United States Senate

WASHINGTON, DC 20510

February 29, 2012

The Honorable Harry Reid
Majority Leader
United States Senator
Washington, D.C. 20510

The Honorable Mitch McConnell
Minority Leader
United States Senator
Washington, D.C. 20510

Dear Leaders Reid and McConnell:

With each passing day, our nation becomes less secure as the number and complexity of cyber threats grow. Not a week goes by that we do not hear about another attempted intrusion of growing sophistication. Though some may differ on how best to approach this critical issue, there is now broad-based bipartisan consensus that we must act to address the serious threat cyber attacks pose to our national security. That is why we urge you to bring S. 2105, the Cybersecurity Act of 2012, to the floor for consideration by the full Senate as soon as possible.

Some of our colleagues recently wrote you asking that you delay consideration of this critical legislation, claiming that the Senate is not prepared to debate on the Senate floor how best to address cybersecurity and that further study and process is necessary to ensure that the views of all members of the Senate are considered. Given the extensive and exhaustive bipartisan and multi-Committee process through which S. 2105 was created, and the serious nature of the cyber threat to our national security, we wholeheartedly disagree.

There is perhaps no body that calls for as much extensive debate as the United States Senate and the process through which S. 2105 was created is no exception. Since 2005, the Senate Homeland Security and Governmental Affairs Committee alone has held 10 hearings on the cyber threat. Since the Senate began concentrated work on cybersecurity legislation in 2009 – over three years ago – the Senate has: (1) held more than 20 cybersecurity hearings across at least seven different committees, and addressed cybersecurity questions in dozens of additional hearings; (2) held numerous briefings for Senators and staff on cybersecurity; (3) organized several other forums for Senators to examine cybersecurity issues, including the Intelligence Committee's 2010 Cyber Security Task Force and an ongoing informal discussion group led by Senators Whitehouse, Blunt, Mikulski, and Kyl; (4) considered nearly twenty separate cybersecurity bills and numerous cybersecurity amendments; and (5) held mark-ups of cybersecurity legislation in five separate committees under regular order.

Because comprehensive cybersecurity legislation cuts across multiple committees of jurisdiction making a markup of comprehensive legislation infeasible, you agreed last year to bring all the committees with jurisdiction over some aspect of cybersecurity together to form working groups that allowed work across jurisdictional lines to develop comprehensive cybersecurity legislation. We strongly supported your approach, which built on two years of bipartisan work that we had previously undertaken and went to work immediately.

Despite this bipartisan and cross-jurisdictional process, some of our colleagues chose not to engage fully. Still, we went to great lengths to incorporate their ideas and address their concerns. For instance, we have clarified the definition of what critical infrastructure would be covered by the bill to ensure that only the most critical systems – ones that if disrupted could reasonably lead to mass casualties, mass evacuations, catastrophic economic damage, or severe degradation of national security – would be designated as covered critical infrastructure.

Additionally, we have changed the bill to ensure that only covered systems that are not currently secure would be required to meet performance requirements – entities already sufficiently securing their systems would be exempted from the bill. We have added provisions giving the President authority to waive a covered critical infrastructure sector or portion of a sector if an existing Federal agency has sufficient security standards in place. We also added provisions ensuring that DHS does not develop performance requirements where existing regulations already require an appropriate level of security and provisions requiring DHS to work with other Federal agencies to ensure that any performance requirements take into account existing regulations and reporting obligations to avoid duplication. To address concerns by particular Members, we removed the White House Office of National Cyberspace Policy from the bill. Finally, we included Senator Feinstein's information sharing bill to facilitate greater sharing of cybersecurity threat information.

Recently, several of the members who wrote to you last week have indicated that they will introduce their own cybersecurity bill in short order. We are encouraged by their recognition that we must act to address the increasingly sophisticated and dangerous attacks on our national infrastructure. We invite them to put forward their ideas as soon as possible so that we can begin working together on this important national security issue.

We are being attacked in cyber space now and we need to respond now. Our enemies would enthusiastically welcome us to further postpone this bill in the name of even more "process." But, after years of work to develop legislation on this pressing problem, the time has come to make the hard choices on how we are going to defend our nation's security from cyber attacks. We can no longer delay action on deciding how to deal with this critical issue and reiterate our request that you bring comprehensive cybersecurity legislation to the Senate floor as soon as possible.

Sincerely,

Joseph I. Lieberman
Chairman
Senate Committee on Homeland Security
and Governmental Affairs

Susan M. Collins
Ranking Member
Senate Committee on Homeland Security
and Governmental Affairs

John D. Rockfeller IV
Chairman
Senate Committee on Commerce,
Science, and Transportation

Dianne Feinstein
Chairman
Senate Select Committee on Intelligence