ASSISTANT SECRETARY OF DEFENSE
3600 DEFENSE PENTAGON
WASHINGTON, DC 20301-3600

ACQUISITION

DEC 17 2018

MEMORANDUM FOR COMMANDER, UNITED STATES CYBER COMMAND
(ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES SPECIAL OPERATIONS
COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES 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: Strengthening Contract Requirements Language for Cybersecurity in the Defense Industrial Base

The Department amended the Defense Federal Acquisition Regulation Supplement (DFARS) in 2016 by adding DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. This clause requires contractors to implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," as a means to safeguard covered defense information that is processed, stored or transmitted on the contractor's internal unclassified information system or network. To effectively implement these cybersecurity requirements, it is imperative for the Department to identify and track flow down of DoD's controlled unclassified information, and to ensure these requirements are addressed and assessed as part of the procurement process.

The Director, Defense Pricing and Contracting (DPC), issued a memorandum on November 6, 2018 providing guidance for assessing compliance and enhancing protections required by the DFARS 252.204-7012 clause. This DPC guidance provides acquisition personnel with a framework of actions that can be tailored by a program office/requiring activity, commensurate with program risk, to assess the contractor's approach to protecting the Department's controlled unclassified information. The guidance includes sample Contract Data Requirements Lists and associated Data Item Descriptions and can be found at https://www.acq.osd.mil/dpap/pdi/cyber/guidance_for_assessing_compliance_and_enhancing_protections.html.

This memorandum provides program offices and requiring activities with sample Statement of Work (SOW) language that can be used in conjunction with the DPC guidance. The attached sample language assists in SOW and associated CDRL implementation of existing

requirements of DFARS clause 252.204-7012 by addressing access to/delivery of the contractor's system security plan (or extracts thereof), access to/delivery of the contractor's plan to track flow down of covered defense information and assess compliance of known Tier 1 Level suppliers.

Collectively, this language supports development of cybersecurity measures designed to enhance existing protection requirements provided by DFARS Clause 252.204-7012. I strongly encourage DoD program managers and requiring activities to incorporate the attached sample requirements language, as appropriate, when risk to their programs and technologies warrant it.

Kevin Fahey
Assistant Secretary of Defense
for Acquisition

Program 1-2-3

Sample Statement of Work (SOW) Language for Requesting the System Security Plan and Any Associated Plans of Action as a Contract Deliverable in accordance with NIST SP 800-171

Statement of Work (SOW) Paragraph x,y,z:

x.y.1. The Contractor shall, upon request, provide to the government, a system security plan (or extract thereof) and any associated plans of action developed to satisfy the adequate security requirements of DFARS 252.204-7012, and in accordance with NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" in effect at the time the solicitation is issued or as authorized by the contracting officer, to describe the contractor's unclassified information system(s)/network(s) where covered defense information associated with the execution and performance of this contract is processed, is stored, or transmits. System Security Plan and Associated Plans of Action for a Contractor's Internal Unclassified Information System [Insert Contract Data Requirements List (CDRL)* Data Item Number Block 1 of DD Forum 1423-1].

x.y.2. The Contractor shall, upon request, provide the government with access to the system security plan(s) (or extracts thereof) and any associated plans of action for each of the Contractor's tier one level subcontractor(s), vendor(s), and/or supplier(s), and the subcontractor's tier one level subcontractor(s), vendor(s), and/or supplier(s), who process, store, or transmit covered defense information associated with the execution and performance of this contract. System Security Plan and Associated Plans of Action for a Contractor's Internal Unclassified Information System [Insert Contract Data Requirements List (CDRL)* Data Item Number Block 1 of DD Forum 1423-1].

* CDRL for System Security Plan and Associated Plans of Action for a Contractor's Internal Unclassified Information System is found in Defense Pricing and Contracting Memo, Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, dated November 6, 2018 (https://www.acg.osd.mil/dpap/pdi/cyber/index.html).

Program 1-2-3

Sample Statement of Work (SOW) for Requesting the Identification, Tracking, and Restricted Flow Down of all Covered Defense Information, and for Requesting the Contractor's Record of Tier 1 Level Subcontractors, Vendors, and/or Suppliers who Receive or Develop Covered Defense Information

Statement of Work (SOW) Paragraph x,y,z:

x.y.1 Identify all covered defense information associated with the execution and performance of this contract. At the post-award conference the Contractor and the Government/Program Office shall identify and affirm marking requirements for all covered defense information, as prescribed by DoDM 5200.01 Vol 4, Controlled Unclassified Information, and DoDI 5230.24, Distribution Statements on Technical Documents, to be provided to the Contractor, and/or to be developed by the contractor, associated with the execution and performance of this contract.

x.y.2 Track all covered defense information associated with the execution and performance of this contract. The Contractor shall document, maintain, and provide to the Government, a record of tier 1 level subcontractors, vendors, and/or suppliers who will receive or develop covered defense information – as defined in DFARS Clause 252.204-7012 and associated with the execution and performance of this contract. Contractor's Record of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information [Insert Contract Data Requirements List (CDRL)* Data Item Number Block 1 of DD Forum 1423-1].

- Restrict unnecessary sharing and/or flow down of covered defense information associated with the execution and performance of this contract. The Contractor shall restrict unnecessary sharing and/or flow down of covered defense information – as defined in DFARS Clause 252.204-7012 and associated with the execution and performance of this contract – in accordance with marking and dissemination requirements specified in the contract and based on a 'need-to-know' to execute and perform the requirements of this contract. This shall be addressed and documented at the post-award conference.

x.y.3 The Contractor shall flow down the requirements in x.y.1 and x.y.2 to their tier 1 level subcontractors, vendors, and/or suppliers.

* CDRL for Contractor's Record of Tier 1 Level Suppliers Receiving/Developing Covered Defense Information, is found in Defense Pricing and Contracting Memo, Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, dated November 6, 2018, (https://www.acg.osd.mil/dpap/pdi/cyber/index.html)