EDWARD J. MARKEY
MASSACHUSETTS

COMMITTEES:
ENVIRONMENT AND PUBLIC WORKS
FOREIGN RELATIONS
RANKING MEMBER:
SUBCOMMITTEE ON EAST ASIA, THE PACIFIC, AND INTERNATIONAL CYBERSECURITY POLICY
COMMERCE, SCIENCE, AND TRANSPORTATION
RANKING MEMBER:
SUBCOMMITTEE ON SPACE, SCIENCE, AND COMPETITIVENESS
SMALL BUSINESS AND ENTREPRENEURSHIP
CHAIRMAN:
U.S. SENATE CLIMATE CHANGE TASK FORCE

United States Senate

SUITE SD-255
DIRKSEN BUILDING
WASHINGTON, DC 20510–2107
202–224–2742

975 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
617–565–8519

222 MILLIKEN BOULEVARD, SUITE 312
FALL RIVER, MA 02721
508–677–0523

1550 MAIN STREET, 4TH FLOOR
SPRINGFIELD, MA 01103
413–785–4610

March 12, 2019

The Honorable Patrick Shanahan
Acting Secretary of Defense
1000 Defense Pentagon
Washington, DC 20301

Dear Acting Secretary Shanahan,

According to a story in the *Wall Street Journal* ("Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets", March 5, 2019), a known Chinese hacking group is behind a series of cyberattacks on universities in the United States and abroad in an elaborate scheme to steal research about military maritime technology.[1] These hackers, previously identified in other cybersecurity breaches of Navy contractors, have successfully stolen sensitive military information as part of an ongoing cyber campaign since at least April 2017. In light of this recent revelation, I write to better understand how the Department of Defense is ensuring the security of our military research and technology developed through partnerships with U.S. universities and other academic and research institutions.

The *Wall Street Journal* reports that cybersecurity researchers determined that hackers linked to Beijing have targeted at least 27 universities in the United States and around the globe to steal sensitive military information. Nearly all the universities targeted, including the University of Hawaii, the University of Washington, and the Massachusetts Institute of Technology, have a direct connection to the important research done at Woods Hole Oceanographic Institution, located in Falmouth, Massachusetts, the largest independent oceanographic research institution in the country. Woods Hole is instrumental in developing undersea communications technology such as sonar and cameras, and many of the targeted institutions, including Woods Hole, receive significant Department of Defense research dollars.

Cybersecurity experts believe these cyberattacks are the latest incident in China's continued efforts to steal American military and economic secrets. In December, a senior official at the National Security Agency reported that Chinese cyberattacks against the United States continue to increase, including attacks on the U.S. energy, financial, transportation, and health care

[1] Dustin Volz, *Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets*, Wall Street Journal (Mar. 5, 2019), https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800

sectors.[2] The Chinese-affiliated group in this incident is the same one that allegedly has been targeting and stealing military technology from defense contractors for the last 18 months.[3]

The American university system is the world's greatest engine of research and innovation, and the Department of Defense relies on our incredible academic ingenuity to help develop the military technologies of the future. In this age of great power competition, it should come as no surprise that Chinese hackers are targeting academic institutions ripe with valuable information about U.S. military capabilities. Ensuring our military remains the greatest in the world requires us to safeguard its assets against the attacks of the 21st century. To gain a better understanding of the federal government's work in protecting our nation's military research and innovation, I request you respond to the following questions by March 29, 2019.

1. What role does the Department of Defense (DoD) play in identifying, analyzing, responding to, or creating standards or best practices to address cyber vulnerabilities of research institutions that receive grants or other research money from DoD?

2. Does DoD currently have best practices for university partnerships and grant-receiving organizations that are working on military research? If so, how does DoD share these best practices with these research entities? If not, why not?

3. If DoD does have cybersecurity best practices or standards, how often are these standards revisited and are they adjusted when information about breaches is revealed?

4. How does DoD verify that research institutions are following cybersecurity standards or best practices?

5. Are cybersecurity capabilities or the adoption of DoD cybersecurity standards or best practices a factor in deciding which institutions may receive grants or otherwise partner with DoD to conduct military research?

6. Does DoD require that universities or researchers receiving DoD contracts or grants report any cybersecurity breaches to DoD? If so, what are these reporting requirements? If not, how does DoD keep track of cybersecurity vulnerabilities at these entities?

7. For the last five years how many notices has DoD received of cybersecurity attacks or breaches at third-party research entities conducting military research? For each of these reports, what did DoD do to address them?

[2] Jim Finkle and Christopher Bing, *China's hacking against U.S. on the rise: U.S. intelligence official*, Reuters (Dec. 11, 2018), https://www.reuters.com/article/us-usa-cyber-china/chinese-hacking-against-u-s-on-the-rise-u-s-intelligence-official-idUSKBN1OA1TB.

[3] Gordon Lubold and Dustin Volz, *Chinese Hackers Breach U.S. Navy Contractors*, Wall Street Journal (Dec. 14, 2018), https://www.wsj.com/articles/u-s-navy-is-struggling-to-fend-off-chinese-hackers-officials-say-11544783401?mod=article_inline.

8. What has DoD identified as commonalities between the 27 institutions that were reported to have been targeted for cybersecurity attacks? How were these potential attacks conducted? Was there a common entry point or vulnerability that made these 27 institutions targets?

9. When DoD is made aware of a cybersecurity attack at one of its funded research institutions, does DoD share information about the nature of the attack with other funded institutions to avoid similar attacks? If so, how are these communications formalized? Is there a university cybersecurity working group for defense research?

10. Has DoD identified any additional cyber vulnerabilities of military research conducted at universities and research institutions? How do you plan to address any of these additional vulnerabilities?

11. How does DoD — whether acting alone or in concert with other federal agencies — deter cyberattacks targeting military secrets and research held by our nation's universities?

12. How does DoD respond to cyberattacks targeting military secrets and research held by our nation's universities? Does DoD:

    a. Publicly attribute the attacks to the hostile foreign actor when confident about the attacks origins? If no, please explain why not.
    b. Reevaluate our capabilities to identify, protect, detect, respond to, or recover from cyberattacks? If no, please explain why not.

Thank you for your prompt attention to this important matter. Should you have any questions about this request please contact Zachary Hosford of my staff at 202-224-2742.

Sincerely,

Edward J. Markey

Edward J. Markey
United States Senator

cc: Richard Spencer, United States Secretary of the Navy