



ACQUISITION  
AND SUSTAINMENT

## THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3010

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](mailto: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](mailto:john.a.ellis.civ@mail.mil).



Ellen M. Lord