TOM COTTON
ARKANSAS

SUITE SR-B33
RUSSELL SENATE OFFICE BUILDING
WASHINGTON, DC 20510
PHONE: (202) 224-2353
FAX: (202) 228-0908

United States Senate

COMMITTEES
ARMED SERVICES
BANKING, HOUSING, AND URBAN AFFAIRS
JOINT ECONOMIC COMMITTEE
SELECT COMMITTEE ON INTELLIGENCE
SPECIAL COMMITTEE ON AGING

April 8, 2016

The Honorable Ashton Carter
Secretary of Defense
1000 Pentagon
Washington, DC 20301

Dear Secretary Carter:

Last year *The New York Times*, *The Wall Street Journal* and other news outlets highlighted a concerning trend of technology transfers to China by U.S. companies. These technology transfers are a result of Chinese government policies designed to coerce U.S. technology firms to disclose sensitive information and intellectual property. If China employs this technology it will weaken America's military technological advantage, putting servicemembers at increased risk from advanced weapon systems. Further, it would enable foreign hackers to exploit cyber vulnerabilities that could cripple our supply chains and undermine critical infrastructure at home.

I am concerned this type of technology transfer endangers the national and economic security of the United States; jeopardizes the cybersecurity of individuals, enterprises and governments globally; and undermines decades of U.S. non-proliferation policies regarding high-performance computing. The commercial consequence of China's industrial policy is also clear—China seeks to use technology transferred by U.S. firms to develop substitute products and replace U.S. technology providers with Chinese equivalents, first in their domestic market and then in markets U.S. tech companies now service.

The *Times* article in particular raised significant national-security concerns related to a series of transactions between IBM and Chinese companies—including those associated with or controlled by the Chinese government and military. A report published by a security firm with ties to the Department of Defense and referenced by the *Times*, notes that "The transfer of IBM's intellectual property, source code, and proprietary information to Chinese end-users compromises the integrity of IBM systems used by the U.S. government and military. Security concerns related to this sale have already forced the U.S. Navy to find new sources for procuring servers critical to Ballistic Missile Defense upgrades for the Aegis Combat System."

IBM claims all of their activities in China are legal, and that other companies take a similar approach. Perhaps, but that doesn't rebut the facts presented by the report or address concerns that these actions could put U.S. national and economic security at risk. To address these concerns I'm requesting the following additional information from the Department of Defense so that Congress may better address this pressing matter:

1. IBM's transfer of high performance OpenPOWER processor designs has serious national security implications, particularly as products based on technologies transferred to

JONESBORO
300 SOUTH CHURCH, SUITE 338
JONESBORO, AR 72401
PHONE: (870) 933-6223
FAX: (870) 933-6590

SPRINGDALE
1108 SOUTH OLD MISSOURI ROAD
SUITE B
SPRINGDALE, AR 72764
PHONE: (479) 751-0879
FAX: (479) 927-1092

LITTLE ROCK
11809 HINSON ROAD
SUITE 100
LITTLE ROCK, AR 72212
PHONE: (501) 223-9081
FAX: (501) 223-9105

EL DORADO
106 WEST MAIN STREET, SUITE 410
EL DORADO, AR 71730
PHONE: (870) 864-8582
FAX: (870) 864-8571

Chinese companies are used by various U.S. government agencies and support research on and testing of advanced weapons, aerospace and missile technology.

a. Are weapons systems, testing platforms, or research programs currently using IBM POWER or OpenPOWER processors?
b. What is the relationship of Lawrence Livermore National Laboratory, Oak Ridge National Laboratory, and Sandia National Laboratory with IBM's OpenPOWER Foundation?
c. Are the aforementioned National Laboratories contributing Department of Defense funded research, technology, or expertise to IBM's OpenPOWER Foundation, where it is available to Chinese companies such as the Zhongxing New Telecommunications Equipment Co., Ltd (ZTE)?

2. The U.S. Navy took prudent action to replace elements of the Aegis Ballistic Missile Defense mission systems as a result of technology transfers to China thereby reducing the risk of cyber exploitation.
    a. What process is in place to evaluate alternate technologies and suppliers to IBM high performance chip sets transferred under the OpenPOWER Foundation?
    b. Because the OpenPOWER designs transferred to China are based on IBM's POWER chipsets, has the Department of Defense identified what other mission systems or supporting infrastructure may also be at risk for cyber exploitation?

3. IBM's transfer of middleware and database software source code to Chinese firms tied to the People's Liberation Army and the Ministry of State Security also increases the risk to U.S. government IT systems relying on these software products.
    a. Has the Department of Defense inventoried the mission systems or supporting infrastructure using these components?
    b. In addition to wholly-owned and operated systems, has the Department of Defense evaluated if any contracted Cloud service companies rely on these software products to provide services to the Department of Defense?
    c. Are alternative middleware and database software products available to meet mission requirements?
    d. Can you please identify mission systems or support infrastructure using IBM middleware and database software code that are open to disruption or manipulation?

Thank you for your prompt response to these important questions.

Sincerely,

Tom Cotton
United States Senator