allow any entity of the federal government, including intelligence agencies and law enforcement, to use that information for a broad array of garden-variety investigations and prosecutions, not just for cybercrimes. Moreover, CISA would provide a blanket authorization for companies to monitor their users' activities for purposes other than protecting their own networks, as they are currently allowed to do. It also provides companies with complete liability protection for information sharing and monitoring pursuant to the Act. Lastly, CISA includes worrisome provisions that have nothing to do with information sharing at all, like an authorization for private entities to operate defensive measures on their networks which may still have harmful effects on innocent third parties, and some out-of-place language that has worrisome implications for the NSA's development and use of cyberweapons.

What follows is our best attempt to highlight the most glaring problems with CISA—and propose solutions.

Problem #1: CISA would authorize excessive information sharing, including unnecessary sharing of personal information.

First, the definition of the term "cybersecurity threat" is very broad, and would allow companies to share a wide variety of information with the government if there is the mere possibility that there may be "an unauthorized effort to adversely impact" an information system, or information stored on or transiting that system. Before sharing their users' information with the government, a company should at least be required to make a determination that the purported cyber threat is likely to cause harm. (Sec. 2(5))

Additionally, CISA would authorize companies to share an excessive amount of their users' information with the government and with one another. It defines what can be shared, "cyber threat indicators," to include "information that is necessary to describe or identify" any "attribute of a cybersecurity threat" so long as disclosure of the underlying attribute is not otherwise legally prohibited. Something that "describe[s]" an "attribute" of a "threat" could be interpreted so broadly as to include personally identifiable information (PII) or the content of private online communications, that is not actually needed to detect or protect against that threat. (Sec. 2(6))

Moreover, and notwithstanding any other law, companies may share this information for any "purposes permitted under th[e] Act," including, but not limited to, cybersecurity purposes. (Sec. 4(c)(1)) This means that companies may choose to share information to assist law enforcement in its investigations into and prosecutions of any of the crimes listed in the law enforcement use provisions in the bill, which include many crimes that have nothing to do with cybersecurity threats. (Sec. 5(d)(5)(A))

Further, CISA would fail to protect users' PII. It would merely require that companies remove personal information if they "know" that it is not "directly related" to the threat. This weak protection could result in companies unnecessarily sharing the PII of victims, and even their contacts, with the government and other companies. Additionally, the "knowledge" element would allow companies to default to leaving PII in the indicators they share, since they may not know with absolute certainty that the PII they have identified is not directly related to the threat. Instead, CISA should require companies to remove PII from indicators unless it is necessary to identify or mitigate a threat. The bill should also require that government entities review indicators for improperly shared PII, and remove it before using or disseminating the indicators. (Sec. 4(d)(2))

Solution #1: CISA should only authorize a company to share information, including PII, if it is necessary to identify, block or mitigate the impact of a cyber-attack or vulnerability that the company has determined to be likely to cause harm. Additionally, government entities receiving that information should be required to review it for improperly shared PII and remove that PII before disseminating the information further.

Problem 2: CISA Would Require DHS to automatically and indiscriminately disseminate to the NSA all indicators it receives.

In addition to authorizing companies to share threat indicators with the Department of Homeland Security (DHS) in exchange for liability protection, CISA would also require that DHS immediately disseminate all of those threat indicators, including all of the personal information that comes with them, to a myriad of government agencies ranging from the NSA and the Central Intelligence Agency (CIA) to the Federal Bureau of Investigation (FBI) and the Department of Commerce. (Sec. 4(b)(2)) It would also prohibit DHS from doing anything to impede the real-time dissemination of those indicators, or to modify them in any way. (Sec. 5(a)(3)(ii)) This would make it impossible for DHS to conduct a second review of indicators to identify and remove improperly shared personal information before transmitting it to the NSA or any other agency.

