THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION
AND SUSTAINMENT

NOV 14 2019

MEMORANDUM FOR COMMANDER, U.S. CYBER COMMAND
(ATTN: ACQUISITION EXECUTIVE)
COMMANDER, U.S. SPECIAL OPERATIONS COMMAND
(ATTN: ACQUISITION EXECUTIVE)
COMMANDER, U.S. TRANSPORTATION COMMAND
(ATTN: ACQUISITION EXECUTIVE)
ASSISTANT SECRETARY OF THE ARMY FOR ACQUISITION, LOGISTICS, AND TECHNOLOGY
ASSISTANT SECRETARY OF THE NAVY FOR RESEARCH, DEVELOPMENT, AND ACQUISITION
ASSISTANT SECRETARY OF THE AIR FORCE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Assessing Contractor Implementation of Cybersecurity Requirements

Over the past year, the Department of Defense (DoD) has strengthened its efforts to ensure that DoD's controlled unclassified information (CUI) is safeguarded when processed, stored or transmitted on a contractor's internal unclassified information system or network, and the DoD Components have worked to assess contractor compliance with cybersecurity requirements on a contract-by-contract basis. While these efforts have been effective at the contract level, we have learned that efficiencies can be gained by strategically assessing a contractor's implementation of cybersecurity requirements at the corporate level.

Per my direction on February 5, 2019, Strategically Implementing Cybersecurity Contract Clauses (https://www.acq.osd.mil/dpap/pdi/cyber/index.html), the Director, Defense Contract Management Agency (DCMA), in partnership with the Acting Principal Director, Defense Pricing and Contracting (DPC), the DoD Chief Information Officer, the Office of the Under Secretary of Defense for Research and Engineering, the Office of the Under Secretary of Defense for Intelligence, and other DoD Components, developed the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment Methodology, Version 1.0 (https://www.acq.osd.mil/dpap/pdi/cyber/index.html). This standard methodology enables the strategic assessment of a contractor's implementation of NIST SP 800-171, "Protecting CUI In Nonfederal Systems and Organizations," a requirement for compliance with Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting."

The standard DoD methodology consists of three assessment levels, each resulting in a different level of confidence. Specifically, the levels are as follows:

- Basic Assessment. Contractor self-assessment of system security plan(s) developed in accordance with NIST SP 800-171, resulting in a 'low' level of confidence in the resulting score.

- Medium Assessment. DoD review of the system security plan(s) informed by interviews, discussion, and clarification with the Contractor, resulting in a 'medium' level of confidence in the resulting score.

- High Assessment. DoD review of the system security plan(s), informed by interviews, discussion, and clarification with the Contractor, and on-site validation of implementation, conducted in accordance with NIST SP 800-171A, "Assessing Security Requirements for CUI," resulting in a 'high' level of confidence in the resulting score.

DCMA, with assistance from the Defense Counterintelligence and Security Agency (DCSA) and other DoD Components, initiated a pilot program in June 2019 to implement and test this methodology, completing High Assessments for the Department's largest contractors. The feedback and collaboration provided during this pilot helped streamline the methodology and documentation of assessment results. The Supplier Performance Risk System (SPRS), the DoD's authoritative source for supplier and product performance information, has been updated to include summary results of these assessments and provide the following information:

- The organization that conducted the assessment (e.g., DCMA, DCSA, or DoD component)

- Scope of the information system/system security plan(s) assessed (e.g., the internal unclassified information system(s)/network(s), mapped to contractor CAGE codes, that support(s) performance of DoD contracts)

- Date and level of the assessment (i.e., Basic, Medium, or High)

- Total summary score for each system security plan(s) assessed

- Date that a score of 110 (full implementation) is expected to be achieved

DCMA will continue to work with our DoD and industry partners to conduct assessments in accordance with this methodology and update SPRS with the results. Acquisition officials should access SPRS to determine if assessment results have been documented for a contractor information system(s) associated with contract performance. DoD Components are encouraged to consider the assessment results documented in SPRS whenever possible in lieu of requesting an additional assessment.

The standard DoD-wide methodology for assessing DoD contractor implementation of the security requirements in NIST SP 800-171 will be implemented in the DFARS. If you have

any questions regarding this matter, my point of contact is Ms. Mary Thomas, at 703-693-7895 or mary.s.thomas.civ@mail.mil. The DCMA point of contact is Mr. John Ellis, at 804-734-0476 or john.a.ellis.civ@mail.mil.

