



Legislative Bulletin.....April 26, 2012

Contents:

H.R. 3523 – Cyber Intelligence Sharing and Protection Act

**H.R. 3523 – Cyber Intelligence Sharing and Protection Act
(Rogers, R-MI)**

Order of Business: H.R. 3523 is scheduled to be considered on April 26-27, 2012, under a structured rule making sixteen amendments in order. The rule waives all points of order against provisions in the bill and the rule also waives all points of order against consideration of the bill. The rule provides for one hour of general debate equally divided and controlled by the chair and ranking minority member of the Permanent Select Committee on Intelligence. The rule also provides one motion to recommit with or without instructions.

Summary: This [legislation](#) amends the National Security Act of 1947 to allow and encourage the sharing of cyber threat intelligence with private-sector entities. The legislation requires the Director of National Intelligence to establish procedures for the sharing of this information with properly certified entities to help protect U.S. national security while protecting information from unauthorized disclosure. The legislation also allows cybersecurity providers to gain access to, and share, information when they have the express consent of a protected entity to do so. Regulations are put in place to protect shared information from being used to gain a competitive advantage, and information the federal government collects is exempt from public disclosure. No legal cause of action can be maintained in federal or state court for someone, acting in good faith, who either shares or does not act on shared information.

In principle, everyone agrees to information sharing in some form, in fact there already is a large amount of information sharing between companies like Verizon and Comcast. These companies claim, however, that legal uncertainty prevents them from sharing much more information. This lack of information sharing, according to the involved parties, makes it hard to track attack patterns, allegedly leaving both sides in the dark.

Since everyone agrees to information sharing, in principle, the critical questions are:

- **What is the federal government's role?**
- **What information is shared?**
- **How is that information shared?**
- **Has that information been stripped of personally identifiable information (PII)?**
- **Who will have access to that information? The government? And if so, civilian agencies or NSA?**
- **And perhaps most importantly, what happens to that information after? Can it be used by the government for a non-cyber purpose? How long is it retained?**

These are critical questions in part because this legislation will pre-empt over 20 existing laws, including the Privacy Act, Wiretap Act, Electronic Communications Privacy Act etc. (it's unclear even what federal and state laws CISPAs might implicate). Some argue, that in order to retain existing privacy protections, not to create new ones, this legislation must have similar privacy protections to protect our private information from being wrongfully used by the government or by the private sector.

For these reasons, Rep. Thornberry's House Republican Cybersecurity Task Force, [advised](#) that "the protection of personal privacy should be at the forefront of any limited legal protection proposal" relating to information sharing.

Federal Cybersecurity:

Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for critical infrastructure, such as the Department of Transportation for the transportation sector. Cross-agency responsibilities are complex, and any brief description is necessarily oversimplified.

- In general, in addition to the roles of White House entities, Department of Homeland Security (DHS) is the primary civil-sector cybersecurity agency.
- National Institute of Standards and Technology (NIST), in the Department of Commerce, develops cybersecurity standards and guidelines that are promulgated by Office of Management and Budget (OMB). The Department of Justice is largely responsible for the enforcement of laws relating to cybersecurity.
- The National Science Foundation (NSF), NIST, and DHS all perform research and development (R&D) related to cybersecurity.
- The National Security Agency (NSA) is the primary cybersecurity agency in the national security sector, although other agencies also play significant roles.
- The recently established U.S. Cyber Command, part of the U.S. Strategic Command in the Department of Defense (DOD), has primary responsibility for military cyberspace operations.

Current Law on Privacy and Cybersecurity:

- The collection and sharing of communications information for cybersecurity purposes currently must comport with surveillance statutes, including the Wiretap Act, the Stored Communications Act, the Foreign Intelligence Surveillance Act, and the pen register and trap and trace statute.
- These laws already give substantial authority to providers and other system operators to monitor their own networks for cybersecurity.
 - For example, the Wiretap Act permits electronic communication service providers to intercept, use, and disclose communications passing over their networks while they are engaged in any activity that is a “necessary incident” to the protection of their rights and property.
- In addition, the computer trespasser exception to the Wiretap Act permits a service provider to authorize the government to intercept the communications of a person who accesses a computer without authorization if there are reasonable grounds to believe that the communication is relevant to an investigation of the trespass. Transparency about the extent of disclosures now being made under these exceptions would enhance the ability of Congress and the public to assess their effectiveness and impact on privacy.

Rep. Thornberry’s House Cybersecurity Task Force:

In October, 2011, the House Cybersecurity Task Force unveiled its [recommendations](#) to help guide legislative action. Their recommendations are critical for understanding current cybersecurity proposals. Regarding information sharing, this document explained:

“Liability concerns have also been a common roadblock for information sharing within existing structures. We believe that information sharing within existing structures can be improved through limited safe harbors when private sector entities voluntarily disclose threat, vulnerability, or incident information to the federal government or ask for advice or assistance to help increase protections on their own systems. These protections would need to address concerns about antitrust issues, liability, an exemption from the Freedom of Information Act (FOIA), protection from public disclosure, protection from regulatory use by government, and whether or not a private entity is operating as an agent of the government.”

“However, the protection of personal privacy should be at the forefront of any limited legal protection proposal.”

Analysis of Potential Conservative Concerns: The following are some concerns that have been expressed by some conservative analysts and groups. While many conservatives support the bill, or would disagree with these arguments, the following analysis (with counter-arguments in the conservative support section) is provided for your information.

