Myth v. Fact: The Protecting Cyber Networks Act (H.R. 1560)

MYTH:

This legislation creates a government surveillance program.

FACT:

- ✓ The bill has nothing to do with government surveillance; rather, it provides narrow authority for the government and the private sector to share anonymous cyber threat information so companies can better protect their networks and their customers' private information from hackers and other bad actors.

- ✓ The bill expressly does not give authority to companies to send information directly to the NSA or the military.

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

- ✓ The bill also expressly states that it creates no new government surveillance authorities.

MYTH:

The definition of "cyber threat indicators" in the bill is too broad.

FACT:

- ✓ Under the bill a company may only identify and share cyber threat indicators for "cybersecurity purposes"; that is, only when they are seeking to protect their own systems or networks.

- ✓ The bill's definition of 'cyber threat indictor' includes only technical data like malicious reconnaissance, malware signatures, and security vulnerabilities, not sensitive personal information

- ✓ The bill requires companies to strip out personally identifiable information (PII) not directly related to a cyber threat before sharing cyber threat indicators with the federal government. Upon receipt, the government is required to perform an additional scrub to ensure all unnecessary PII is removed.

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 bill provides no surveillance authorities. Even if a cyber threat indicator did include information relevant to a criminal investigation, law enforcement officers would still need to obtain a warrant supported by probable cause before carrying out surveillance.

- ✓ The bill narrowly restricts information shared to a small number of uses: (1) cybersecurity; (2) investigation and prosecution of a threat of death or physical injury; (3) protection of minors from physical or psychological harm such as child pornography; and (4) the investigation and prosecution of espionage and serious violent felonies like rape and kidnapping.

MYTH:

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

FACT:

- ✓ Under the bill, private companies can only share cyber threat indicators like malicious reconnaissance, malware signatures, and security vulnerabilities with the federal government—not sensitive personal information.

- ✓ In fact, the bill expressly requires companies to remove any PII that is not directly related to a cyber threat before sharing with the government.

- ✓ Even if a company accidentally shares PII with the government, the agency that receives the information must perform a second scrub to remove all unnecessary PII.

MYTH:

The bill allows companies to "hack back" against cyber threats and unleash cyber wars.

FACT:

- ✓ Companies can perform defensive measures on their own networks to protect from degradation of their infrastructure, to mitigate ongoing attacks, or to maintain service. Companies cannot

“hack back” information or otherwise manipulate networks they do not own or have no explicit authorization to protect.