JOHN McCAIN
ARIZONA

CHAIRMAN, COMMITTEE ON
ARMED SERVICES
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS
COMMITTEE ON INDIAN AFFAIRS

United States Senate

225 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

November 18, 2015

VIA U.S. MAIL & EMAIL (Deirdre.Walsh@dni.gov)

The Honorable James R. Clapper
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director Clapper:

In recent testimony before the House Select Committee on Intelligence, you acknowledged that the United States continues to lack "both the substance and the psychology of deterrence" in cyberspace, and that until an effective policy of deterrence is in place, our country will continue to face attacks and intellectual property theft from cyber adversaries, such as China. This, along with President Obama's recent and belated observation that "[w]e're going to have to be much more rapid in responding to attacks," as well as news that the Administration would not be imposing sanctions on Chinese businesses and individuals most responsible for the egregious industrial espionage against U.S. companies, I write seeking an explanation for the Administration's delay in developing a cyber deterrence policy and utilizing the many tools available to it to achieve substantive deterrence.

The National Defense Authorization Acts (NDAA) over the past three years have included numerous provisions concerning cyber deterrence. Unfortunately, thus far the Administration has failed to implement or utilize many of the tools already authorized by law. Section 941 of the Fiscal Year 2014 NDAA, required the President to develop an integrated policy to deter adversaries in cyberspace and to provide that policy to Congress not later than 270 days from the enactment of that act. The President signed that bill into law on December 26, 2013 and the required policy is now well over a year late.

Section 1637 of the NDAA for Fiscal Year 2015, which was signed into law on December 19, 2014, required an annual report to Congress on "foreign countries that engage in economic or industrial espionage in cyberspace with respect to trade secrets or proprietary information owned by United States persons." That report was due to the appropriate congressional committees in June and has yet to be delivered. This report will be especially important as a way to measure whether the bilateral agreement with China or a similar agreement announced this week among the Group of 20 will result in a change of behavior and reduction of cyber-attacks.

Section 1637 granted the President new authority to respond to persistent cyber theft against U.S. persons and companies by imposing sanctions on individuals who engage in and

benefit from such espionage. By cutting off from our financial system those who seek to gain a competitive advantage over U.S. companies through industrial espionage, this authority would help deter the further theft of American economic, military, and political secrets. The President, recognizing the utility of sanctions in confronting cyber adversaries, in April signed Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." However, neither of these authorities have been utilized to sanction individuals and hold accountable the worst perpetrators of these activities, or to deter continued cyber-enabled theft.

This Administration has so far refused to articulate a robust strategy to deter cyberattacks against the United States. And, you testified recently that "hope springs eternal" that a recent agreement between the U.S. and China on activities in cyberspace will result in any meaningful change to China's behavior in this arena. The reality is the activity will persist until those determined to attack understand there is a cost associated with cyber theft. Repeated attacks demonstrate the potential cost of a weak cyber strategy and the national security price we may pay for refusal to utilize available tools to deter further attacks.

Please provide an update on the status of the reports required by Section 941 of the FY14 NDAA and Section 1637 of the FY15 NDAA and an update on how the sanction authority provided for in this section will be utilized as part of a strategy to defend our nation from increasingly advanced and determined cyber adversaries. Furthermore, please provide an assessment of whether mandatory sanctions authority would better accomplish the goal of this authority to hold accountable foreign countries and individuals that engage in and sponsor repeated and costly economic and industrial espionage against U.S. companies and individuals.

Sincerely,

John McCain
United States Senator