Myth v. Fact: H.R. 624, The Cyber Intelligence Sharing and Protection Act (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.

  From H.R. 624, Page 11, Line 1 the government can only use cyber threat information for*: "cybersecurity purposes; the investigation and prosecution of cybersecurity crimes; the protection of individuals from the danger of death or serious bodily harm and the investigation and prosecution of crimes involving such danger of death or serious bodily harm; or for the protection of minors from child pornography, any risk of sexual exploitation, and serious threats to the physical safety of minors, including kidnapping and trafficking and the investigation and prosecution of crimes involving child pornography, any risk of sexual exploitation, and serious threats to the physical safety of minors, including kidnapping and trafficking, and any crime referred to in section 2258A(a)(2) of title 18, United States 19 Code."*

- ✓ The bill does not require anyone to provide information to or receive information from the government. The entire program would be voluntary.

  Page 12, Line 1: *''ANTI-TASKING RESTRICTION.—Nothing in this section shall be construed to permit the Federal Government to (A) require a private-sector entity or utility to share information with the Federal Government; or (B) condition the sharing of cyber threat intelligence with a private-sector entity or utility on the provision of cyber threat information to the Federal Government."*

- ✓ The bill creates no new authorities for the government to monitor private networks or communications.

  Page 21, Line 9: *"(4) LIMITATION ON FEDERAL GOVERNMENT USE OF CYBERSECURITY SYSTEMS.—Nothing in this section shall be construed to provide additional authority to, or modify an existing authority of, any entity to use a cybersecurity system owned or controlled by the Federal Government on a private-sector system or network to protect such private-sector system or network."*

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.

  Page 23, Line 2: ''*(A) IN GENERAL.—The term 'cyber threat information' means information directly pertaining to— ''(i) a vulnerability of a system or network of a government or private entity or utility; ''(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network; ''(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or ''(iv) efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity or utility."*

MYTH:

The bill would allow the government to obtain tax, medical, library or gun records.

FACT:

On Page 12 the bill states that under CISPA the government may not obtain: library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records.

MYTH:

The bill will allow the federal government unfettered access to read private emails or read Internet history 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 operating at network speed—largely 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 cyber threat information, not private email or Internet histories, for four 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.

- ✓ The bill requires the government to establish minimization procedures to limit the receipt, retention and use of personally identifiable information not necessary to protect systems or networks.

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 creates a role for the Privacy and Civil Liberties Board (PCLOB) and the individual agency privacy officers to provide additional oversight of the government's use of information received from the private sector under this bill.

- ✓ 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:

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.

- ✓ The bill requires the government to establish minimization procedures to limit the receipt, retention and use of personally identifiable information not necessary to protect systems or networks.

MYTH:

There is no redress against the government if the government mishandles an individual's private information.

FACT:

- ✓ The bill establishes liability if the government violates restrictions on use, disclosure or retention of information.

Page 16, Line 1: *''(d) FEDERAL GOVERNMENT LIABILITY FOR VIOLATIONS OF RESTRICTIONS ON THE DISCLOSURE, USE, AND PROTECTION OF VOLUNTARILY SHARED INFORMATION.—''(1) IN GENERAL.—If a department or agency of the Federal Government intentionally or willfully violates subsection (b)(3)(D) or subsection (c) with respect to the disclosure, use, or protection of voluntarily shared cyber threat information shared under this section, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—(A) the actual damages sustained by the person as a result of the violation or $1,000, whichever is greater; and (B) the costs of the action together with reasonable attorney fees as determined by the court. (2) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—(A) the district in which the complainant resides; (B) the district in which the principal place of business of the complainant is located;*

(C) the district in which the department or agency of the Federal Government that disclosed the information is located; or (D) the District of Columbia. (3) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such action is commenced not later than two years after the date of the violation of subsection (b)(3)(D) or subsection (c) that is the basis for the action.(4) EXCLUSIVE CAUSE OF ACTION.—A cause of action under this subsection shall be the exclusive means available to a complainant seeking a remedy for a violation of subsection (b)(3)(D) or subsection (c).”

MYTH:

The private sector will be able to share individuals’ private information under this bill or can use it for marketing purposes.

FACT:

- ✓ The bill only allows the private sector to share information that relates directly to a cyber security purpose and they can only share cyber threat information.

- ✓ Cyber threat information is specifically defined in the bill starting on Page 23, Line 2 (listed above).

MYTH:

CISPA would nullify private contracts.

FACT:

- ✓ First, and most importantly, **nothing** in the bill voids private contracts, explicitly or implicitly, and private sector participation is entirely **voluntary**. Private contracts may always provide obligations beyond what is required by statutory law and those obligations are binding and may be enforced in a legal action for breach of contract. Nothing in the bill alters this basic principle of law, either. In fact, the bill also requires express consent of a “protected entity” to share information.

- ✓ More specifically, the immunity in the bill is narrow and does not alter private contractual agreements, including user agreements with service providers. Found on Page 8, starting on Line 19: *(4) EXEMPTION FROM LIABILITY.—EXEMPTION.—No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of an entity, self-protected entity, or cybersecurity provider, acting in good faith—(i) for using cybersecurity systems to identify or obtain cyber threat information or for sharing such information in accordance with this section; or (ii) for decisions made for cybersecurity purposes and based on cyber threat information identified, obtained, or shared under this section.* A cause of action for **breach of contract** is not a cause of action for use of cybersecurity systems or decisions made for cybersecurity purposes. It is a cause of action for a breach of a private contract that can provide additional protections and obligations not required by statutory law such as the framework provided in the bill. Nothing in the immunity provision changes that.

  Further, for the same reason, the “notwithstanding any other provision of law” clause contained in the bill does not operate to void private contracts for the same basic contractual principles – a cause of action for breach of contract is rooted in that private contractual obligation, and **not** the statutory law that this clause refers to.

- ✓ It is also important to emphasize that the immunity in the bill applies **only** when companies are acting in good faith. Page 9, Line 11: *''(B) LACK OF GOOD FAITH.—For purposes of the exemption from liability under subparagraph (A), a lack of good faith includes any act or omission taken with intent to injure, defraud, or otherwise endanger any individual, government entity, private entity, or utility."* Violation of a private contract certainly would bear on the question of whether a company had acted in good faith under this provision.

- ✓ Finally, the ONLY information that can be shared is cyber threat information, defined on Page 23, Line 2: ''*(A) IN GENERAL.—The term 'cyber threat information' means information directly pertaining to—''(i) a vulnerability of a system or network of a government or private entity or utility; ''(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network; ''(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or ''(iv) efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity or utility."* Nothing in this definition allows sharing of **any** information that is not within this narrow definition and for cybersecurity purposes.