

1150 18th Street, NW
Suite 700
Washington, DC 20036

p.202/872.5500
f.202/872.5501

July 30, 2012

The Honorable Joseph Lieberman
Chairman, Committee on Homeland
Security and Governmental Affairs
U.S. Senate Governmental Affairs

The Honorable Susan Collins
Ranking Member, Committee on
Homeland Security and
U.S. Senate

The Honorable John D. Rockefeller IV
Chairman, Committee on Commerce,
and Transportation
U.S. Senate

The Honorable Dianne Feinstein
Chairman, Select Committee on Science
Intelligence
U.S. Senate

The Honorable Thomas Carper
Chairman, Subcommittee on Federal
Financial Management, Government Information,
Federal Services, and International Security
U.S. Senate

Dear Senators Lieberman, Collins, Rockefeller, Feinstein, and Carper:

On behalf of the Business Software Alliance and its member companies, I am writing to applaud your reintroduction of the Cybersecurity Act of 2012 (S.3414). We also want to thank you and your colleagues for the strong bipartisan vote on the motion to proceed to a debate on the bill. The vote was an important signal demonstrating the Senate's commitment to tackling a complex set of issues that require careful consideration. We believe S.3414 creates a solid framework and foundation for the cybersecurity debate over the coming days.

The Business Software Alliance is the leading advocate for the global software industry. Our members operate on the front lines of the digital economy and are experts in cybersecurity. In January of this year we wrote to the Senate outlining BSA's top priorities for cybersecurity legislation. Many of these priorities are reflected in S.3414, including the need to improve real-time information sharing while meaningfully protecting privacy and civil liberties; reform the Federal Information Security Management Act 2002; increase cyber research and development; promote cyber-education; and foster better international cybersecurity cooperation. In addition, we have consistently advocated for voluntary critical infrastructure protections that leverage market-based incentives, some of which are reflected in the bill.

We appreciate the bill's focus on improving real-time sharing of cyber threat information while addressing privacy and civil liberties concerns associated with new information-sharing authorities. The bill will break down barriers and provide incentives for the government and private sector to work together to better disseminate details about cyber threats, which is critical for bolstering our defenses against America's enemies. The bill also demonstrates your recognition that other currently permitted information-sharing arrangements must be allowed to continue.

Furthermore, we believe it is of the utmost importance that the country's critical infrastructure is protected. In order to do this, industry players must work together with government entities to build collaborative solutions. This is why we have consistently opposed highly regulatory schemes

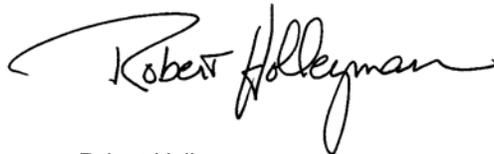
that will bog down rather than enhance security. Instead, we have long advocated for voluntary, incentive-based policies for addressing the cybersecurity of critical infrastructure. The bill represents progress in the right direction toward a voluntary regime, but we believe it should be amended to make clear that any new mechanism contemplated for protecting critical infrastructure must be truly voluntary.

The legislation demonstrates the importance of ensuring that the federal government serves as an example for the private sector by reforming FISMA to better secure its own operations. The changes you have proposed will allow agencies to allocate their limited resources to the most effective tools for managing risk, including continuous, real-time monitoring of their networks—rather than mandating that they conduct rigid, “check-the-box” exercises. This shift in strategy will make federal information technology systems more adaptive and reliable.

Finally, the bill’s emphasis on research and development — including educating a stronger cyber workforce — will help strengthen our defenses for years to come. And the inclusion of provisions that promote international cooperation in the fight against cyber threats is also important because cyber intrusions know no borders.

For these reasons, we believe that S.3414 represents a path forward for the Senate to discuss cybersecurity legislation that will help protect our country. We hope there will be a robust and open debate on the floor and look forward to working with Senators on both sides of the aisle to ensure a well-crafted bill is passed.

Sincerely,

A handwritten signature in black ink that reads "Robert Holleyman". The signature is fluid and cursive, with a large, sweeping initial "R" that extends to the left.

Robert Holleyman
President and CEO