

JOHN McCAIN
ARIZONA

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

United States Senate

November 18, 2015

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

VIA U.S. MAIL & EMAIL (doj.correspondence@usdoj.gov; CongresstoDHS@hq.dhs.gov) TELEPHONE FOR HEARING IMPAIRED (602) 952-0170

The Honorable Loretta Lynch
Attorney General
U. S. Department of Justice
Robert F. Kennedy Building
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

The Honorable Jeh Johnson
Secretary of Homeland Security
U.S. Department of Homeland Security
Nebraska Avenue Complex
3801 Nebraska Avenue, N.W.
Washington, DC 20528

Dear Attorney General Lynch and Secretary Johnson:

In the days leading up to Chinese President Xi Jinping's recent visit to the United States, it became clear that, despite public statements to the contrary, President Obama would not be imposing sanctions on Chinese businesses and individuals most responsible for egregious acts of industrial cyber-espionage against U.S. companies. Instead, the President announced a bilateral commitment with China that neither government would conduct or support the theft of intellectual property through cyber-space for economic gain. This was followed by a similar agreement among the Group of 20 (G20) this week. Questions remain about the scope of these agreements, how compliance will be monitored and verified, and what penalties would result from failures in compliance.

Deputy Secretary of Homeland Security Alejandro Mayorkas recently traveled to China in preparation for upcoming meetings between you and your Chinese counterparts in Washington, DC aimed at advancing the bilateral agreement with China. As you prepare for these discussions, I write to remind you of the range of tools available to our government in the face of complex cybersecurity challenges and the importance of utilizing these tools to deter further cyberattacks and intellectual property theft.

The record of theft of valuable and sensitive information from our government and private sector is well documented. What General Keith Alexander identified as the "greatest transfer of wealth in human history" in 2012 continues unabated and undeterred today. President Obama recently stated that "there comes a point where we consider this a core national security

threat” and that “we can choose to make this an area of competition” with China or we can seek areas of agreement. I am dismayed by this President’s inability to recognize that this is already a national security threat as well as an area of competition with China. Economic espionage undermines the competitiveness and survival of key sectors of the American economy; and, the theft of intellectual property, particularly from the defense industry, represents a serious threat to our national security. This wide-scale theft of economic data paired with the exfiltration of government data, as occurred with the recent cyber-attacks at the Office of Personnel Management, represents a multi-pronged attack on, and declination of, any national military, economic, and intelligence advantage we might enjoy.

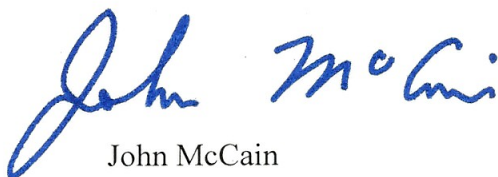
With these serious national security threats in mind, Congress included provisions in the National Defense Authorization Act (NDAA) for Fiscal Year 2015 in Section 1637 granting the President new authority to respond to persistent cyber theft against U.S. persons and companies by imposing sanctions on 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 could potentially deter the further theft of American economic, military, and political secrets.

The authority provided in Section 1637 to sanction culpable individuals represents a tool that would deter future espionage by raising the cost on individuals and nations that seek to gain a competitive military, economic, and political edge by infiltrating our industry and government networks. Most would agree that it represents a more powerful tool than the symbolic steps this Administration has taken to date, including the indictment of 5 members of the People’s Liberation Army (PLA), who are assumed will never see the inside of a U.S. courtroom.

President Obama has similarly recognized the potential impact sanctions can have in responding to cyber-attacks, signing Executive Order 13694, to “[block] the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,” in April of these year. Despite all of this, the Administration has so far refused to utilize these authorities to deter continued cyber theft.

The failure to utilize these authorities is alarmingly consistent with this Administration's refusal to articulate a robust strategy to deter cyberattacks against the United States. The theft of economic data means the United States is footing the bill for the research and development of our enemies to acquire tools to be used against us, and this will continue until our adversaries understand that attacking and pilfering the United States in cyber space is no longer a low-cost endeavor, but instead will carry real consequences, in the form of sanctions or otherwise.

Sincerely,



John McCain
United States Senator