Privacy Concerns:

The Department of Homeland Security, in 2008, articulated a series of [principles](#) of dealing with privacy in the context of cyber security. They explained that this protection means:

- Users are given notice of the cybersecurity monitoring and information sharing program and that it may involve collection and use of personally identifiable information (PII).
- The cybersecurity purpose for which the PII would be collected is carefully articulated.
- Only the PII necessary to accomplish the purpose is collected and shared, and it is used only for cybersecurity matters.
- PII collected for cybersecurity purposes should be retained only as long as it takes to fulfill the specified purpose, and then should be deleted by all parties.
- To the maximum extent feasible, information is sanitized of information identifying innocent parties before it is shared.
- The PII collected is accurate, relevant, and timely, and it is properly safeguarded against unauthorized access or improper disclosure
- Actual use of the PII is audited to ensure compliance with these principles.

Privacy advocates argue that H.R. 3523 does not abide by the DHS's principles on privacy.

Privacy Groups Concerns
(including CDT, Cato, EFF among others):

Over twenty existing provisions of federal law would be preempted by this law (in the context of information sharing). These laws have decades of built in privacy protections, so the privacy concerns expressed by some conservative groups are not about new privacy protections; rather, they are simply about preserving some of the old privacy protections in the context of information sharing of even more private information (our hard drives, web history, e-mails etc.).

CISPA would also preempt all forms of legal action arising under common law, including actions for breach of contract, intrusion upon seclusion, etc. Therefore, a private entity sharing information with a government agency pursuant to CISPA may not be sued by an individual or business user—even if such sharing violated a voluntary contract and caused economic injury to the user.

In the context of this legislation, several groups worry that in bypassing over twenty separate pieces of legislation that protect our privacy interests, we need to re-build those privacy protections into this legislation as outlined in the DHS principles, and reiterated in Rep. Thornberry's Taskforce [Report](#).

These privacy groups have five major privacy concerns:

1. CISPA may allow intelligence agencies to collect sensitive data on US citizens.
 2. There are no limitations on the secondary use of collected cyber-data.
 3. The legislation requires no anonymization, minimization, or removal of PII before it is turned over to the federal government.
 4. The technical definitions related to "cybersecurity" are too vague.
 5. A lack of oversight over the legislation's implementation.
-
1. *CISPA allows companies to share with intelligence agencies sensitive data on U.S. citizens.*
 - I. In the US, long standing laws prevent the military and intelligence agencies operating on US soil against American citizens. In addition, electronic surveillance laws prevent companies from sharing the content of Internet communications as well as transactional information about Internet communications without a court order.
 - a. However, CISPA may create a backdoor for the National Security Agency (NSA) to collect sensitive information about individual Internet users. As CISPA is currently written, a cybersecurity provider or self-protected entity "notwithstanding any other provision of law," may share data with any other entity "including the Federal Government."
 - b. The information may be transferred to the Department of Homeland Security (DHS) or to other agencies that then pass the data to DHS. From there, DHS is permitted to hand the information over to other government agencies, including the NSA. This creates a mechanism for the NSA to receive the communications of American citizens.
 2. *Secondary uses of collected data. What can the government do with information after it has been shared for cyber security purposes?:*
 - I. Under CISPA, although data collected by companies may only be shared for 'cybersecurity' purposes, the government can use it for unrelated purposes as well. First, the bill allows the government to use it for "national security purposes." Then, provided "at least one significant purpose" is a cybersecurity or national security purpose, it may be used for *other* unrelated purposes.
 - II. When a government agency receives cyber threat information, it may use that information *for any non-regulatory purpose* as long as at least "one significant use" is for a "cybersecurity" or "national security" purpose.

- Therefore, data obtained by government pursuant to CISPA could be used for any number of reasons entirely unrelated to cybersecurity (e.g., prosecutions for violations of the Internal Revenue Code, National Firearms Act, etc.).
- III. This language fails to appropriately restrict information usage, allowing data collected for cybersecurity purposes to be used for investigations by the IRS, DEA or other agencies so long as one additional use of the data are either national security or cybersecurity.
 - Combined with broad immunities to companies to collect data and share it with the government, the trove of data collected under the auspices of a cybersecurity purpose could prove to be fecund ground for investigations on issues related to a variety of minor investigations.
3. *The legislation requires no anonymization, minimization, or removal of PII by the private sector:*
 - I. Other than the definitions in the bill, no real guidelines are provided to companies about what data can be collected and transferred, and the bill offers companies sweeping immunities provided they act in "good faith," giving them complete exemption from liability for all "decisions made" based on "cyber threat information" —a term the bill leaves nebulous. If CISPA passes, companies acting in good faith lose any legally-based incentive to protect user privacy, such as federal or state privacy laws that stop companies from sharing sensitive personal information.
 - II. Companies are not obligated to remove the sensitive personal information of individuals unrelated to the cybersecurity issue that is prompting them to share customer information with other companies or with the government. The bill places all reliance on minimizing and anonymizing personal information at a sharing company's discretion.
 - III. As a result PII about people who are of no cybersecurity interest can end up in intelligence data bases.
 4. *The definitions related to "cybersecurity" may be too vague. How does a company decide whether there's enough relationship to a threat to justify sharing a given user's information?:*
 - I. The language authorizes the sharing of "cyber threat information" defined as "information pertaining to the protection of a system or network" from efforts degrade, disrupt or destroy it, or to gain unauthorized access.
 - a. Since every communication may include malware and since providers routinely examine all communications passing over their networks in order to protect their networks against these evils, this may permit companies to share entire streams of communications with the government.
 - b. Could that information include user names, addresses, or credit card data? Could it include the contents of private emails, social

networking postings, or enterprise databases containing customer information and trade secrets stored with cloud computing providers?

