OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
AND SUSTAINMENT

NOV 2018

MEMORANDUM FOR COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES TRANSPORTATION COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES CYBER COMMAND (ATTN: ACQUISITION EXECUTIVE)
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DEPUTY ASSISTANT SECRETARY OF THE ARMY (PROCUREMENT), ASA (ALT)
DEPUTY ASSISTANT SECRETARY OF THE NAVY (RESEARCH, DEVELOPMENT AND ACQUISITION), ASN (RDA)
DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE (CONTRACTING), SAF/AQC
DIRECTORS, DEFENSE AGENCIES
DIRECTORS, DEFENSE FIELD ACTIVITIES

SUBJECT: Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

The Department amended the Defense Federal Acquisition Regulation Supplement (DFARS) in 2016 to provide for the safeguarding of the Department's covered defense information when residing on or transiting through a contractor's internal unclassified information system or network. DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, 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," to safeguard covered defense information that is processed, stored, or transmitted on the contractor's internal unclassified information system or network.

The Office of the Principal Director, Defense Pricing and Contracting, in collaboration with the Office of the Deputy Assistant Secretary of Defense for Information and Integration Portfolio Management, the Office of the Undersecretary of Defense for Research and Engineering, and the Office of the DoD Chief Information Officer, drafted "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented," and "Guidance for Assessing Compliance of and Enhancing Protections for a Contractor's Internal Unclassified Information System," to assist acquisition personnel in the development of effective cybersecurity strategies to enhance existing protection requirements provided by DFARS clause 252.204-7012 and NIST SP 800-171. Acquisition personnel are reminded that these measures to enhance the protection requirements of DFARS Clause 252.204-7012

may only be used when the contractor's unclassified information system will process, store, or transmit covered defense information, and should be tailored commensurate with the risk to the program. This guidance was made available to the public for comment in Federal Register, Volume 83 Issue 79 (Tuesday, April 24, 2018). All comments were considered and integrated, when appropriate, into the final documents described below:

- "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented," available at https://www.acq.osd.mil/dpap/pdi/cyber/index.html, is provided to:
  - Enable the consistent review of System Security Plans and Plans of Action when such plans are required by the solicitation or contract to be provided to the Government.
  - Address the impact of 'not yet implemented' security requirements on a contractor's unclassified internal information system.
  - Provide clarification on implementing NIST SP 800-171 security requirements.

- "Guidance for Assessing Compliance of and Enhancing Protections for a Contractor's Internal Unclassified Information System," available at https://www.acq.osd.mil/dpap/pdi/cyber/index.html, provides 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 providing adequate security to protect the Department's controlled unclassified information. Tailorable actions include:
  - Requiring delivery of the contractor's system security plan (or extracts thereof)
  - Requiring the contractor to identify known Tier 1 Level suppliers
  - Requesting the contractor's plan to track flow down of covered defense information and to assess DFARS clause 252.204-7012 compliance of known Tier 1 Level suppliers.

It is critical that efforts to identify, track, and safeguard DoD controlled unclassified information are addressed, and assessed, as part of the procurement process. To assist program offices/requiring activities in the execution of these actions to enhance the protection requirements of DFARS Clause 252.204-7012 when risk to the program warrants it, a Contract Data Requirements List (CDRL) entitled, "Request Contractor's Record of Tier 1 Level Suppliers who Receive or Develop Covered Defense Information," a CDRL entitled, "Request Contractor's System Security Plan and Any Associated Plans of Action for Contractor's Internal Information System," and the corresponding Data Item Descriptions (DIDs) referenced in the CDRLs, are also included as attachments to "Guidance for Assessing Compliance of and Enhancing Protections for a Contractor's Internal Unclassified Information System."

DoD Components are strongly encouraged to implement the guidance referenced above to address their individual program needs and requirements. This guidance will be integrated into DFARS Procedures, Guidance, and Information 204.73 – Safeguarding Covered Defense Information and Cyber Incident Reporting, as appropriate. If you have

questions or concerns related to this guidance, please contact Mary Thomas at mary.s.thomas.civ@mail.mil, or 703-693-7895.

for LeAnna Sumpter
Kim Herrington
Acting Principal Director
Defense Pricing and Contracting