Additionally, companies are authorized to share indicators directly with any federal entity, including the NSA, though they would forgo liability protection if they chose to share with any federal entity other than DHS. (Sec. 4(c))

Management of and response to domestic cybersecurity threats should be controlled by a civilian agency. Requiring a civilian agency like DHS to automatically and indiscriminately disseminate that information to military intelligence agencies like the NSA undermines civilian control. Additionally, CISA should not create a new authorization that would allow companies to share information with any non-civilian federal entity. Entities within the Department of Defense, like the NSA, should only have access to information concerning significant cyber threats, such as threats that could result in a significant loss of life or physical destruction of critical infrastructure; state sponsored espionage, including economic espionage; or the activities of foreign criminal organizations.

Solution #2: CISA-derived information should only be disseminated to the NSA to address a discrete set of significant threats to national security.

Problem #3: Law enforcement agencies are authorized to use CISA-derived information to investigate a wide array of garden-variety crimes.

If excessive sharing of Americans' personal information is not enough to establish that CISA is as much a surveillance bill as it is a cybersecurity bill, the breadth of investigations and prosecutions that law enforcement can use the information for leaves no room for doubt. It is reasonable to authorize federal and state law enforcement to use CISA-derived cyber threat indicators to investigate and prosecute a clearly defined set of computer crimes. However, CISA authorizes this and much, much more.

CISA would allow any entity within the federal government, including intelligence agencies and law enforcement, to use the information it receives from companies for investigation or prosecution of any crimes that could result in imminent death or serious bodily harm, or even

just serious economic harm. That means the data shared under this "cybersecurity" bill would be used to investigate garden-variety violent crimes or economic crimes that have nothing to do with cyber threats. This allowance for investigation or prosecution of imminent physical or economic crimes that are unrelated to cybersecurity also extends to acts of terrorism, which as we've seen over the last year and a half of NSA leaks, may be interpreted by the Intelligence Community to constitute a blank check for surveillance of all Americans. If that weren't worrisome enough, the bill would also let law enforcement and other government agencies use information it receives to investigate, without a requirement for imminence or any connection to computer crime, even more crimes like carjacking, robbery, arson, possession or use of firearms, ID fraud, and espionage. And that's just a few of the crimes on the very long list of crimes for which CISA-derived information can be used.

While some of these are terrible crimes, and law enforcement should take reasonable steps to investigate them, they should not do so with information that was shared under the guise of enhancing cybersecurity. This authorization would not just seriously undermine Americans' Fourth Amendment rights, which would otherwise require the government to obtain a warrant based on probable cause to access much of that same information, it would create an expansive new means of general-purpose government surveillance. (Sec. 5(d)(5)(A))

Solution #3: Law enforcement entities like the FBI should only be able to use CISA-derived information to investigate or prosecute a clearly defined set of computer crimes. Any authorization for use in investigating violent crimes should be limited to cases where violence is imminent.

Problem #4: CISA authorizes companies to monitor all of their users' activities and communications.

CISA's monitoring provision is unnecessary, overbroad, and would threaten Americans' privacy and Internet security. The federal Electronic Communications Privacy Act (ECPA) protects Internet users' privacy and Internet security by only authorizing companies to monitor their users' activities as necessary to protect their own systems from threats. CISA would undermine those reasonable limitations by providing a blanket authorization for companies to generally monitor their networks for any cybersecurity purpose. (Sec. 4(a))

This would significantly increase the scope of how companies can monitor their customers' online communications and activities. For example, an Internet Service Provider (ISP) that is currently authorized by federal law to monitor traffic on its network in order to identify and counter threats to its own systems would be authorized under CISA to monitor *all* traffic looking for *any* threat to *any* system. That would make everyone a target for monitoring, not just suspicious actors threatening the ISP's network.

Solution #4: CISA should not create any new authorization for monitoring, as adequate authorizations already exist in the law.

Problem #5: CISA's liability protections leave customers no recourse if they are wrongly harmed by information sharing and monitoring.

CISA would absolve companies of any liability associated with sharing or monitoring of information pursuant to the Act, except for actions that constitute gross negligence. This provision would preclude causes of action for violations of the Computer Fraud and Abuse Act as well as privacy statutes such as the Stored Communications Act and Wiretap Act portions of ECPA. (Sec. 6)

Solution #5: CISA's liability protections should be narrowed to ensure that there is reasonable recourse for those harmed in the event that a company unnecessarily monitors or shares their personal information.