- c. A large amount of information is shown through your activities online, including a personally identifiable MAC address for every computer and IP number for every internet connection (which can be easily, and legally traced to your home address). Further, your cookies and user profile data show information from many of your previous online sessions.
- d. Technologists have raised red flags about these definitions; it is unclear what they will translate to in practice and they provide a tremendous amount of leeway. This raises a host of questions, such as what restrictions there are on communications that could be transferred to the government and whether the ordinary use of important privacy-enhancing technologies or encryption will justify information-sharing under this proposed statute.
- e. Users will not know whether their information was inappropriately shared because it is not FOIA able.
- f. The Department of Justice holds that the term “unauthorized access” as used in the Computer Fraud and Abuse Act includes violating a website’s terms of service, or an employer’s computer use agreement. Under the DOJ interpretation, attempts to create a Facebook account by entering an inaccurate age, or using an employer-provided computer to watch YouTube videos, would fall under the CISPA definition of “cyber threat information.”

II. “Cybersecurity system” is defined as a system that “cybersecurity providers” or self-protected entities use to monitor and defend against cyber threats. As it stands now, the definition may be too broad.

- a. This is a “system” intended to safeguard “a system or network.” But that could mean anything -- a password for Local Area Network or a Wide Area Network, a microchip, a security control for a website, online service, or a DVD. It could also mean the government’s own Einstein intrusion detection system.
 - It might easily be stretched to be a catch-all term with no meaning. For example, it is unclear whether Digital rights Management (DRM) on a DVD constitutes a “cybersecurity system.”
- b. Such a “cybersecurity system” is defined to protect a system or network from “efforts to degrade, disrupt or destroy” and this language is similarly too broad.
 - Degrading a network could be construed to mean using a privacy-enhancing technology like encryption, or a p2p protocol, or downloading too many files.

- c. Such a “cybersecurity system” is defined to protect against “efforts to gain unauthorized access,” and this appears to be very broad. This could be implicated, for example, by using pseudonyms on social networking websites, or using an open Wi-Fi network.

5. *Potential oversight problems:*

- a. Tragically, both the law enforcement and intelligence sides of the federal government have a history of abusing access to information, with very little in the way of accountability for abuse.
 - For example, the FBI has been called out multiple times for [abusing "national security letters"](#) to get access to information without a warrant, but it doesn't appear that just calling them out on it has stopped the abuse.
- b. The sweeping immunity provisions exempt companies from all forms of civil or criminal liability as long as the company is acting in “good faith” in accordance with the statute. This effectively denies a private company or user any legal recourse against a provider for sharing sensitive data in breach of contract, so long as that provider honestly believed the data pertained to a cyber threat. This undermines the ability of providers to compete on privacy and make enforceable promises to customers about how their data will be shared.

Outside groups with privacy concerns:

- American Conservative Union, Americans for Limited Government, FreedomWorks, Tech Freedom and the Liberty Coalition recently released a [letter](#) to Chairman Rogers on their privacy related concerns, and requests for amendments.
- Center for Democracy and Technology has written several [posts](#), and [here](#), on their concerns with the legislation and presented several [briefings](#) to explain their privacy concerns. They recently released a [chart](#) comparing the different cyber legislation for consideration (Lungren’s bill has changed and that block is out of date).
 - Also read their [document](#) on their seven-step plan for cybersecurity while protecting privacy.
- [Here](#) is another article on overall privacy concerns.

Should the Federal Government be Involved in Private Sector Cybersecurity?

Some argue the answer is no because:

1. Some argue that cybersecurity is thousands of different problems that will be handled by hundreds of thousands of different actors over the coming decades. Rather than trying to regulate the private sector’s approach to secure technical infrastructure, the government should ensure that responsibility lies with the owners of it in the private sector, and then get out of the way. The private sector has the incentives and the knowledge to address cybersecurity problems.

2. Some argue that to the extent information sharing is needed, much of it is already happening. There is no need for a government program to create information sharing. In the narrow areas where federal law and regulation stand in the way of appropriate cybersecurity efforts, Congress should clear out that regulatory underbrush, not make more of it.
 - Companies are saying they want information sharing because they want immunity from liability. If they say they would share more or other information, you should ask them what information they are not sharing and why. Then amend or repeal whatever law it is that is preventing the information sharing. Chairman Roger's staff responds to this by explaining that the private sector has less of an incentive to share information if they are subject to potential liability from sharing too much information.

Some conservative groups, like [Mercatus](#) and [Cato](#), have questioned whether this is a situation where there is a market failure (as far as the private sector defending on cybersecurity) that requires federal government involvement at all. Jerry Brito, with Mercatus, argues [here](#) that:

“[J]ust because a threat exists doesn't mean regulation is necessary. If that were the case, Americans would need laws to tell us what kind of locks to put on our doors. We don't have such laws, of course, because individuals have an incentive to protect their own homes.”

Brito explains in another [paper](#), that the threat of cyber-terrorism is greatly exaggerated:

“Security risks to private and government networks from criminals and malicious state actors are no doubt real and pressing. However, the rhetoric of “cyber doom” employed by proponents of increased federal intervention in cybersecurity implies an almost existential threat that requires instant and immense action. Yet these proponents lack clear evidence of such doomsday threats that can be verified by the public.”

His recent briefing on April 12, 2012, is available in [video](#) with his [PowerPoint](#) presentation as well. This provides the more thorough presentation of his argument.

Cato's Jim Harper has also provided skepticism of this being an area that requires federal government involvement (see [here](#) at a recent briefing, and a blog post [here](#)):

"For me the question isn't which bills in which House should move, but whether Congress can provide any value to the problem of fixing all the problems that comprise cybersecurity" (read article [here](#)).

