JOHN McCAIN
ARIZONA

COMMITTEE ON ARMED SERVICES
COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
COMMITTEE ON INDIAN AFFAIRS

United States Senate

241 RUSSELL SENATE OFFICE BUILDING
WASHINGTON, DC 20510-0303
(202) 224-2235

2201 EAST CAMELBACK ROAD
SUITE 115
PHOENIX, AZ 85016
(602) 952-2410

122 NORTH CORTEZ STREET
SUITE 108
PRESCOTT, AZ 86301
(928) 445-0833

407 WEST CONGRESS STREET
SUITE 103
TUCSON, AZ 85701
(520) 670-6334

TELEPHONE FOR HEARING IMPAIRED
(602) 952-0170

May 9, 2012

General Keith B. Alexander
Director, National Security Agency
Commander, U.S. Cyber Command
Fort George G. Meade, MD 20755-6000

Dear General Alexander:

Thank you for your response to my March 29, 2012, letter regarding our nation's cybersecurity strategy. After reading your letter I was struck by the disparity between the position taken in your response to my questions and the legislative proposal being supported by the Administration in the United States Senate.

It is widely known that we both agree much remains to be done to deter and dissuade our adversaries in cyberspace. We both understand that the current strategy is insufficient and overly reliant on defense, doing little to discourage those who look to hold U.S. interests at risk in cyberspace. And like you, I believe that the Congress should pass and the President should sign legislation to improve our nation's cybersecurity. The issue is too important to our economic and national security for anyone to either ignore or politicize. This is why I was extremely disappointed to learn of the Statement of Administration Policy recommending a veto of cybersecurity legislation in the House of Representatives. Thankfully, the Administration's attempt to stop progress was ignored by a strong bipartisan bloc of House Members. The bill easily passed 248 to 168.

As you know, there are multiple layers to the cybersecurity discussion. The issues are as complex and diverse as the entities who utilize the Internet. So we should not allow ourselves to believe one policy approach will end our Nation's cybersecurity debate. Cybersecurity was an issue yesterday, is an issue today, and will be an issue the day after any legislation is signed into law. We can only hope to provide our government and those in the private sector with the necessary information, incentive, and freedom to possess more secure networks. The assertion that we can have totally secure cyber networks is a fiction.

Turning to the substance of your letter, it is evident that information sharing and regulatory requirements, or government standards, for critical infrastructure are at issue. The debates taking place in the House of Representatives, the Senate and the media reflect that reality. The fundamental difference in approaches to each of these proposals is the facilitation of a cooperative relationship between the government and the private sector – who own roughly 90 percent of critical cyber infrastructure – or to establish an adversarial one.

With respect to information sharing, I agree with my colleagues on the other side of the aisle that removing legal hurdles to promote information sharing across industry and within the government is critical to better cybersecurity. It is clear that a more complete understanding of our cyber threats is essential to affording the government and the private sector the opportunity to protect their own networks. However, I do not believe tying liability protection exclusively to sharing with the government should be characterized as voluntary, that it encourages better information sharing practices in general or does enough to protect individual privacy. It could in fact do the opposite.

Additionally, I recognize that confronting the cyber threats we face will take a wide-ranging approach. Our odds are much more favorable when we leverage all assets and expertise within the federal government and the private sector to protect our interests and combat against those who seek to harm us. And since a significant component of the threat we face today originates outside the United States from sophisticated international actors and nation states like China and Russia, it seems counter-intuitive to add a layer of bureaucracy between those on the front lines, and those best equipped to respond. The bill the Administration supports, the 'Cybersecurity Act of 2012' (Cybersecurity Act), favors building such a bureaucracy. Rather than empowering those with the actual capabilities to defend the homeland from foreign threats, the Administration is supporting a policy which elevates the Department of Homeland Security (DHS) as a regulator and an information broker, at the expense of improved national security and private sector flexibility.

In previous statements, you have said that "if the Department of Defense (DOD) is to defend the Nation against cyber attacks originating from outside the United States, it must be able to see those attacks in real time." To be clear, no piece of cybersecurity legislation before either body of Congress authorizes surveillance, government monitoring or Internet militarization. However, your statement infers a premium should be placed on speed and rapidity of response. I support this notion and therefore fail to see how building additional layers of bureaucracy is consistent with this position or would result in better cybersecurity. Unfortunately, by supporting these additional layers of bureaucracy, which would have the effect of erecting walls around information, the Administration indicates that it does not share our view.

One area where we clearly disagree is the authorization of the DHS to impose regulatory requirements or standards on whatever the Secretary determines to be critical infrastructure. I do, however, appreciate the fact that you acknowledge such "requirements should not be too burdensome." Unfortunately, the authorities that would be granted to the Secretary in the Cybersecurity Act are in fact, too burdensome. I am unaware of the Congress ever creating a regulatory regime in which it does not say what entities would be regulated, and simultaneously authorizes a government agency, an agency with few if any regulatory successes, to determine what needs to be regulated and how to regulate it.

I also take issue with your statement that "the proposed security requirements in the Administration's proposal would not dictate specific measures that may become outdated, but rather would require critical infrastructure to achieve security results using methods of their

choice." It is hardly a choice when the options are to either comply with the DHS regulations or face civil penalties. These regulations or standards would have the effect of diverting resources from actual cybersecurity towards compliance with government mandates. These mandates would provide a false sense of security. After all, the DHS does not possess the expertise to craft cybersecurity standards and one need only review its woeful record on the Chemical Facility Anti-Terrorism Standards (CFATS) program to understand its lack of expertise in standard setting.

After re-reviewing the Cybersecurity Act, it should become apparent to you and the Administration that the bill adds layers of bureaucracy and grants burdensome regulatory authorities to the DHS. Further, if your goal is to improve voluntary information sharing, fully leverage a government-wide cyber effort, increase the speed at which the government can respond to cyber threats, and not add burdensome regulations on the owners of critical infrastructure, you should support S. 2151, the 'SECURE IT of 2012.' Our bill avoids a burdensome regulatory framework, improves cybersecurity through a cooperative, non-adversarial relationship between the government and the private sector, and allows those who have the greatest capabilities to protect us to have the best opportunity to do so.

Thank you for your attention to this important matter.

Sincerely,

John McCain
United States Senator