Opening Statement of the Honorable Fred Upton
Committee on Energy and Commerce
Hearing on "Cyber Threats and Security Solutions"
May 21, 2013

(As Prepared for Delivery)

Today's hearing continues the Energy & Commerce Committee's oversight of a topic of great national significance – cybersecurity. The committee continues to closely monitor the cybersecurity protection and mitigation efforts of those vital sectors within the committee's jurisdiction, including oil and gas pipelines, the electric grid, nuclear energy, chemical facilities, sewer and water, and telecommunications.

As the nation becomes more reliant on digital communications technology, we also increase our exposure to cyber threats. Indeed, cyber risks to our nation's critical infrastructure have increased significantly in recent years, including multiple high-profile cyber incidents that have confirmed the steady rise in cyber-attacks.

But combatting such threats requires a cybersecurity regime that provides ample flexibility to afford owners and operators of critical infrastructure the ability to protect against and respond to rapidly evolving threats. A one-size-fits-all approach to cybersecurity is ill-suited for the diverse range of critical infrastructure sectors, each of which has its own complex characteristics. Owners and operators know best how to protect their own systems, and it is nearly impossible for the speed of bureaucracy to keep pace with ever changing threats.

Undertaking certain reasonable actions in the short-term can have a marked improvement in protecting critical assets. These actions include enhanced information sharing between the federal government and the private sector, greater emphasis on public-private partnerships, and improved cross-sector collaboration. Regarding information sharing, we continue to support Intelligence Committee Chairman Rogers's legislation, which passed the House last month.

I believe that the best approach to improving cybersecurity is for existing regulators to work with industry stakeholders, and for robust information sharing between government and stakeholders. In contrast, I continue to be skeptical of continued calls for a top-down, command-and-control regulatory approach centralized at the Department of Homeland Security or any other federal agency. Along those lines, the committee will continue to monitor with great interest implementation of the President's Executive Order on cybersecurity.

###