"Congress has no particular capacity or knowledge of how to do cybersecurity," Harper says. "It's not a choice between two different versions in the House and two different versions in the Senate. The question is still open: is Congress capable of doing any good here?" (read [here](#)).

Other legislation, particularly on the Senate side, includes private sector mandates, and provides broad authority for the federal government in the realm of cyber (which will soon be everything), and vague definitions of who would be affected (e.g. "critical infrastructure"). H.R. 3523 appears to be significantly less intrusive than those alternatives, but these conservative groups argue that it could still give the federal government a larger role.

Conservative Support:

Appearing before the [Senate Armed Services Committee](#) in June, then-CIA Director Leon Panetta said, "The next Pearl Harbor could very well be a cyber-attack that cripples our government, security and financial systems." Cybersecurity has been identified as one of the most pressing national security challenges of our time by our national security agencies ([see here](#)). In addition, [cyber-weapons](#) are considered to be part of the American military arsenal, as well as that of our adversaries ([see here](#)).

With roughly [1.8 million cyber-attacks](#) already aimed at Congress and federal agencies, cyber-terrorism already poses a massive threat to our national security, and with 60,000 new malicious software files being developed daily, the problem will only get bigger. The United States is dependent upon our internet-enabled infrastructure. Hackers and nation-states have shut down American websites and stolen terabytes of private information (including classified information).

Center for Strategic and International Studies (CSIS) has prepared a list of 96 significant cyber incidents since 2006 (see [here](#)). Nation states are currently able to attack, exploit and exfiltrate data from thousands of private companies as well as the federal government. There are few defense contractors that have not either been hacked or been targeted in a sophisticated attempt. Even more worrying, these capacities are starting to trickle down to sophisticated criminal syndicates and it is widely believed that some cyber techniques are already available to terrorist groups.

Because of the relative anonymity of cyber-attacks, the ability to attack an adversary from afar, and a current policy of non-retaliation, there is little incentive for a nation-state or terrorist group not to use this technology. By far the most common current occurrence of cyber-attack is [cyber espionage](#), where foreign countries, specifically [China](#), steal billions of dollars of American intellectual property both in the civilian world and in the defense industry. According to the bill's sponsors, estimates of loss from economic espionage range from \$2 billion per year to \$400 billion per year worldwide. Information related to aircraft, cars, and chemicals are among some of the major technology areas stolen by the Chinese through cyber-espionage.

American Companies and the Federal Government Remains Vulnerable.

- CSIS has prepared a thorough report for incoming President Obama, prepared in December 2008, regarding the importance of securing cyberspace ([see here](#)). This report found, “Inadequate cyber security and the loss of information has inflicted unacceptable damage to U.S. national and economic security.” The Commission’s three major findings are:
 1. Cybersecurity is now a major national security problem for the United States.
 2. Decisions and Actions must respect privacy and civil liberties.
 3. Only a comprehensive national security strategy that embraces both the domestic and international aspects of cybersecurity will make us more secure.
- Recently, April 17, 2012, at the Cyber Security Caucus briefing, previous Director of Homeland Security Michael Chertoff explained the necessity of acting to address the threat that he identified as intolerable ([see here](#), and [here](#)).
 - Other videos from this briefing: Jeff Snyder (Raytheon) and Thomas Gann

State of Cyber Attacks and the problems

- There are no international boundaries on the Internet
- There are safe havens for criminals where they may operate without consequence. Some havens provided in return for services or technology
- Governments enlisting the services of traditional cybercrime criminals to advance their information warfare capabilities.
- Governments funding training programs for information warfare
- Cost of Cyber Attacks is decreasing, effectiveness is increasing.
- Cyberspace is part of the battlefield of the 21st Century

(McAfee) (see [here](#)).

- Liesyl Franz (TechAmerica) (see [here](#))
- The Council on Foreign Relations fellow Mike Cote has put out a useful power-point on the threats we face ([see here](#)):
- Individual hackers are also able utilize exploits to gain [private information](#), credit card data or even access your laptop’s [camera](#):

“Despite billions spent on technology that lets us broadcast our daily lives, all it takes is one guy, a self-taught hacker with no college degree, to turn that power against us.”

- Denial of Service (DDoS) attacks, a relatively simple technique, have been used by “Hacktivists” to shut down thousands of websites (see [Anonymous](#)’s [attacks](#) as an [example](#)).

Benefits of this legislation over alternatives:

- To be clear, this legislation does not have an “[internet kill switch](#)” which some inferred from previous legislative text, specifically on the Senate side from several years ago.
- This legislation does not have language referring to “critical infrastructure” and mandating certain requirements for this “critical infrastructure.” These provisions are in some other bills, specifically in the Lieberman-Collins legislation. H.R. 3523 is entirely voluntary for the companies involved.
 - This “critical infrastructure” requirement was very worrying for a number of industries. It remained unclear to several industries if they were, or were not “critical infrastructure” and the term seems designed for federal encroachment (as it’s easy to argue that many industries are “critical,” there is, in fact, a legitimate question as to whether or not Google would be “critical infrastructure”).

Why we need this form of information sharing:

From Chairman Rogers (R-MI) on his legislation (read [here](#), and here is an [article](#) by him in US News & World Report on his legislation):

“Today, the United States government protects itself against cyber espionage by using both classified and unclassified cyber threat information.”