Ellen M. Lord

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION
AND SUSTAINMENT

FEB - 5 2019

MEMORANDUM FOR COMMANDER, U.S. CYBER COMMAND
(ATTN: ACQUISITION EXECUTIVE)
COMMANDER, U.S. SPECIAL OPERATIONS
COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, U.S. TRANSPORTATION
COMMAND (ATTN: ACQUISITION EXECUTIVE)
ASSISTANT SECRETARY OF THE ARMY FOR ACQUISITION,
LOGISTICS, AND TECHNOLOGY
ASSISTANT SECRETARY OF THE NAVY FOR RESEARCH,
DEVELOPMENT, AND ACQUISITION
ASSISTANT SECRETARY OF THE AIR FORCE FOR
ACQUISITION, TECHNOLOGY, AND LOGISTICS
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Strategically Implementing Cybersecurity Contract Clauses

Implementing Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 across all Department of Defense (DoD) contracts, with the exception of those for commercially available off-the-shelf items, is vital to the future security of the United States. DFARS 252.204-7008 requires contractors to represent on a contract-by-contract basis that their implementation of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 is complete. To document the implementation of NIST SP 800-171, companies must develop, document, and periodically update a system security plan that describes system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. If implementation of the security requirements is not complete, companies must develop and implement plans of action to describe how and when any unimplemented security requirements will be met.

This individual contract approach is inefficient for both Industry and Government, and impedes the effective implementation of requirements to protect DoD's Controlled Unclassified Information for contracts containing DFARS clause 252.204-7012. Therefore, pursuant to this memorandum, I direct the Director, Defense Contract Management Agency (DCMA), to develop a proposed path ahead using its administration authority under Federal Acquisition Regulation Part 42 and 43 and DFARS 242.302 to modify contracts that are administered by DCMA to achieve the objectives below. Such authority will be limited to bilateral modifications that do not result in a change to any contract price, obligated amount, or fee arrangement. DCMA, in partnership with the Principal Director, Defense Pricing and Contracting (DPC); the DoD Chief Information Officer; the Deputy Director, Strategic Technology Protection and Exploitation; the Office of the Under Secretary of Defense for Intelligence; and the DoD Components, will:

- Assess and recommend to the Under Secretary of Defense for Acquisition and Sustainment a set of business strategies to—
  - Obtain and assess contractor system security plans, and any associated plans of action, strategically (not contract-by-contract);
  - Propose a methodology to determine industry cybersecurity readiness, and a level of confidence in the readiness assessment, at the corporate, business sector (division) or facility level; and
  - Propose how to communicate (document and share) that cybersecurity readiness and confidence level to the DoD Components.
- Engage industry to discuss methods to oversee the implementation of DFARS Clause 252.204-7012 and NIST SP 800-171.
- Include within the business strategies above, consideration of leveraging DCMA's contracting officers authority to incorporate a repeatable strategic process/discussion to pursue a no-cost bilateral block change to:
  - Require submission of company's system security plan (or extracts thereof), and any associated plans of action, at a strategic level;
  - Document industry cybersecurity readiness at a strategic level;
  - Apply a standard methodology to recognize industry cybersecurity readiness at a strategic level and include a process to update this recognition as cybersecurity readiness changes over time; and
  - Negotiate inclusion of DFARS clause 252.204-7012 to existing contracts without the clause as part of the block change modification process.

To ensure a similar corporate approach may be taken with companies for which DCMA does not administer contracts (such as the Secretary of the Navy's shipbuilding contracts), DPC will work with representatives of those communities to implement a similar solution. DPC will host a meeting on Wednesday, February 6, 2019 to address the proposed methodology to recognize industry cybersecurity readiness, and address any concerns that you may have. Please contact Ms. Mary Thomas at 703-693-7895 or mary.s.thomas.civ@mail.mil with the name of any attendees. I have directed DCMA not to exercise this authority until after March 1, 2019. If you do not agree with the approach, please notify the action officers identified below before that date.

If you have any questions regarding this matter, my point of contact is Ms. Mary Thomas. The DCMA point of contact is Mr. John Ellis, at 804-734-0476 or john.a.ellis.civ@mail.mil.

Ellen M. Lord