Committee on
HOMELAND SECURITY
Chairman Michael McCaul

"National Cybersecurity and Critical Infrastructure Protection Act of 2013" (NCCIP Act)

The cybersecurity threat to our nation is real, evolving and imminent. At a recent Congressional hearing, FBI Director James Comey said that "we anticipate that in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats."[1] Our adversaries, including China, Iran and Russia are relentlessly looking for ways to exploit American digital networks to disrupt and destroy our nation's critical infrastructure and steal intellectual property for financial gain. The *"National Cybersecurity and Critical Infrastructure Protection Act of 2013"* (NCCIP Act) will strengthen our nation's efforts to protect the homeland from a cyber attack on our critical infrastructure while prohibiting any new regulations at the Department of Homeland Security (DHS).

Specifically, the NCCIP Act:

- Prohibits new regulatory authority at DHS and is budget neutral;
- Codifies and strengthens the National Cybersecurity and Communications Integration Center (NCCIC), a federal civilian, transparent interface to facilitate real-time cyber threat information sharing across critical infrastructure sectors;
- Establishes an equal partnership between private industry and DHS, and ensures that DHS properly recognizes industry-led entities to facilitate critical infrastructure protection and incident response;
- Codifies and strengthens the successful aspects of the National Infrastructure Protection Plan (NIPP), a public-private partnership framework that has been supported by the private sector since 2003;
- Codifies the Cyber Incident Response Teams to provide timely technical assistance, crisis management, and actionable recommendations on cyber threats to critical infrastructure owners and operators on a voluntary basis;
- Ensures that the National Cybersecurity Incident Response Plan is regularly updated and exercised in coordination with federal, state, local, and private sector stakeholders;
- Codifies DHS operational information security activities to protect and ensure the integrity and resiliency of all federal civilian information systems and networks (.gov); and
- Amends the SAFETY Act to establish a threshold for qualifying cyber incidents so private entities can voluntarily submit their cybersecurity procedures to the SAFETY Act Office to gain additional liability protections in the event of a qualifying cyber incident.

[1] Comey, James. Statement before the Senate Committee on Homeland Security and Governmental Affairs. November 14, 2013. http://www.fbi.gov/news/testimony/homeland-threats-and-the-fbis-response