H.R. 1560 House Floor Statement

As Prepared for Delivery by Chairman Devin Nunes

April 22, 2015

Madame Chairwoman:

Over the last several years, the threat of cyber attacks has become an urgent concern to the United States. Anthem, Home Depot, Sony, Target, JP Morgan Chase, and other companies have been subject to major attacks that have compromised the personal information of employees and customers alike.

The House has passed cybersecurity information-sharing legislation with strong majorities in the past two Congresses. Ranking Member Schiff and I have continued this bipartisan tradition, working closely together to draft a bill that will increase the security of our networks while protecting users' privacy. We have also worked closely with Leadership, Chairman McCaul, Chairman Goodlatte, and the Senate Intelligence Committee to ensure that our bills complement each other.

The Protecting Cyber Networks Act addresses a core problem in our digital security infrastructure: because of legal ambiguities, many companies are afraid to share information about cyber threats with each other or with the government. If a company sees some threat or attack, this bill will allow it to quickly report the intrusion without fearing a lawsuit, so that other companies can take measures to guard against the threat.

The bill, which is 100 percent voluntary, encourages three kinds of sharing: private-to-private; government-to-private; and private-to-government. In that third scenario, the bill will allow companies to share cyber threat information with a variety of government agencies. If banks are comfortable sharing with the Treasury Department, they can share with Treasury; if utilities prefer sharing with the Department of Energy, they can share with Energy; if companies want to share with DHS, the Justice Department, or the Commerce Department, they can share with them. The only sharing that the bill does not encourage is direct sharing to DOD and

NSA. Companies can still share with DOD and NSA, they just do not receive any new liability protections.

This bill does not provide the government with any new surveillance authorities. To the contrary, it includes robust privacy protections. It only authorizes the sharing of cyber threat indicators and defensive measures—technical information like malware signatures and malicious code. In fact, before companies share with the federal government, they must remove all personal information that might be attached to cyber threats. If companies don't follow those requirements, they will not receive liability protection.

Furthermore, the government agency that receives the information must scrub it a second time to ensure all personal information has been removed. Only then can it forward the information to other federal agencies.

Finally, the bill 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.

The increasing pace and scope of cyber attacks cannot be ignored. This bill will strengthen our digital defenses so that American consumers and businesses will not be put at the mercy of malevolent cyber thieves. I look forward to passing this legislation. Thank you.