UNITED STATES CYBER COMMAND
FORT GEORGE G. MEADE, MARYLAND 20755-6000

The Honorable John McCain
Ranking Member, Committee on Armed Services
United States Senate
241 Senate Russell Office Building
Washington, DC 20510-0303

Dear Senator McCain:

(U//FOUO) Thank you for your letter of 29 March 2012 expressing concerns about the cyber threats facing our nation. I share your view that the United States will inevitably face a large-scale cyber attack, and I take very seriously the issues you outlined. Both U.S. Cyber Command (USCYBERCOM) and the National Security Agency/Central Security Service (NSA/CSS) are taking measures to mitigate the threat and build the capability to respond in cyberspace as directed by the President. I would like to invite you to visit us at Fort Meade and see for yourself the capabilities we have currently, and those we are developing to take actions in cyberspace against potential adversaries. In the interim, I appreciate the opportunity to respond to your questions and concerns.

- (U//FOUO) What additional authorities do you believe are necessary to defend the United States from a cyber attack initiated by a peer-competitor like China or Russia?

(U//FOUO) Let me clarify my views about what I believe we need now to defend the Nation in cyberspace. I believe we need both supportive legislation and appropriately delegated authorities. My views on these issues have been consistent and are reflected in my public statements and testimony. I believe supportive legislation is needed in two related areas - information sharing and core critical infrastructure hardening. 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. This requires legislation that, at a minimum, removes existing barriers and disincentives that inhibit the owners of the critical infrastructure from sharing cyber threat indicators with the Government.

(U//FOUO) Additionally, given DoD reliance on certain core critical infrastructure to execute its mission, as well as the importance of the Nation's critical infrastructure to our national and economic security overall, legislation is also needed to ensure that infrastructure is sufficiently hardened and resilient. Recent events have shown that a purely voluntary and market driven system is not sufficient. Some minimum security requirements will be necessary to ensure that the core critical infrastructure is taking appropriate measures to harden its networks to dissuade adversaries and make it more difficult for them to penetrate those networks. At the same time, it is important that legislative requirements not be too burdensome.

(U//FOUO) The President has the necessary authority to order military action to defend our nation against all attacks whether they come from terrorists or nation states and in any domain from sea, air, land, or cyberspace. Since the President can delegate appropriate authorities to the Secretary of Defense to use the Department's operational capabilities, including USCYBERCOM, to defend the Nation from cyber attack, legislative action is not required. This has been the subject of extensive dialogue with the Senate Armed Services Committee and I look forward to the continuation of that dialogue. I will keep you and the Committee informed as we mature our operational capabilities in cyberspace.

- (U//FOUO) Which agency within the federal government has the most cybersecurity expertise and is most capable of protecting critical infrastructure?

(U//FOUO) No single public or private entity has all of the required authorities, resources, and capabilities; cybersecurity requires a team. In the Federal Government, the responsibilities and capabilities are distributed across Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the DoD/Intelligence Community (IC), most notably USCYBERCOM and NSA/CSS. This distribution is, at once, both distinguished and complementary. All three, working as a team, play a role in protecting our networks, preventing intrusions, and responding to cyber events.

(U//FOUO) DHS' primary roles are to protect civilian government networks, increase the cybersecurity capability of core critical infrastructure networks, and enhance national resilience and preparedness. DHS secures unclassified federal civilian government networks and provides response mitigation and support to the private sector. DHS also coordinates the response to significant cyber incidents.

(U//FOUO) The role of FBI is to investigate, prevent, and respond to cyber events that are criminal or counterintelligence-related inside the United States. FBI is the lead for domestic cyber threat intelligence and attribution, as well as law enforcement and domestic counterintelligence. FBI also informs DHS' cyber mission by providing information to aid their preparation and protection efforts.

(U//FOUO) With respect to both the DHS and FBI roles, the limited, voluntary information sharing by the private sector inhibits the government's ability to protect domestic cyberspace, which is why it must be a key element of any cyber legislation as I mentioned earlier. It would also greatly benefit DoD, which assists DHS and the FBI with intelligence support in their respective roles.

(U//FOUO) As a member of the DoD and IC, NSA/CSS is responsible for: foreign cyber threat intelligence and attribution; providing guidance to secure national security systems; and furnishing DHS with intelligence and expertise to enhance the protection of U.S. networks. USCYBERCOM is responsible for defending the Nation from a cyber attack and for the operations, defense, and security of military systems and networks. USCYBERCOM also supports other Combatant Commands (CCMD) with offensive and defensive cyber capabilities and integrating these capabilities into CCMD Operational Plans.

- (U//FOUO) Does the Department of Defense rely on any critical infrastructure that, under the Administration's proposals, would be subject to Department of Homeland Security oversight?

(U//FOUO) Yes, DoD does rely on certain key critical infrastructure, to include power, transportation, telecommunications, and the Defense Industrial Base (DIB). Pursuant to the Administration's proposals, DHS would, in consultation with the private sector, and in coordination with DoD and other sector-specific agencies, be responsible for setting cybersecurity requirements and ensuring they achieve a baseline level of security. DoD would share the responsibility to protect the DIB with DHS, support DHS efforts to protect other critical infrastructure, and defend the Nation in the event of a cyber attack on the critical infrastructure. FBI would be responsible for conducting investigations of intrusion activity in those critical infrastructure networks inside the United States.

- (U//FOUO) Can the Department of Homeland Security currently protect our national interest in the cyber realm without NSA involvement?

(U//FOUO) No, protecting our national interest in the cyber realm requires a team effort consisting of DHS, FBI, NSA/CSS and USCYBERCOM.

- (U//FOUO) Do you believe we are deterring and dissuading our adversaries in cyberspace?

(U//FOUO) No, while work is ongoing in each area, much remains to be done across both the public and private sectors.

- (U//FOUO) With respect to imposing requirements on the private sector, if the rate of technological advances outpaces the implementation of performance requirements and regulation, how would imposing additional regulations better protect us from a catastrophic cyber attack?

(U//FOUO) 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. We expect this approach will actually result in greater innovation, as companies look to the commercial market to produce security products and services that satisfy these requirements. Additionally, it is important to note that the Administration's proposal leverages, rather than duplicates existing regulatory processes, allows for exemption of certain core infrastructure for which sector-specific regulatory agencies have sufficient requirements and enforcement mechanisms, and explicitly excludes regulation of technology products and services.

(U//FOUO) Lastly, at the 27 March SASC/Senate Select Committee on Intelligence briefing, you voiced concerns about an imbalance in the cyber workforce allocation between offense and defense. My response focused on the need to move to a new paradigm where our military cyber professionals are trained and equipped to execute both offensive and defensive missions. As you know, this is analogous to how DoD routinely employs Fighter-Attack aircraft in multiple roles; from interdiction of enemy forces to defensive counter air missions. Our recent experiences at CYBER FLAG, which was modeled after the DoD's realistic RED FLAG exercises, saw us for the first time employing cyber teams that seamlessly executed both offensive and defensive missions. The lessons learned prove the powerful operational capability inherent in this organizational model, which combines both attack and defend capabilities under a single commander.

(U//FOUO) Senator, I look forward to discussing this and any other issues you would like at your convenience, and again I would welcome your visit to Team Cyber at Fort Meade if your schedule permits. I remain committed to providing you my best military and technical advice and expertise.

VR

KEITH B. ALEXANDER
General, U.S. Army
Commander