THE ASSISTANT SECRETARY OF THE NAVY
(RESEARCH, DEVELOPMENT AND ACQUISITION)
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SEP 28 2018

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks

Reference: (a) Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012
(b) National Institute of Standards and Technologies (NIST) Special Publication 800-171
(c) NIST Special Publication 800-53

Given the cybersecurity threats to networks that house controlled unclassified information (CUI) and the intrusions into contractor's unclassified networks, it is apparent that information critical to Naval warfighting is being maintained without adequate considerations to cybersecurity risk. It is imperative that the Department of the Navy (DON) take immediate steps to increase the protection of its critical information.

Effective immediately, in addition to the protection requirements in reference (a) and (b), DON program managers with current and future contracts, task or delivery orders (hereafter referred to as "contracts"), that are under my purview as the Service Acquisition Executive and for which the respective Program Executive Officer or Chief of Naval Research, in coordination with Resource Sponsor, has determined that the risk to a critical program and/or technology warrants it, shall immediately include a Contract Data Requirement List (CDRL) requiring the delivery and approval of a Systems Security Plan (SSP) that implements the security requirements in reference (a).

The CDRL shall contain a requirement that permits the Government to validate the information in the contractor's submission every three years, on an ad hoc basis with no notice to the contractor, or upon replacement or rotation of the Government program manager.

Program managers shall not approve the contractor's submitted System Security Plan that does not:

- Fully implement Multi-factor authentication, including authentication and authorization of users in a manner that is auditable;
- Fully implement FIPS 140-2 validated encryption;
- Employ the principle of least privilege or "need to know";
- Require the contractor to review in a manner that can be audited user privileges at least annually;

- Require Monitoring and controlling remote access sessions and include mechanisms to audit the sessions and methods; and
- Implement, at a minimum, all security requirements in NIST 800-171 (Rev. 1) standards 3.1 to 3.14; or ensure that any unimplemented security requirements have been adjudicated by an authorized representative of the DoD CIO to be non-applicable or to have an alternative, but equally effective security measure in its place, and provide proof of such adjudication by DoD CIO.

In accordance with reference (a) DoD defense contractors are required to report cyber incidents to the Damage Assessment Management Office (DAMO) via the DIB-Net website within 72 hours. In addition to the notification requirements in reference (a), program mangers shall include in all applicable contracts, a CRDL requiring delivery of all information related to cyber incidents (as defined in reference (a)) to the Defense Cyber Crime Center within 15 days of a cyber incident. The CDRL shall require segregation of DON CUI from contractor-owned information, when feasible. Segregation can be implemented through logical isolation, physical isolation, a hybrid approach, or other technological processes are acceptable to achieve required delivery of compromised data in cyber incidents.

In additional to the CDRL requirements outlined above, program managers shall include the following requirements in contract statements of work:

- A requirement for encryption of data at rest, as defined in reference (c), Security Controls SC-13 and SC-28(1).
- A requirement for the contractor to allow the Naval Criminal Investigative Service (NCIS) to install network sensors, owned and maintained by NCIS, on the contractor's information systems or information technology assets when intelligence indicates a vulnerability, or potential vulnerability.
- A requirement that the contractor engage with NCIS industry outreach efforts and consider recommendations for hardening of DON critical programs and technologies.

In solicitations for contracts to be awarded in the future, program managers shall work with their contracting officers to include a requirement in solicitations for the submission of the pertinent sections of the SSP for evaluation as part of any competitive source selection or sole source proposal review.

SUBJECT: Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks

Within 30 days of this memorandum, program managers shall provide me with the following information:

- A summary of the methodology used to assess whether the current contracts, within my purview as the Service Acquisition Executive, should employ the additional requirements in this memorandum.
- A list of the current contracts and upcoming efforts that will be subject to the additional requirements in the memorandum.
- A summary of the contracts considered but that will not include the requirements of this memorandum.

Within 180 days of this memorandum, Program Executive Officers and Chief of Naval Research shall provide me an update on the current contracts subject to the additional requirements of this memorandum that have not yet been modified to incorporate them.

My point of contact is Deputy Assistant Secretary of the Navy for Acquisition and Procurement (DASN (AP)), Mr. Elliott Branch. He can be reached at elliott.branch@navy.mil.

James F. Geurts

Distribution:
CMC (DC, I&L)
CNR

Distribution con't:
COMMARCORSYSCOM
COMNAVAIRSYSCOM
COMNAVFACENGCOM
COMNAVSEASYSCOM
COMNAVSUPSYSCOM
COMSC
COMSPAWARSYSCOM
DRPM SSP
PEO (A)
PEO (T)
PEO (U&W)
PEO (CARRIERS)
PEO (C4I)
PEO (SPACE)
PEO (EIS)

PEO (IWS)
PEO (JSF)
PEO (LS)
PEO (SHIPS)
PEO (SUBS)

Copy to:
AGC
CMC (LB)
DONAA
MARCORSYSCOM (CT)
MSC (N10)
NAVAIRSYSCOM (2.0)
NAVFACENGCOM (ACQ)
NAVSEASYSCOM (02)
NAVSUPSYSCOM (N7)
ONR (02)
SPAWARSYSCOM (2.0)
SSP (SPN)
DASN (AIR)
DASN (SHIP)
DASN (C41 & SPACE)
DASN (RDT&E)
DASN (ELM)
DASN (IP)
DASN (M&B)