

Myths and Facts about the Cyber Intelligence Sharing and Protection Act (CISPA)

MYTH: The cyber threat is being exaggerated.

FACT: Cyber attacks are a huge threat to American lives, national security, and the economy. In the past year alone, cyber attacks have hit vital resources, financial services, government agencies, media companies, and untold numbers of private sector businesses. The potential harm to our national security cannot be underestimated. Billions of dollars in intellectual property and trade secrets – and jobs – have been stolen from the United States. Current law does not permit the information sharing necessary to protect America from cyber threats.

MYTH: CISPA militarizes the internet and cyber security and creates new authorities for the government to collect personal information on Americans.

FACT: The Cyber Intelligence Sharing and Protection Act, known as CISPA, does not allow the military, including the National Security Agency (NSA), to collect any personal information about Americans. In fact, the legislation strictly prohibits any expansion of any agency's (including the NSA's) current authorities.

During our April 2013 markup, we added an important amendment that requires the government to eliminate any personal information it happens to receive that is not necessary to understand the cyber threat. This is also known as “minimization” of personally identifiable information, or PII.

The bill allows the government to give private industry cyber threat intelligence so they can use this information to protect their networks. Companies can then voluntarily share cyber threat information with the government. In effect, CISPA allows companies voluntarily to place a cyber 911 call to the government after they've been hacked. Like a 911 call for a robbery or fire, this call allows the government to respond quickly to a cyber attack and to prevent it from spreading. The information shared is primarily code language (zeroes and ones), and not personal information. This information is helpful to prevent future cyber attacks and determine where the cyber attack originated.

The bill does not dictate which government agency with which a company shares its information. It gives companies the flexibility to go to the government agency with which a company is most comfortable, or with which it already has a pre-existing relationship. If a bank would like to share information with the Treasury Department, it is allowed to do that. If a defense company is comfortable sharing with NSA, it is allowed to do that, as well.

MYTH: CISPA creates a wide-ranging government surveillance program.

FACT: CISPA has nothing to do with government surveillance. It simply provides narrow authority to share anonymous cyber threat information between the government and the private sector so they can protect their networks and their customers' private information. CISPA does not authorize the government to monitor private networks or communications, including emails, Facebook posts, and Tweets. The bill does not require anyone to provide information to or receive information from the government. All private sector cybersecurity sharing activities are completely voluntary.

MYTH: Cyber programs are better housed ONLY at a civilian agency. Programs housed under non-civilian agencies are not subject to any meaningful public oversight.

FACT: Both non-civilian agencies, such as the NSA, and civilian agencies, like the Department of Homeland Security (DHS), have the capacity to ensure accountability and rigorous internal and external oversight. For example, not only does the NSA have an internal Compliance Department and an Inspector General, but it is also accountable to external oversight by the Office of the Director of National Intelligence (ODNI), Department of Defense (DoD), Department of Justice (DoJ) and the White House. NSA also must report to congressional oversight committees, including the House and Senate Intelligence Committees. Extensive processes are already in place at the NSA to thoroughly scrub and permanently purge personal information.

MYTH: CISPA requires that all cyber security incidents impacting domestic internet users merit a military response.

FACT: There is nothing in the bill requiring a military response. The bill is about information sharing. Under CISPA, the private sector may place the cyber 911 call to whichever agency they choose.

MYTH: There is no oversight of or accountability for this cyber intelligence sharing regime.

FACT: That is not true. There is rigorous oversight built into CISPA. The bill requires the Intelligence Community's Inspector General annually to review and report on the government's handling and use of information that has been shared by the private sector under this bill to prevent and remedy any instances of abuse.

During our markup, we added an amendment that expanded our privacy protections and oversight requirements by adding an extra layer of review by the Privacy and Civil Liberties Oversight Board and requiring senior privacy officials from the government agencies to complete annual reviews evaluating the cyber threat information sharing regime's effect on privacy.

The bill also provides that the government shall be liable to an adversely-affected person for intentional or willful violations with respect to disclosure, use, or protection of voluntarily-shared cyber threat information and provides for damages for such violations.

MYTH: Congress drafted CISPA based on input only from federal government agencies and industry groups.

FACT: Not at all. The key bipartisan sponsors of the legislation have met a number of times with various groups, including key representatives from the business community, privacy and civil liberties groups and the Administration to address questions and concerns. These meetings will continue as the bill is marked up and heads to the House floor. In fact, multiple amendments were made based on input from privacy and civil liberties groups. In addition, at the urging of the privacy community, CISPA includes strong use limitations to restrict how the government may share, retain, and use any data voluntarily provided by the private sector.

MYTH: The White House's Executive Order, "Improving Critical Infrastructure Cybersecurity" solves our cyber threat problem.