- “However, the vast majority of the private sector doesn’t get the benefit of the classified threat intelligence that the government already has in its possession.”
 - “If the government were able to share its classified threat information, the private sector would be able to better defend itself against nation-state actors in cyberspace.”
 - “An important experiment recently conducted by the Defense Department proves that this can work. The Defense Industrial Base Pilot program provided classified cyber threat intelligence to communications service providers who used it protect defense contractors. The pilot showed that sharing intelligence can enhance private cybersecurity without any government monitoring.”
- “The bill provides positive authority to private sector entities to defend their own networks and those of their corporate customers, and to share cyber threat information with others in the private sector, as well as with the federal government on a purely voluntary basis.”

- “Voluntary information sharing with the federal government improves the Government’s ability to protect against foreign cyber threats.”
- “By allowing the private sector to expand its own cyber defense efforts and to employ classified information to protect systems and networks, this bill will harness private sector drive and innovation while also keeping the government out of the business of monitoring and guarding private sector networks.”

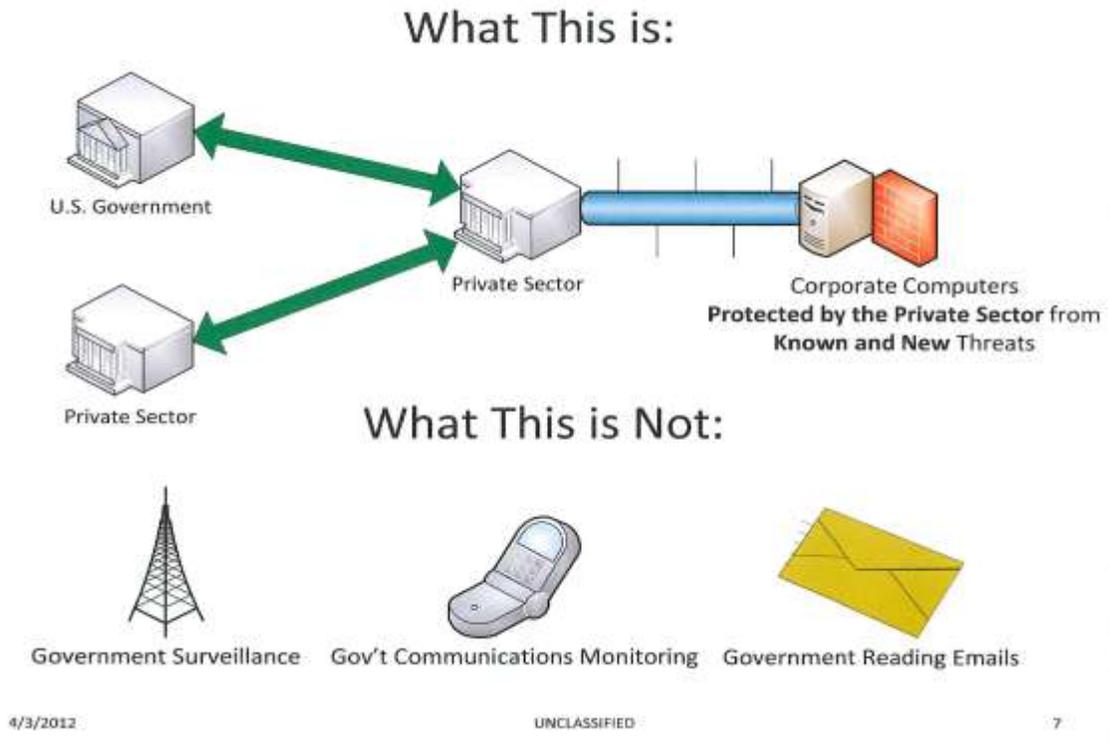
In regard to privacy concerns, Chairman Rogers (R-MI) responds:

“The bill protects privacy by prohibiting the government from requiring private sector entities to provide information to the government, and by encouraging the private sector to “anonymize” or “minimize” the information it voluntarily shares with others, including the government. In addition, the bill requires an independent Inspector General audit of any voluntary information sharing with the government.”

In particular, Chairman Rogers (R-MI) responds:

- The information sharing is completely voluntary by the private sector.
- Quid pro quo for information sharing is specifically disallowed.
- Data mining is restricted “The Federal Government may not affirmatively search cyber threat information shared with the Federal Government. . . for a purpose other than [a cybersecurity purpose or the protection of the national security of the United States].
- Annual Inspector General Review, “submit to the congressional intelligence committees a report containing a review of the use of information shared with the Federal Government under this section” including “a review of the use by the Federal Government of such information for a purpose other than a cyber security purpose. . .”

From Chairman Rogers (R-MI):



In regard to criticism of the term “cyber threat information” and “cybersecurity purposes” being too broad, Chairman Rogers responds:

- “The definition of “cyber threat information” in the bill is limited only to information that directly pertains to a threat to, or vulnerability of, a system or network.”
 - “This definition ensures that the only information being identified or shared is limited to information about real cyber threats and vulnerabilities.”
 - “Today, the Chinese and other nation-state actors are stealing large amounts of corporate information and sensitive government information; this expansive, aggressive effort undermines the free market and costs valuable American jobs. We must provide our private sector the information it needs to defend itself.”
 - “Similarly, hackers stealing tremendous amounts of personal information belonging to individuals, from credit card and social security numbers to medical records. We must provide the companies that provide critical services to ordinary Americans with the threat information they need to protect our personal information.”
 - “We continue to work with various groups to see if the definitions in the legislation can be even more narrowly tailored, but it is important that any

definitions be flexible enough to deal with rapidly changing technologies and the various adaptive tactics used by high-end nation-state hackers. “

- “The law is hard to change and locking in technology-based definitions can lead to significant challenges.”
 - “It is also important to ensure that any definitions in the law not provide a roadmap for attackers to determine exactly what types of threats can be identified and then develop techniques that aren’t covered by the law.”
- “It is also important to note that under the bill a company may only identify and share cyber threat information for “cybersecurity purposes”; that is only when they are seeking to protect their own systems or networks or those of their corporate customers.”
 - “This means that the bill only authorizes activities when companies are actually protecting themselves or their corporate customers against real threats to their systems or networks.”

