

June 24, 2010

The Honorable Joseph Lieberman, Chairman
The Honorable Susan Collins, Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
Senate Office Building
Washington, DC 20510

Dear Chairman Lieberman and Senator Collins:

The Internet Security Alliance (ISA) wishes to express its gratitude to you for calling attention to the severe and growing cyber security problems our nation faces by introducing S 3480 Protecting Cyberspace as a National Asset. ISA also wishes to commend Committee staff for their exhaustive efforts over the past year or more to bring the Protecting Cyberspace as a National Asset Act to where it is today.

The ISA supports approving this modified bill out of the Homeland Security Committee and looks forward to working with the Committee members and their staff as the bill continues through the legislative process.

The ISA supports the Senate Homeland Security Committee approving S 3480 for several reasons including:

- S 3480 properly targets an intensified public private process to assure the security of our most critical cyber systems. The addition in the mark-up vehicle of specified criteria for inclusion as “covered critical infrastructure” and an appellate process will provide greater assurance that government and industry will work together in a risk management framework to protect our nation’s most sensitive information systems.
- S 3480 properly refines current law with respect to the Emergency Powers the President may need to exercise in case of a true cyber emergency and adds protections for individual privacy and coordination with Congress and the Private sector
- S 3480 properly appreciates that cyber security is as much an economic and strategic issue as a technical and operational issue by focusing on promoting the most cost effective solutions for cyber security
- S 3480 properly addresses the need for improving cyber security in the broader infrastructure by creating mechanisms for the promotion of adoption of best practices for cyber security within the private sector including educational programs addressing the financial aspects of poor cyber security

That said, ISA believes there are a few remaining areas where the bill could be strengthened to ensure that it becomes an even more effective tool for protecting our strategic cyber security goals and our national security.

First, the standards and practices for critical infrastructure recognized by the federal government ought to be those developed by the private sector. While government entities such as NIST are and ought to be involved the development of international standards, they ought not to be the final judge of what is promoted.

The criteria for adoption or promotion of standards ought to simply be the effectiveness of the standards not who created them. Several independent studies have documented that standards and practices developed through the existing private sector system would, if implemented, eliminate or mitigate between 80-90% of cyber attacks, and there are proven technologies, including some certified by DHS under the SAFETY Act that can help combat the cyber threat.

Relying on the robust international private sector system to develop cyber security standards and practices will allow for much faster evolution of needed security upgrades than a centralized US federal system would, and as a result, create a more secure infrastructure. In addition, relying on the private sector system will also allow American companies to continue to innovate and compete in a world economy free of new costs and regulatory burdens applied only to American companies.

Second, the modified bill also takes positive initial steps toward establishing a system of market incentives to motivate the private sector to make security investments that may go beyond their own corporate business needs but serves broader national security interests. Among the incentives included in this bill are procurement incentives, the prospect for streamlined regulation and limited civil liability relief.

While these incentive programs are laudable, they are not currently broad enough or powerful enough to provide sufficient motivations across the expanse of companies involved in the critical infrastructure.

ISA believes much more ought to be done to stimulate the cyber insurance industry to transfer the current massive financial risk the American taxpayer faces from the prospect of a major cyber event. Greater use of cyber insurance can also motivate adoption of improved security practices by private enterprise and provide a private sector funded mechanism to monitor adoption of adequate cyber security procedures throughout the business community.

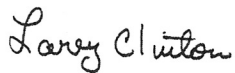
In addition, the broader liability reforms and tax incentives advocated in the Cyber Space Policy Review released by President Obama following a comprehensive review of our nation's cyber security status a last spring, need to be included in any final package to come to the floor of the Senate.

However, since Congress is not well structured to address 21st century issues such as cyber security, committee jurisdictional restrictions meant these provisions could not be included in the bill before the Homeland Security and Government Affairs Committee. ISA looks forward to hearings and mark ups in the other committees of jurisdiction including Judiciary, Intelligence,

Finance and Banking so that these items can be added prior to the bill being considered on the Senate floor.

The fact that the current bill is in need of additional refinement as it works its way through a multi-committee process does not detract from the reason for the Homeland Security Committee to approve this initial step today. S 3480 calls attention to an urgent national problem, lays out necessary programs for enhanced education training and awareness, begins to define a new relationship between the public and private sector, which will hopefully grow into a comprehensive market based incentive program that can establish the sort of incentive-based cyber security program that our nation needs. ISA is pleased to have participated in this process, congratulates the authors and Committee for its actions, and looks forward to working with the Senate, House and Administration as this process moves on to its next stages.

Sincerely,

A handwritten signature in cursive script that reads "Larry Clinton".

Larry Clinton
President & CEO
Internet Security Alliance

cc. Members and staff of Senate Commerce Committee

*The **Internet Security Alliance** is a multi-sector trade association established in collaboration with Carnegie Mellon University in 2000. ISA represents an array of organizations concerned with information security from the aviation, banking, communications, defense, education, financial services, insurance, manufacturing, security and technology sectors. The ISA mission is to combine advanced technology with the economic realities and help create effective public policy leading to a sustainable system of worldwide cyber security. ISA advocates a modernized social contract between industry and government creating market-based incentives to motivate enhanced security of cyber systems. ISA provides a range of technical, business and public policy services to its members to assist them in fulfilling their mission.*