Problem #6: CISA authorizes companies to deploy potentially dangerous defensive measures that could harm the computers of innocent people, and contains worrisome language regarding military cyber operations.

Lastly, CISA includes provisions that have nothing to do with information sharing at all. It authorizes companies, "notwithstanding any other provision of law," including anti-hacking statutes like the Computer Fraud and Abuse Act, to deploy defensive measures on their systems against perceived attackers. (Sec. 4(b)(1)) The definition of "defensive measure" (Sec. 2(7)(a)) has been significantly narrowed from the original draft, which defined and authorized "countermeasures" instead of "defensive measures." Nonetheless, this provision is still broad enough to cause serious concern.

CISA would authorize entities to deploy defensive measures for "cybersecurity purposes." (Sec. 4(b)(1)) The bill defines cybersecurity purposes so broadly as to potentially include any actions taken to protect a computer system or data against any possible threat, even where there is an extremely low likelihood that harm would result from the threat. (Sec. 2(4)). CISA would require that an entity apply a defensive measure only to its own network or on another consenting entity's network (Sec. 4(b)(1)), and would further require that a defensive measure not "destroy[], render[] unusable, or substantially harm[]" another entity's information system or data on their system without their permission. (Sec. 2(7)) These are important limits. However, it is unclear what level of harm must occur to constitute "substantial harm," and CISA would immunize a company that negligently or even intentionally deployed a defensive measure in a manner that caused harm to an innocent third party's systems, so long as that harm was not determined to be substantial. Even if the harm was to the computer systems of a hospital, a Fortune 500 business, a power plant, a friendly foreign government or any other innocent entity or individual, that company would still have been acting within CISA's authorization and be protected against liability for that harm. Similarly, CISA could be aggressively read to authorize and immunize the use of defensive measures that rendered another information system only partially unusable rather than completely unusable, regardless of whether the owner of that system did anything wrong, and regardless of what critical services that system might offer.

In addition to the concern about what harms may result from the authorization to deploy defensive measures, the need for this new authorization is unclear. Entities can already take actions on their own networks to defend those networks under current law. For example, they can employ firewalls, block known malicious IP addresses from accessing their networks with DNS blacklists, allow only authorized users access to their networks with DNS white lists, scan traffic on their networks to identify malicious code, and set up fake targets or "honeypots" on their networks to lure attackers away from sensitive information and gain information about them that is needed to defend those networks. With such a range of options already available, new language authorizing broadly defined "defensive measures" carries great risk for little clear reward.

In addition to the troubling allowance for "defensive measures", CISA also includes an odd rule of construction that states that nothing in the Act should be interpreted to limit the authority of the Secretary of Defense to "develop, prepare, coordinate, or, when directed by the President, conduct military cyber operations." (Sec. 8(m)) It is unclear why such a statement concerning the Secretary of Defense's authority is needed, or what its intended effect is. What is clear is that the NSA engages in a wide array of offensive cyber activities from purchasing and stockpiling vulnerabilities, to inserting vulnerabilities into software and firmware, to undermining encryption standards, to deploying surveillance malware and even cyberweapons like Stuxnet. Some of these activities may be reasonable; many are certainly not. Regardless, they unquestionably impact the security and functionality of the Internet and the broader computing environment, and their efficacy and legality should be the subject of public debate rather than the subject of vague carve-outs in overbroad cybersecurity information sharing bills.

Solution #6: CISA should not create any new authorization to use defensive measures, and it should not include a Rule of Construction concerning military cyber operations, since the necessity and intent of both provisions is unclear.

If CISA is intended to increase cybersecurity and not surveillance, it should exclude unnecessary and dangerously broad authorizations for new monitoring and defensive measures, and it must narrowly define what information can be shared (including robust requirements to remove unnecessary personal information), when information can be shared, and how information can be used. Unless all of the problems we've summarized above are addressed, CISA will do much more to enhance the government's cyber-*surveillance* than it will do to enhance everyone's cybersecurity, and should be strongly opposed.