THE CYBERSECURITY ACT OF 2012

The bipartisan *Cybersecurity Act of 2012* was developed in response to the ever-increasing number of cyber attacks on both private companies and the United States government. As the country increasingly relies upon the Internet to conduct business, the critical services upon which we rely have become increasingly vulnerable to cyber threats. The country's most critical infrastructure can now be manipulated or attacked by malicious actors using computers halfway across the globe. The destruction or exploitation of critical infrastructure through a cyber attack, whether a nuclear power plant, a region's water supply, or a major financial market, could devastate the American economy, our national security, and our way of life. Defense and intelligence leaders have called malicious cyber actors an "existential threat" to our country.

Working closely with Senate leadership, the *Cybersecurity Act of 2012* is a joint effort by leaders and senior members of the Senate Committees on Commerce, Homeland Security and Governmental Affairs, and Intelligence to give the federal government and the private sector the tools necessary to protect our most critical infrastructure from growing cyber threats. The bill is a combination of legislation passed by the Commerce and Homeland Security Committees, and it incorporates extensive input from companies and trade associations representing a large swath of the private sector, including the information technology, financial services, telecommunications, chemical, and energy sectors. Other Members of Congress, national security, privacy and civil liberties experts, and government agencies have also provided important input.

To ensure the federal government and the private sector take the necessary steps to secure our nation, the *Cybersecurity Act of 2012* would do the following:

Determine the Greatest Cyber Vulnerabilities. The bill would require the Secretary of Homeland Security, in consultation with the private sector, the Intelligence Community, and others, to conduct risk assessments to determine which sectors are subject to the greatest and most immediate cyber risks.

Protect Our Most Critical Infrastructure. The bill would authorize the Secretary of Homeland Security, with the private sector, to determine cybersecurity performance requirements based upon the risk assessments. The performance requirements would cover critical infrastructure systems and assets whose disruption could result in severe degradation of national security, catastrophic economic damage, or the interruption of life-sustaining services sufficient to cause mass casualties or mass evacuations. The bill would only cover the most critical systems and assets in a given sector, and only if they are not already being appropriately secured.

Protect and Promote Innovation. Owners of "covered critical infrastructure" would have the flexibility to meet the cybersecurity performance requirements in the manner they deem appropriate. The private sector also would have the opportunity to develop and propose performance requirements for “covered critical infrastructure.” The bill would prohibit the government from regulating the design or development of information technology products.

Improve Information Sharing While Protecting Privacy and Civil Liberties. As the sophistication of cyber threats and attacks has grown, it is increasingly clear that improved information sharing is a vital tool to combat cyber crime and espionage, and to alert owners of our nation’s most critical infrastructure of cyber threats to their systems and assets. Both the government and the private sector collect valuable cyber threat information. This bill would provide a responsible framework for the sharing of cyber threat information between the federal government and the private sector, and within the private sector, while ensuring appropriate measures and oversight to protect privacy and preserve civil liberties.

Improve the Security of the Federal Government’s Networks. To strengthen the security and resilience of federal government systems, the bill would amend the Federal Information Security Management Act (FISMA) and require the federal government to develop a comprehensive acquisition risk management strategy. The amendments to FISMA would move agencies away from a culture of compliance to a culture of security by giving the Department of Homeland Security authority to streamline agency reporting requirements and reduce paperwork through continuous monitoring and risk assessment. The bill would emphasize “red team” exercises and operational testing to ensure federal agencies are aware of their networks’ vulnerabilities. By directing OMB to develop security requirements and best practices for federal IT contracts, the bill would also ensure agencies make informed decisions when purchasing IT products and services.

Clarify the Roles of Federal Agencies. The bill would clarify and improve federal efforts to address cyber threats. The bill would strengthen the critical partnership between the Department of Defense and the Department of Homeland Security. It would consolidate existing cyber offices at the Department of Homeland Security into a unified National Center for Cybersecurity and Communications to carry out the Department’s current responsibilities for protecting the networks of federal civilian agencies and critical infrastructure. Existing relationships between infrastructure owners and government agencies, as well as existing oversight frameworks, would remain intact, wherever possible, to avoid duplication.

Strengthen the Cybersecurity Workforce. The bill would reform the way cybersecurity personnel are recruited, hired, and trained to ensure that the federal government has the necessary talent to lead and manage the protection of its own networks.

Coordinate Cybersecurity Research and Development. The bill would provide for a coordinated cybersecurity R&D program to advance the development of new technologies to secure our nation from ever-evolving cyber threats.