

JOHN McCAIN, ARIZONA, CHAIRMAN

JAMES M. INHOFE, OKLAHOMA
ROGER F. WICKER, MISSISSIPPI
DEB FISCHER, NEBRASKA
TOM COTTON, ARKANSAS
MIKE ROUNDS, SOUTH DAKOTA
JONI ERNST, IOWA
THOM TILLIS, NORTH CAROLINA
DAN SULLIVAN, ALASKA
DAVID PERDUE, GEORGIA
TED CRUZ, TEXAS
LINDSEY GRAHAM, SOUTH CAROLINA
BEN SASSE, NEBRASKA
TIM SCOTT, SOUTH CAROLINA

JACK REED, RHODE ISLAND
BILL NELSON, FLORIDA
CLAIRE McCASKILL, MISSOURI
JEANNE SHAHEEN, NEW HAMPSHIRE
KIRSTEN E. GILLIBRAND, NEW YORK
RICHARD BLUMENTHAL, CONNECTICUT
JOE DONNELLY, INDIANA
MAZIE K. HIRONO, HAWAII
TIM Kaine, VIRGINIA
ANGUS S. KING, JR., MAINE
MARTIN HEINRICH, NEW MEXICO
ELIZABETH WARREN, MASSACHUSETTS
GARY C. PETERS, MICHIGAN

United States Senate

COMMITTEE ON ARMED SERVICES

WASHINGTON, DC 20510-6050

CHRISTIAN D. BROSE, STAFF DIRECTOR
ELIZABETH L. KING, MINORITY STAFF DIRECTOR

July 27, 2018

The Honorable James N. Mattis
Secretary of Defense
1000 Defense Pentagon
Washington, DC 20301-1000

Dear Secretary Mattis:

We write to express our concern over the cybersecurity risks posed to Department of Defense (DoD) information held by defense contractors. We were alarmed to read about the breach of a Navy contractor's computer network in a June 8th 2018, *Washington Post* article titled "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare." This article brought to the fore many challenges facing most, if not all, defense contractors who handle controlled unclassified information.

Since this article's publication, the Senate Armed Services Committee has gathered information that suggests DoD simply is not doing enough to protect controlled unclassified government information. We are concerned with existing regulations and best practices related to protecting controlled unclassified information in the following areas: (1) Contracts lacking the appropriate National Institute for Science and Technology (NIST) cybersecurity clauses; (2) Computer networks operating without multi-factor authentication, strong remote user policies, and encryption of data at rest; and (3) Insufficient third-party verification of compliance with cybersecurity standards.

Furthermore, we understand that the cybersecurity standard for defense contractors contained in NIST Special Publication (SP) 800-171 is a lower standard than the NIST standard (800-53) that is applied elsewhere in the federal government. We do not understand why defense contractors working on projects of national security importance are held to a *lower* cybersecurity standard.

Finally, we believe a single senior DoD official must be put in charge and *take charge* of the policy, procedures, and compliance regarding the handling of controlled unclassified information among defense contractors. Until a single official is given the authority, responsibility, and accountability for protecting the government's interests in this regard, our defense contractors will continue to be woefully underequipped to defeat the threat.

We understand the Deputy Secretary of Defense indicated that these responsibilities would be assigned to the Department's Chief Information Officer. The official must be fully empowered to exercise this function if he is to be successful. We look forward to regular updates on his progress.

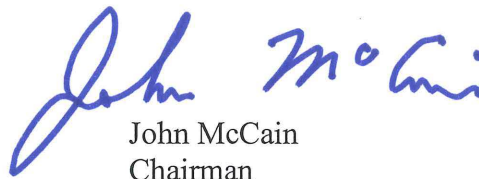
Time is of the essence to do more to defend the controlled unclassified information held by our defense contractors. Action is needed now to improve compliance with existing regulations and best practices, as well as increase the cybersecurity standard for defense contractors, with a single DoD official in charge.

We stand ready to work with you and look forward to your response.

Sincerely,



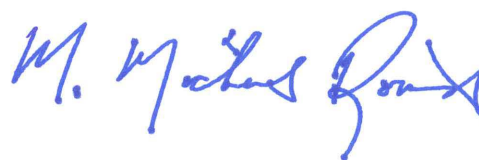
Jack Reed
Ranking Member
Senate Armed Services
Committee



John McCain
Chairman
Senate Armed Services
Committee



Bill Nelson
Ranking Member
Subcommittee on
Cybersecurity



M. Michael Rounds
Chairman
Subcommittee on
Cybersecurity