

Microsoft Corporation  
Law and Corporate Affairs  
1401 Eye Street NW, Suite 500  
Washington, DC 20005

Tel. 202-263-5900  
Fax 202-263-5901 or 5902  
<http://www.microsoft.com/>



June 24, 2010

The Honorable Joseph I. Lieberman  
Chairman  
Committee on Homeland Security and  
Governmental Affairs  
340 Dirksen Senate Office Building  
Washington, DC 20510

The Honorable Susan M. Collins  
Ranking Member  
Committee on Homeland Security and  
Governmental Affairs  
350 Dirksen Senate Office Building  
Washington, DC 20510

The Honorable Thomas R. Carper  
Chairman  
Subcommittee on Federal Financial Management, Government  
Information, Federal Services, and International Security  
Committee on Homeland Security & Governmental Affairs  
340 Dirksen Senate Office Building  
Washington, DC 20510

Dear Chairman Lieberman, Ranking Member Collins, and Chairman Carper:

Microsoft thanks you for your commitment to, and leadership, on cyber security and critical information infrastructure protection. Your bill, the Protecting Cyberspace as a National Asset Act of 2010 (S. 3480), demonstrates a deep understanding of the challenges that the nation faces in cyberspace, and provides a much needed structure and process to address those issues.

One of the most significant challenges facing government is that it must balance dual, and often interrelated, roles to effectively manage emerging cyber threats. The government, as a public policy entity, is responsible for protecting public safety, as well as economic and national security, and the United States must develop and implement a comprehensive strategy to address the full spectrum of risks presented in cyberspace. At the same time, the federal government is a large and widely distributed enterprise, with countless globally distributed "customers" (e.g., citizens who want to connect with their government), partners, operations, networks, and resources. Although distinct, the government's policy and enterprise roles are not entirely separate, as each affects and informs the other. The work you and your staff have put into developing S. 3480 clearly demonstrates your understanding and commitment to advancing these roles.

If enacted, S. 3480 will help to strengthen the appropriate roles of government in building and implementing a national strategy and also in protecting its own enterprise. We strongly support the intended outcomes of this legislation and key provisions it offers to advance cyber security. For example, Title I requires the development of a much needed comprehensive national strategy to increase security

and resiliency in cyberspace. Title II provides a constructive risk-based approach to preparing for and mitigating the potential implications of cyber attacks, and also makes important clarifications about roles and responsibilities. In particular, we applaud the enhancements that focus on the full spectrum of risk management, and require government to work with industry not only to understand those risks, but also to respond to actual emergencies.

Further, the addition of Section 254 is an important enhancement that provides greater clarity to both government and the private sector about the criteria for the designation of covered critical infrastructure, as well as a mechanism and a process for the designation. Title III provides a needed modernization of the Federal Information Security Management Act (FISMA). Enacting this legislation will advance cyber security and governance across the federal enterprise.

While we support this bill, there are a few provisions that will be challenging to implement with respect to private industry. In particular, the federal government lacks expertise at understanding private sector enterprises and their information security programs. This is primarily due to not having enough personnel with the requisite skills to implement the bill as drafted. Title IV puts the government on the right track to increase its capacity to engage on these issues over the long-term. In the meantime, leveraging international standards for preparedness and security, as well as third-party audits which are part of industry's regular rhythm of business should be integrated into the efforts defined by the bill.

Developing legislation of this nature is a major undertaking and we appreciate that you and your staff have taken the time to engage with and consider views from the private sector. That engagement is appreciated and clearly reflected by enhancements incorporated into the bill.

Microsoft thanks you for your continued efforts to improve the cyber security posture of the Nation and of the federal agencies. We look forward to continuing to work with you and your staff as S. 3480 advances in the Senate.

Sincerely,

A handwritten signature in blue ink that reads "Fred S. Humphries, Jr." The signature is written in a cursive, slightly slanted style.

Fred S. Humphries, Jr.  
Managing Director, U.S. Government Affairs  
Microsoft Corporation