THE PROTECTING CYBERSPACE AS A NATIONAL ASSET ACT OF 2010

Homeland Security and Governmental Affairs Committee
Chairman Joe Lieberman
Ranking Member Susan Collins
Senator Thomas Carper

The Protecting Cyberspace as a National Asset Act of 2010 – introduced by Senators Lieberman, Collins, and Carper – will modernize the government's ability to safeguard the nation's cyber networks from attack and will establish a public/private partnership to set national cyber security priorities and improve national cyber security defenses.

Significant provisions of the bill include:

White House Office for Cyberspace Policy: The Act establishes an office in the Executive Office of the President, run by a Senate-confirmed Director, who will advise the President on all cybersecurity matters. The Director will lead and harmonize federal efforts to secure cyberspace and will develop a national strategy that incorporates all elements of cyberspace policy, including military, law enforcement, intelligence, and diplomatic. The Director will oversee all related federal cyberspace activities to ensure efficiency and coordination. The Director will report regularly to Congress to ensure transparency and oversight.

National Center for Cybersecurity and Communications: The Act establishes the National Center for Cybersecurity and Communications (NCCC) at the Department of Homeland Security (DHS) to elevate and strengthen the Department's cyber security capabilities and authorities. The NCCC will be led by a Senate-confirmed Director, who will report to the Secretary. The Director will regularly advise the President regarding the exercise of authorities relating to the security of federal networks. The NCCC will include the United States Computer Emergency Response Team (US-CERT), and will lead federal efforts to protect public and private sector cyber and communications networks. The NCCC will detect, prevent, analyze, and warn of cyber threats to these networks.

Protecting Critical Infrastructure: The NCCC will work with the private sector to establish risk-based security requirements that strengthen the cyber security for the nation's most critical infrastructure, such as vital components of the electric grid, telecommunications networks, and control systems in other critical infrastructure that, if disrupted, would result in a national or regional catastrophe. Owners and operators of critical infrastructure covered under the Act could choose which security measures to implement to meet these risk-based performance requirements. Covered critical infrastructure must report significant breaches to the NCCC to ensure the federal government has a complete picture of the security of these networks. The NCCC must share information, including threat analysis, with owners and operators regarding risks to their networks. The Act will provide liability protections to owners/operators that comply with the new risk-based security requirements. The NCCC will work with other federal agencies to avoid duplication of effort and to promote efficiency.

Promoting Cybersecurity: The NCCC will produce and share useful warning, analysis, and threat information with the private sector, other federal agencies, state and local governments, and international partners. The NCCC will collaborate with the private sector to develop best

practices for cyber security. By developing and promoting best practices and providing voluntary technical assistance as resources permit, the NCCC will help improve cyber security across the nation. Information the private sector shares with the NCCC will be protected from public disclosure, and private sector owners and operators may obtain security clearances to access information necessary to protect the IT networks the American people depend upon.

Protecting Against Catastrophic Attack: The Act will provide a responsible framework, developed in coordination with the private sector, for the President to authorize emergency measures, limited in both scope and duration, to protect the nation's most critical infrastructure if a cyber vulnerability is being exploited or is about to be exploited. The President must notify Congress in advance about the threat and the emergency measures that will be taken to mitigate it. Any emergency measures imposed must be the least disruptive necessary to respond to the threat. These emergency measures will expire after 30 days unless the President orders an extension. The bill does not authorize any new surveillance authorities, or permit the government to "take over" private networks.

Protection of Federal Networks: The Act will codify and strengthen DHS authorities to establish complete situational awareness for federal networks and develop tools to improve resilience of federal government systems and networks. The Act reforms the Federal Information Security Management Act (FISMA) to transition from paper-based to real-time response to threats against government systems.

Procurement Reform: The Act will require development of a comprehensive supply chain risk management strategy to address risks and threats to the information technology products and services the federal government relies upon. This strategy will allow agencies to make informed decisions when purchasing IT products and services. It will be implemented through the Federal Acquisition Regulation, requiring contracting officers to consider the security risks inherent in agency IT procurements. The bill would also require specific training for the federal acquisition workforce to enhance the security of federal networks.

Workforce Reform: The Office of Personal Management will reform the way cyber security personnel are recruited, hired, and trained to ensure that the federal government has the talent necessary to lead the national cyber security effort and protect its own networks. The Act also provides DHS with temporary hiring and pay flexibilities to assist in the quick establishment of the NCCC.