In response to limiting secondary uses of the information by the federal government, Chairman Rogers (R-MI) ’s responds:

- “Limiting the government’s use of voluntarily shared information to a handful of specific purposes runs the risk of the government having to ignore information that it has in its possession.”
 - “For example, if the government was restricted to only using the information shared for cybersecurity purposes, the government might be required to ignore information properly provided to the government, even if it described a terrorist plot or contained specific evidence of child pornography being created.”

Outside Support:

- Heritage Foundation’s Paul Rosenzweig has put out a [paper](#) in support of several of the House bills, including the Rogers bill:

“Under the Rogers–Ruppersberger approach, ambiguities in the law would be eliminated. Private sector entities would be given clear legal authority to defend their own networks and share cyber threat information with others in the private sector as well”

“Public–Private Cooperation. In short, these concepts are based on a cooperative public–private sector arrangement, where government cyber threat information is leveraged to enable the private sector to be aggressive in its own cyber defense. Instead of a command-and-control model that mandates certain actions and contemplates an expanded regulatory state, greater sharing within the private sector and between the government and private-sector actors is a modest first step

that would, in a bipartisan way, attempt to harness the creativity and innovation of the American private sector.”

- His most recent [paper](#) specifically endorses the Rogers approach. In response to privacy concerns he explains:

“Those concerned with CISPA argued that the bill allowed the government to use voluntarily shared information for purposes beyond cybersecurity. But this criticism misses the point that limiting how the government uses lawfully collected information re-erects the artificial walls between intelligence and law enforcement that were a partial cause of the failure to stop the 9/11 attacks. CISPA authorizes the use of shared information if one significant purpose of the use is ‘a cybersecurity purpose or the protection of the national security of the United States.’”

“Civil liberties and technology advocates were concerned that the bill does not mandate that the private sector remove any personally identifiable information before sharing cyberthreat information with the government. While CISPA does not mandate the removal of such personal information, it allows and encourages “appropriate anonymization or minimization of” cyber threat information. A mandate to scrub all personal identifiable information would likely make it difficult if not impossible for private-sector actors to share certain critical threat details. The bill also requires that a cybersecurity provider obtain “the express consent” of an entity that it is protecting before sharing threat information, adding another level of protection to individuals’ information.”

- Mike Brownfield’s piece in Heritage’s Blog: The Foundry, [explains](#):

“Though the United States government has the capability to protect itself against cyber espionage by using both classified and unclassified cyber threat information, the private sector doesn’t get the benefit of this information. Today, the House of Representatives will vote on a crucial bill to do something about it — the Cybersecurity Information Sharing and Protection Act (CISPA), introduced by House Permanent Select Committee on Intelligence chairman Mike Rogers (R-MI) and ranking member Dutch Ruppersberger (D-MD).

Under CISPA, the U.S. government will be able to share information about incoming cyber attacks — that includes providing American companies details on malware, viruses, and other malicious code that pose a threat to their security. That way, attacks can be stopped before they even begin. For their part, the companies would be encouraged to share information about the threats they identify — all on a completely voluntary basis — so that other networks can be protected. That’s valuable information that computer analysts can use to understand the attack, who launched it, where it’s coming from, and how to protect against other attacks like it.

Civil liberty advocates and other critics of the bill have raised concerns that CISPA is a threat to privacy or could result in the blocking of websites, as was the worry with the Stop Online Piracy Act. However, nothing could be further from the truth

[Analysis of the bill shows](#) that CISPA does not allow for any blocking of websites but merely facilitates the sharing of cyberthreat information. It gives no additional authority to the Department of Defense, the National Security Agency, or any other “element of intelligence community to control, modify, require or otherwise direct the cybersecurity efforts of a private-sector entity or a component of the Federal Government or a State, local, or tribal government.”

In addition, the bill includes new measures that would allow the government to use shared cybersecurity information only for a cybersecurity purpose, for a national security purpose, to prevent death or serious bodily harm, or to protect minors from sexual exploitation, kidnapping, and trafficking. That’s in addition to other protections against the improper use of data.”

Contrast between H.R. 3523 and SOPA: Three months ago, Internet activists blacked out their websites in protest and thousands of concerns constituents ended, at least temporarily, the prospects for that legislation to pass. CISPA has been dubbed “SOPA 2” by some tech [blogs](#).

- This fear, if it was ever legitimate, is now superseded by new legislative text. The old language that led some to fear that this was the new SOPA included the bill defining “cyber threat intelligence” and “cybersecurity purpose” to include “theft or misappropriation of private or government information, intellectual property, or personally identifiable information.”
- This latter quotation in the language has been entirely removed, and there is nothing in the text that deals with intellectual property.

Public Protest:

- The fear of this turning into a SOPA 2 are slightly [overblown](#), SOPA’s successful protest had a nexus of the privacy players in the technology community, but also some of the real muscle from Google, Wikipedia, and Reddit. It seems unclear where these organizations are on CISPA, but they are certainly not as vehemently opposed as last time.
- However, some of the previous organizations involved with SOPA are still [mobilizing](#), one [petition](#) has over 750,000 signatories as of writing.

