THE REVISED CYBERSECURITY ACT OF 2012
S. 3414, (introduced July 19, 2012)

The revised bipartisan *Cybersecurity Act of 2012 or "CSA2012"* was developed in response to what defense and intelligence leaders have called an "existential threat" to our country. Our critical infrastructure is increasingly vulnerable to cyber threats, and can be manipulated or attacked by faceless individuals using computers halfway around 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 cripple our economy, our national security, and the American way of life. We must act now.

To address this threat, this revised legislation would establish a robust public-private partnership to improve the cybersecurity of our nation's most critical infrastructure, which is mostly owned by the private sector. Industry would develop voluntary cybersecurity practices and a multi-agency Government council would ensure these practices are adequate to secure systems from attacks. Private owners who choose to participate in the voluntary cybersecurity program established by the legislation would receive various benefits. While it promotes the sharing of cyber threat information, this legislation also ensures that privacies and civil liberties are protected.

The revised *Cybersecurity Act of 2012* would do the following:

Determine the Greatest Cyber Vulnerabilities: The bill would establish the National Cybersecurity Council, an interagency body with members from the Departments of Defense, Justice, Commerce, the Intelligence Community, appropriate sector-specific Federal agencies, appropriate Federal agencies with responsibilities for regulating the security of covered critical infrastructure, and chaired by the Department of Homeland Security. This Council would conduct risk assessments to determine which sectors are subject to the greatest and most immediate cyber risk and would identify particular categories of critical infrastructure as critical cyber infrastructure. This Council can only identify categories of infrastructure as critical cyber infrastructure if a cyber attack to that infrastructure could reasonably result in catastrophic consequences such as interruption of life-sustaining services sufficient to cause a mass casualty event or mass evacuations, catastrophic economic damage to the United States, or severe degradation of national security. The Council would identify owners of such critical cyber infrastructure, who would report significant cybersecurity events to help improve our national security against those attacks.

Create a Public-Private Partnership to Combat Cyber Threats. The bill provides that industry led groups will develop and propose to the Council voluntary outcome-based cybersecurity practices. The Council will review such proposals and adopt them, or modify or supplement as necessary to ensure the identified risks are mitigated by the cybersecurity practices. The cybersecurity practices could not prescribe specific products, nor products' design or development. The bill creates no new regulators, and provides no new authority for an agency to establish standards that are not otherwise authorized by law.

Incentivize the Adoption of Voluntary Cybersecurity Practices. Owners of critical infrastructure could choose to participate in a voluntary cybersecurity program. Participating owners are given complete flexibility to meet the cybersecurity practices in any manner they choose. Owners then have the choice of showing they are meeting the cybersecurity practices and thus being admitted to the program either by self-certification or obtaining a third party assessment. Those that join the program would be entitled to benefits such as liability protection from any punitive damages arising from an incident related to a cybersecurity risk where the owner is in substantial compliance with the cybersecurity practices at the time of the incident; expedited provision of security clearances to appropriate personnel employed by the certified owner; priority technical assistance on cyber issues; and receipt of relevant real-time cyber threat information.

Improve Information Sharing While Protecting Privacy and Civil Liberties. Both the private sector and the government have information about cyber threats that help protect networks. This bill would authorize the government to provide security clearances to companies with a need to receive classified information to protect their networks. It would also provide a framework for private sector companies to share information about cyber threats with each other and with the federal government and provide certain liability protection for companies that do so. The information sharing procedures are designed to ensure that privacy and civil liberties are protected when information is shared under this bill.

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. The bill would consolidate existing cyber offices at the Department of Homeland Security into a unified National Center for Cybersecurity and Communications to carry out its current responsibilities.

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.