

The National Cybersecurity Protection Advancement Act

2015

THE PROBLEM

Every day, cyber espionage is being conducted against our government and U.S. businesses, the intellectual property of American companies is being stolen, and the personal information of Americans is being hacked by criminals, hacktivists and nation states.

The hacks on the State Department and White House, health insurer Anthem, Sony Pictures and Target are only the most recent examples of this growing threat. To defend America's vital digital networks the public and private sector must work together.

The Department of Homeland Security's (DHS) center for integrating cyber threat information is the National Cybersecurity and Communications Integration Center (NCCIC) – a civilian interface for private, federal, state and local entities to share cyber threat information.

Unfortunately, in the current environment, companies do not feel they have adequate legal protections to share cyber threat indicators with the NCCIC. Industry needs a "safe harbor" where legal barriers are removed, appropriate privacy protections are in place, and companies are incentivized to be a full NCCIC participant.

THE SOLUTION

H.R. 1731, the National Cybersecurity Protection Advancement (NCPA) Act, is a **bipartisan** bill passed unanimously by the Committee on Homeland Security. This **pro-privacy, pro-security** bill ensures the sharing of cyber threats is **transparent and timely**.

It strengthens the NCCIC's role as the lead civilian interface for cyber threat information sharing by:

- Providing **liability protections for the voluntary sharing** of cyber threat indicators and defensive measures with the NCCIC or private-to-private.
- Granting liability protections for private companies to conduct network awareness of their own information systems.
- Allowing companies to operate defensive measures and conduct network awareness on information systems they own or operate.

The NCPA Act also ensures personal information is removed before sharing cyber threat indicators and that strong safeguards are in place to **protect the privacy and civil liberties** of all Americans.

It bolsters the **robust privacy protections** already in place at DHS without risking exposure of personal data by:

- Enhancing DHS's already robust Privacy Office to ensure the NCCIC complies with all civilian laws that protect Americans' privacy and civil liberties.
- Requiring private companies to **'scrub' and remove personal information** unrelated to the cybersecurity risk before sharing with the NCCIC or other private entities.
- Requiring the NCCIC to conduct a second 'scrub' and destroy any personal information that is unrelated to the cybersecurity risk before further sharing with other government entities or private entities.

The NCPA Act designates the NCCIC as the lead civilian interface. Accordingly, the NCCIC only uses the information it receives **solely to prevent and respond to cyber attacks**, and enhance our nation's cyber defenses – it cannot be used for any law enforcement or surveillance purposes.

The NCPA Act also **preserves existing public-private partnerships** to ensure ongoing collaboration on cybersecurity.

The NCPA Act will increase what we know about cyber threats and, in doing so, will enhance American security while protecting Americans' privacy and civil liberties. **Now is the time for Congress to act.**

Updated 04-15-15