FACT: The Administration's Executive Order (E.O.) -- named "Improving Critical Infrastructure Cybersecurity" -- is an important step toward protecting our nation from cyber attacks. The E.O. creates a partnership between the U.S. Government and critical infrastructure owners and operators to improve cybersecurity with information sharing. The E.O. also incorporates privacy requirements, which are a very important component of any cybersecurity authority.

However, an E.O. cannot do certain crucial things that only legislation can do. Only legislation can provide liability protections for industry, and only legislation can ensure that federal cybersecurity laws do not create conflicts with state and local laws.

The E.O. enables critical infrastructure to share cyber threat information that targets the U.S. homeland. This is a great start. But it is only one piece of the information sharing that we need for full cybersecurity protection of public and private entities.

MYTH: The definition of "cyber threat information" in the bill is too broad.

FACT: 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.

The bill limits "cyber threat information" to a vulnerability of a system or network, a threat to the integrity, confidentiality or availability of such a system or network, or efforts to deny access or to gain unauthorized access to a system or network.

The definition also excludes information pertaining to efforts to gain unauthorized access to a system or network of a government or private entity that solely involve violations of consumer terms of service or consumer licensing agreements, and do not otherwise constitute unauthorized access.

The bill would require the federal government to notify an entity voluntarily sharing cyber threat information with the government if the government determines that the shared information is not in fact cyber threat information.

MYTH: The bill permits the government to use any information that is voluntarily shared by the private sector to read private emails and other private information.

FACT: To the contrary, CISP A limits the government’s use of cyber intelligence information to very narrow areas.

During our markup, we limited the government’s permissible uses for cyber threat information by eliminating the national security use exception. The government now cannot retain or use a company’s cyber threat information for anything other than cyber security purposes, investigating and prosecuting cybersecurity crimes, protection of minors, and protection of individuals from bodily harm.

In addition, CISP A also would require the government to notify an entity if the government determines that the entity voluntarily shared information is not one of the uses listed above.

Finally, the cyber intelligence information as defined in the bill covers information that is primarily made up of numerical code and threat signatures – just 1’s and 0’s.

MYTH: The government will amass countless amounts of data on U.S. citizens which will sit on government computer servers.

FACT: The bill prohibits the federal government from retaining or using information other than for the cyber threat purposes specified in the legislation. CISP A specifically prohibits the Federal Government from using library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, and medical records.

CISP A provides that the federal government shall be liable for improperly using any information shared under this bill, permitting recovery of damages, costs, and fees.

As discussed above, the bill also requires the government to “minimize” and eliminate any and all personal information that happens to be shared along with cyber threat information – likely a rare occurrence, but we have provided measures to ensure personal privacy interests are protected, even in the remote instance that it is shared.

MYTH: CISPA is just another form of the Foreign Intelligence Surveillance Act (FISA), except that CISPA does not require court orders to share information on Americans.

FACT: CISPA and FISA are entirely separate legislative provisions, with completely separate security goals.

CISPA is an information sharing bill. It simply allows the government to warn private industry of a cyber threat. It also allows companies to voluntarily call in a cyber attack or cyber threat to the government. FISA is a bill to gather foreign intelligence on foreign powers and their agents who are engaged in terrorism activities. FISA requires a probable cause finding by a federal judge before any information can be collected on a United States person who is an agent of a foreign power, no matter where that person is located.

MYTH: CISPA is another form of the Stop Online Privacy Act (SOPA)/Protect IP Act (PIPA).

FACT: CISPA and SOPA/PIPA are also entirely separate legislative provisions, and they are unrelated. SOPA/PIPA was about copyright infringement. As described above, CISPA is a cyber threat information sharing bill that is narrowly focused to protect America's computer networks against cyber attacks.

MYTH: CISPA would exempt cybersecurity information sharing from all privacy laws and reverse decades of statutory protections for sensitive information like our communication, financial, and internet information. Companies would then be free to use Americans' sensitive private information as they see fit, and the government could use it for certain reasons other than cybersecurity.

FACT: CISPA provides legal protections for companies only if they act in good faith to share cyber threat information, which should rarely—if ever—include private information. Decisions made on the basis of cyber threat information also must be made in good faith.

During our markup, we also adopted an amendment that limited the private sector's permissible uses for cyber threat information. Now, companies can use cyber threat information received from other private sector entities only for cyber security purposes.

The information shared with the government, in turn, can be used only in very narrow circumstances: to prevent death or serious bodily harm; to protect minors from child pornography and sexual exploitation, and to investigate or prosecute cybersecurity crimes.

It is also important to note that by helping prevent cyber intrusions and attacks, CISPA protects privacy as much as it protects financial and proprietary information. Every day, the companies and agencies with our most private information are being attacked.