Cybersecurity Materials

Reading Material:

- More reading on the subject can be found ([here](#), and [here](#)), and a directory of all cyber security articles/information can be found [here](#).
- [Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper](#) by CDT, Tech America, U.S. Chamber of Commerce, BSA, ISA.
- McAfee's report - [In the Dark: Crucial Industries Confront Cyberattacks](#)
- Jason Healey, of the Atlantic Council's posting: [The Government's Three Cyber Silences](#)
- Nick Hopkins, [Cyberspace Turns into a Military Battleground](#)
- http://asymmetrictthreat.net/docs/asymmetric_threat_5_paper.pdf
- CRS reports:
 - [Cyber Security: Selected Legal Issues](#) (April 20, 2012)
 - [Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions](#) (April 23, 2012)
 - [Terrorist Use of the Internet: Information operations in Cyberspace](#) (March 8, 2011)

Congressional Hearings/Testimony on Cyber:

- [Senate Select Committee on Intelligence Hearing Prehearing Questions for James Clapper, upon his nomination for DNI](#)

“The U.S. confronts a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat awareness. Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication. Acting independently, neither the U.S. Government nor the private sector can fully control or protect the country's information infrastructure. With increased national attention and investment in cyber security initiatives, the US can implement measures to mitigate this negative situation. The Comprehensive National Cybersecurity Initiative (CNCI) is designed to help mitigate vulnerabilities being exploited by our cyber adversaries and provide long-term strategic operational and analytic capabilities to U.S. Government organizations.”

-Director of National Intelligence James Clapper

- [House Armed Services Committee Hearing on FY 2013 budget request hearing on Cyber Operations Programs](#)
- [House Homeland Security Committee Hearing: Examining the Cyber Threat to Critical Infrastructure and the American Economy](#)

- [House Homeland Security Committee Hearing: The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure](#)
- [House Homeland Security Committee Hearing: Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal](#)
- [House Homeland Security Committee Hearing: Cloud Computing – What are the Security Implications](#)
- [House Homeland Security Committee Hearing: America is Under Cyber Attack](#)

“[T]he number and sophistication of cyber attacks has increased dramatically over the past five years and is expected to continue to grow. The threat has reached the point that, given enough time, motivation, and funding, a determined adversary will likely penetrate any system that is accessible directly from the Internet. Even systems not touching the network are susceptible to attack via other than remote access, including the trusted insider using devices such as USB flash drives, and the supply chain.

The threat continues unabated. U.S. critical infrastructure faces a growing cyber threat due to advancements in the availability and sophistication of malicious software tools and the fact that new technologies raise new security issues that are not always addressed prior to adoption. The increasing automation of our infrastructures provides more cyber access points for adversaries to exploit, and the target set grows daily as more and more data is pushed, transmitted, or stored on the network.” – Former Executive Assistant Director of the FBI, Shawn Henry

- [House Homeland Security Committee Testimony: Why Urgent Action is Needed](#)
 “As cyber attack capabilities become ‘commoditized,’ the temptation for these politically motivated groups to use them against vulnerable U.S. targets will increase. We have not seen terrorist groups use cyber attacks – they seem to have neither the capability nor the interest – but since these groups make extensive use of the internet they could eventually be attracted to cyber attack if the means to carry it out are easily available. Some non-state actors are grouped under the label “Anonymous,” a disparate and decentralized federation of internet activists where many members espouse anti-government or anti American ideas. The name “Anonymous” is misleading, however, as it implies a single entity. Anyone can say they are “Anonymous,” from individuals posting comments on 4Chan to members of foreign intelligence agencies (for whom “false flag” operations are routine). In a few cases,

it appears that cyber criminals have used the name
Anonymous when carrying out their for-profit exploits.”
- CSIS’s Fellow, James Lewis

- [Senate Select Committee on Intelligence Hearing on Current and Projected National Security Threats to the United States](#)
- [Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence](#)

Cybersecurity Terms to Know:

Denial-of-Service-Attack (DDoS):

- Comes in variety of forms but normally involves the use of a large number of computers to make thousands or millions of requests to a particular website.
- Since a website may not be able to accommodate these requests, the DDoS slows down the website or even shuts it down.

Conficker B worm:

- Infected between 9-15 million computers by 2009, and made the infected computers effectively zombie clients. The fear, by security experts at the time, was that this large of a botnet has the computing power of a very sophisticated super-computer and could be used in a DDoS attack.
- It was believed that this number of computers may be large enough to bring down a root server of the internet, crippling the internet itself – however, it turns out that the creators and operators of this worm were instead of a criminal syndicate who preferred to steal credit card information.
- For more information, read [here](#), or [here](#).
- Or read the *Worm: The First Digital World War* by Mark Bowden.

Aurora Project:

- A then-classified project from 2007 that demonstrated that a power generator, located in Idaho National Laboratory, could be destroyed by a cyber-attack.
- In the demonstration, hackers gained access to the control units and told the generators to spin until they destroyed themselves (see [here](#)).
- This technology was part, albeit a small part, of the [Stuxnet virus](#) that affected Iranian nuclear centrifuges.
 - After this demonstration, the GAO issued a vulnerability report on May 21, 2008 regarding the Tennessee Valley Authority entitled, [TVA Needs to Address Weaknesses in Control Systems and Networks](#).

