



Myth v. Fact: Cyber Intelligence Sharing and Protection Act of 2013 (CISPA)

MYTH:

This legislation creates a wide-ranging government surveillance program.

FACT:

- ✓ The bill has nothing to do with government surveillance; rather 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.
- ✓ The bill does not require anyone to provide information to or receive information from the government. The entire program would be voluntary.
- ✓ The bill creates no new authorities for the government to monitor private networks or communications.

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 defines "cyber threat information" as a vulnerability of a system or network, a threat to the integrity, confidentiality or availability of such a system or network, or efforts to gain unauthorized access to the 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 or 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 surveillance for law enforcement or other purposes by the government once the information is voluntarily shared by the private sector.

FACT:

- ✓ The definition of a “protected entity” excludes individuals, preventing an Internet Service Provider from sharing information about one of its individual customers.
- ✓ 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 and the information shared with the government is narrowly restricted to a small number of uses: (1) cybersecurity; (2) investigation and prosecution of cybersecurity crimes; (3) protection of individuals from the danger of death or physical injury; (4) protection of minors from physical or psychological harm such as child pornography; and (5) protection of the national security of the United States.

MYTH:

The bill will allow the federal government unfettered access to read private emails without a warrant.

FACT:

- ✓ The highly rapid and automated nature of cyber threat information sharing already lessens the concern that an individual’s private information is being read or mined by someone. Private sector companies protect their networks by scanning their traffic with high-speed automated systems—often without any human involvement—looking for specific digital patterns of malware and vulnerabilities. The overwhelming majority of traffic is ignored by these systems, which only alert on problems or abnormalities.
- ✓ The government can only use and retain information for five purposes: (1) cybersecurity; (2) investigation and prosecution of cybersecurity crimes; (3) protection of individuals from the danger of death or physical injury; (4) protection of minors from physical or psychological harm; and (5) protection of the national security of the United States.

- ✓ The bill provides clear authority to the Federal Government to undertake reasonable efforts to limit the impact on privacy and civil liberties in the act of sharing the cyber threat information.

MYTH:

There is no oversight of or accountability for this new program.

FACT:

- ✓ The bill requires the Intelligence Community's Inspector General to annually 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.
- ✓ The bill 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:

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 purposes specified in the legislation.