Myth v. Fact: Cyber and the Omni

MYTH #1:

The conference version of the cybersecurity bill removes an express prohibition on using shared information for "surveillance" purposes.

FACT #1:

- ✓ 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 indicators so companies can better protect their networks and their customers' private information from hackers and other bad actors.

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

- ✓ The bill only allows the government to use information that companies have already provided. It does not allow the government to force companies to provide information or to obtain information without companies' permission.

MYTH #2:

The bill permits surveillance for law enforcement or other purposes by the government once the information is voluntarily shared by the private sector.

FACT #2:

- ✓ 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 new legal authorities, such as a warrant, before carrying out surveillance.

- ✓ The bill narrowly restricts information shared to a small number of uses: (1) cybersecurity; (2) investigation and prosecution of a specific threat of death, physical injury, or serious economic harm; (3) protection of minors from sexual exploitation; and (4) the investigation and prosecution of espionage and cybercrimes.

- ✓ This list of uses is narrower than a list the House passed in April with more than 300 votes. The bill also has a 10-year sunset, allowing Congress to review how the government uses cyber threat information.

MYTH #3:

The conference version removes the requirement for companies to "scrub" cyber threat indicators for personally identifiable information (PII) before sharing.

FACT #3:

- ✓ Before companies can share information with the government, the conference version requires them to review the information and remove any PII unrelated to cyber threats.

- ✓ In fact, the conference version is **stronger** than both House-passed versions because it **requires** companies to remove any information they know to be PII. The House-passed version only required companies to take "reasonable efforts" to remove PII.

MYTH #4:

The conference version of the bill removes the prohibition on information being shared with the military and NSA.

FACT #4:

- ✓ **The bill sets up the Department of Homeland Security (DHS) as the sole portal for companies to share information with the federal government.** Every bill that passed the House and Senate authorized automated sharing from DHS to the military and the National Security Agency (NSA).

- ✓ The conference bill expressly prohibits the military and NSA from hosting a portal.

- ✓ The military and NSA can receive information from the DHS portal, but only after it has received two "scrubs" for PII: one by the companies before sharing with DHS, and another by DHS before sharing with the rest of the federal government.

- ✓ The military and NSA need cyber threat information to protect defense and national security networks from our enemies.