Stuxnet Virus:

- The Stuxnet computer worm was discovered in 2010, and infected over 10,000 computers around the world. However, for most of these computers, the worm did nothing of a malicious nature.
- Iran was particularly affected by this worm, with 58.85% of Stuxnet infected computers located in Iran and only 1.56% of the infected computers in the United States (according to a [Symantec study](#)).
- But unlike other forms of malware, it is believed that this was a [designed](#) cyber-weapon to destroy Iranian centrifuges. It appeared to have no effect on other computers, but when it found the right systems “it was precisely [calibrated](#) in a way that could send nuclear centrifuges wildly out of control.” It is widely believed that this erratic behavior destroyed a large number of Iranian centrifuges and eventually required the [replacement](#) of thousands of Iranian centrifuges, perhaps [sending their nuclear program back](#) by several months or [years](#).
- The design of this program was so [advanced](#), that it is believed that it could only be the work of a nation-state.
- Stuxnet represents one of the first forms of kinetic action through a cyber-attack, and represents that in practice, the Aurora Project’s findings are applicable in the real world.
- “Stuxnet is the start of a new era,” says Stewart Baker, former general counsel of the U.S. National Security Agency. “It’s the first time we’ve actually seen a weapon created by a state to achieve a goal that you would otherwise have used multiple cruise missiles to achieve.”
- “Stuxnet combined deep engineering knowledge and clandestine intelligence techniques with advanced hacking skills. Private hackers and most governments do not yet have the capability to launch a Stuxnet-like attack (but this is coming). That some of the Stuxnet code is publicly available does not really increase risk. Many cyber-attacks are ‘single use’ exploits that work as a surprise but are much less effective after the target reacts and adjusts. In the United States, for example, a 2010 survey found that three quarters of American utilities said they had put in place defenses against Stuxnet. These utilities would most likely be able to deflect a Stuxnet-like attack, while only the others would still be vulnerable.” (CSIS’s Fellow, James Lewis’ House [testimony](#)).
- Read more [here](#) and [here](#).

Committee Action: The legislation was introduced on November 30, 2011, and it was referred to the House Permanent Select Committee on Intelligence. On December 1, 2011, the Committee held a mark-up session, ordering the bill to be reported with a 17-1 vote. The bill was reported to the House on April 17, 2011. The Chairman and Ranking Member of the Committee have also proposed a discussion draft with various changes to be considered on the House floor.

Administration Position: President Obama has declared that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cybersecurity.”

As a result, the President directed a top-to-bottom review of the Federal Government's efforts to defend our information and communications infrastructure, which resulted in a report titled the [Cyberspace Policy Review](#).

However, the [Administration](#) is against this approach to cyber security. In a [statement](#), National Security Council spokeswoman Caitlin Hayden said any cybersecurity legislation should include strong privacy protections and should set mandatory security standards for critical infrastructure systems, such as electrical grids and water supplies:

“While information sharing legislation is an essential component of comprehensive legislation to address critical infrastructure risks, information sharing provisions must include robust safeguards to preserve the privacy and civil liberties of our citizens. Legislation without new authorities to address our nation’s critical infrastructure vulnerabilities, or legislation that would sacrifice the privacy of our citizens in the name of security, will not meet our nation's urgent needs.”

“The Obama administration opposes CISPA,” Alec Ross, a senior adviser for innovation to Hillary Clinton, told the [Guardian](#). “The president has called for comprehensive cybersecurity legislation. There is absolutely a need for comprehensive cybersecurity legislation.”

On April 25, the Administration released a statement:

“Legislation should address core critical infrastructure vulnerabilities without sacrificing the fundamental values of privacy and civil liberties for our citizens, especially at a time our Nation is facing challenges to our economic well-being and national security. The Administration looks forward to continuing to engage with the Congress in a bipartisan, bicameral fashion to enact cybersecurity legislation to address these critical issues. However, for the reasons stated herein, if H.R. 3523 were presented to the President, his senior advisors would recommend that he veto the bill.”

Cost to Taxpayers: [CBO](#) estimates that implementing the bill would have a discretionary cost of \$15 million over the 2012-2016 period, subject to appropriation. Additional personnel would be needed to administer the program, costing approximately \$3 million annually over the 2012-2016 period. The CBO costs of the intergovernmental and private sector mandates are estimated to fall below the threshold for intergovernmental (\$142 million in 2011) and private-sector mandates (\$71 million in 2011).

Does the Bill Expand the Size and Scope of the Federal Government?: This legislation would expand the role of the federal government by providing a new venue for federal involvement in domestic, private sector, cybersecurity. The federal government already protects government entities, but expanding their capacity to a new role with the private sector is an expansion of federal power. However, many would argue that this is an appropriate role for the federal government.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates?: Yes. The [CBO](#) states: “The bill would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), by extending civil and criminal liability protection to entities and cybersecurity providers that share or use cyberthreat information. The bill also would impose additional intergovernmental mandates by preempting state laws.”

Does the Bill Comply with House Rules Regarding Earmarks/Limited Tax Benefits/Limited Tariff Benefits?: According to [House Report 112-445](#): “Pursuant to clause 9 of rule XXI of the Rules of the House of Representatives, the Committee states that the bill as reported contains no congressional earmarks, limited tax benefits, or limited tariff benefits.”

Constitutional Authority: According to Rep. Rogers’s [statement](#): “The intelligence and intelligence-related activities of the United States government are carried out to support the national security interests of the United States. Article I, section 8 of the Constitution of the United States provides, in pertinent part, that ‘Congress shall have power . . . to pay the debts and provide for the common defense and general welfare of the United States’; and ‘To make all laws which shall be necessary and proper for carrying into Execution the foregoing Powers and all other Powers vested in this Constitution in the Government of the United States, or in any Department or Officer thereof.’”

RSC Staff Contact: Derek S. Khanna, Derek.Khanna@mail.house.gov, (202) 226-0718