June 6, 2012

Dear Senators Reid and McConnell,

We write to urge you to bring cyber security legislation to the floor as soon as possible. Given the time left in this legislative session and the upcoming election this fall, we are concerned that the window of opportunity to pass legislation that is in our view critically necessary to protect our national and economic security is quickly disappearing.

We have spoken a number of times in recent months on the cyber threat – that it is imminent, and that it represents one of the most serious challenges to our national security since the onset of the nuclear age sixty years ago. It appears that this message has been received by many in Congress – and yet we still await conclusive legislative action.

We support the areas that have been addressed so far, most recently in the House: the importance of strengthening the security of the federal government's computer networks, investing in cyber research and development, and fostering information sharing about cyber threats and vulnerabilities across government agencies and with the private sector. We urge the Senate to now keep the ball moving forward in these areas by bringing legislation to the floor as soon as possible.

In addition, ***we also feel that protection of our critical infrastructure is essential in order to effectively protect our national and economic security from the growing cyber threat.*** Infrastructure that controls our electricity, water and sewer, nuclear plants, communications backbone, energy pipelines and financial networks must be required to meet appropriate cyber security standards. Where market forces and existing regulations have failed to drive appropriate security, we believe that our government must do what it can to ensure the protection of our critical infrastructure. Performance standards in some cases will be necessary – these standards should be technology neutral, and risk and outcome based. We do not believe that this requires the imposition of detailed security regimes in every instance, but some standards must be minimally required or promoted through the offer of positive incentives such as liability protection and availability of clearances.

Various drafts of legislation have attempted to address this important area – the Lieberman/Collins bill having received the most traction until recently. We will not advocate one approach over another – however, ***we do feel strongly that critical infrastructure protection needs to be addressed in any cyber security legislation.*** The risk is simply too great considering the reality of our interconnected and interdependent world, and the impact that can result from the failure of even one part of the network across a wide range of physical, economic and social systems.

Finally, we have commented previously about the important role that the National Security Agency (NSA) can and does play in the protection of our country against cyber threats. A piece

of malware sent from Asia to the United States could take as little as 30 milliseconds to traverse such distance. Preventing and defending against such attacks requires the ability to respond to them in real-time. NSA is the only agency dedicated to breaking the codes and understanding the capabilities and intentions of potential enemies, even before they hit "send." ***Any legislation passed by Congress should allow the public and private sectors to harness the capabilities of the NSA to protect our critical infrastructure from malicious actors.***

We carry the burden of knowing that 9/11 might have been averted with the intelligence that existed at the time. We do not want to be in the same position again when 'cyber 9 /11' hits – it is not a question of 'whether' this will happen; it is a question of 'when.'

Therefore ***we urge you to bring cyber security legislation to the floor as soon as possible.***

Sincerely,

Hon. Michael Chertoff

Hon. J. Mike McConnell

Hon. Paul Wolfowitz

Gen. Michael Hayden

Gen. James Cartwright (RET)

Hon. William Lynn III