



**EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503**

July 26, 2012  
(Senate)

## **STATEMENT OF ADMINISTRATION POLICY**

**S. 3414 – Cybersecurity Act of 2012**  
(Sen. Lieberman, I-CT, and 4 cosponsors)

The Administration strongly supports Senate passage of S. 3414, the Cybersecurity Act of 2012. While lacking some of the key provisions of earlier bills, the revised legislation will provide important tools to strengthen the Nation's response to cybersecurity risks. The legislation also reflects many of the priorities included in the Administration's legislative proposal.

The Administration particularly appreciates the bill's strong protections for privacy and civil liberties and would not support amendments that weaken these protections. The Administration agrees that it is essential that the collection, use, and disclosure of such information remain closely tied to the purposes of detecting and mitigating cybersecurity threats, while still allowing law enforcement to investigate and prosecute serious crimes. All entities – public and private – must be accountable for how they handle such data. The bill should take care not to duplicate existing domestic or international law enforcement frameworks. The bill also must protect the confidentiality of statistical data and honor the statutory confidentiality pledges made to respondents. The Administration is confident that S. 3414 can improve the Nation's cybersecurity while protecting the privacy, confidentiality, and civil liberties that are central to American values.

The revised bill contains critical-infrastructure protection measures that are less robust than in earlier drafts, but would still produce meaningful cybersecurity improvements. However, the Administration would not support amendments that would weaken the critical infrastructure protection measures in the legislation, including: (1) reducing the Federal Government's existing roles and responsibilities in coordinating and endorsing the outcome-based cybersecurity practices; (2) weakening the statutory authorities of the Department of Homeland Security to accomplish its critical infrastructure protection mission; or (3) substantially expanding the narrowly-tailored liability protections for private sector entities. While liability limitations are necessary to encourage information sharing, overly broad immunities from legal obligations would undermine the very trust that the bill seeks to strengthen.

S. 3414 would create an interagency National Cybersecurity Council to coordinate the identification of voluntary cybersecurity practices for critical cyber infrastructure. As currently drafted, the structure of the National Cybersecurity Council raises constitutional concerns and should be amended to employ an administrative structure similar to that of other recently established councils. Further, the bill contains provisions purporting to prescribe the Executive branch's responsibilities in coordinating with foreign governments and conducting diplomatic negotiations. These provisions should be clarified so as to maintain the President's exclusive

constitutional authority to conduct diplomacy. The Administration also believes that to ensure consistency with existing law, processes, and Presidential directives, certain provisions must be addressed in the final bill regarding the protection of intelligence sources and methods, as well as information sharing and policy coordination.

The Administration looks forward to working with the Congress to ensure that cybersecurity legislation is sufficiently comprehensive to address the growing cyber threats facing the Nation.

\* \* \* \* \*