The Protecting Cyber Networks Act

2014 will be known as the year of the cyber breach. High profile attacks are a main topic of conversation in the boardroom and at the dinner table. Every day, nation-state actors and criminals target America's businesses for cyber espionage and theft. These hackers steal our intellectual property, trade secrets and even sensitive government information. The same actors who conduct cyber espionage are also capable of significant offensive cyber attacks that could degrade or damage vital private-sector infrastructure.

The *Protecting Cyber Networks Act* enables private companies to share cyber threat indicators with each other and, on a purely voluntary basis, with the federal government but **not through the NSA or the Department of Defense**, all while providing strong protections for privacy and civil liberties. At the same time, the bill makes clear that defense contractors can continue to share cyber threat information with the Department of Defense when required to do so by another law, regulation, or contract.

Voluntary information sharing with the federal government helps improve the government's ability to protect America against foreign cyber threats. It also gives our intelligence agencies tips and leads to help them find advanced foreign cyber hackers overseas. That intelligence allows the government to provide, in turn, even better cyber threat indicators back to the private sector to help companies protect themselves.

Strong Protections for Privacy and Civil Liberties: The *Protecting Cyber Networks Act* permits only voluntary sharing by the private sector of a very limited category of information—cyber threat indicators—and permits only the sharing of such information for cybersecurity purposes, a similarly limited term. The bill also:

- Protects privacy by prohibiting the government from forcing private sector entities to provide information to the government.
- Requires companies to remove personal information before they share cyber threat indicators with the government.

- Requires the federal agency that receives cyber threat indicators to perform a second check for personal information before sharing them with other relevant federal agencies.
- Strictly limits the private-to-private sharing to only cyber threat indicators and defensive measures to combat a threat. The legislation does not allow for the sharing of information for non-cyber purposes.
- Imposes strict restrictions on the use, retention, and searching of any data voluntarily shared by the private sector with the government.
- Does not shield a company from willful misconduct in the course of sharing cyber threat indicators but provides liability protections for companies that share in good faith.
- Enforces these strong privacy and civil liberties protections by permitting individuals to sue the federal government for intentional privacy violations in federal court.
- Provides for strong public and congressional oversight by requiring a detailed biennial Inspectors General (IG) report of appropriate federal entities of the government's receipt, use, and dissemination of cyber threat indicators. The Privacy and Civil Liberties Oversight Board (PCLOB) must also submit a biennial report on the privacy and civil liberties impact of the Act.