OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

March 11, 2024

MEMORANDUM FOR DISTRIBUTION

SUBJECT: DoD Office of Inspector General Report No. DODIG-2024-031, "Special Report: Common Cybersecurity Weaknesses Related to the Protection of DoD Controlled Unclassified Information on Contractor Networks," November 30, 2023 (Report No. DODIG-2024-031)

We are revising two sentences on page 1 in the subject report to correct errors identified after publishing. The revisions are technical and do not affect the overall conclusions presented in the original report. You can find the updated report on our website at http://www.dodig.mil/reports.html.

We are revising the second sentence in the second paragraph, "DFARS 252.204-7012 requires contractors and grantees that maintain CUI to implement security controls specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800 171, which lists security requirements for safeguarding sensitive information on non Federal information networks and systems." to read, "Contractors and grantees that maintain CUI are required by DFARS 252.204-7012 and DoDI 8582.01, as applicable, to implement security controls specified in National Institute of Technology (NIST) Special Publication (SP) 800-171, which lists security requirements for safeguarding sensitive information on non-Federal information networks and systems." We are also revising the last sentence in the second paragraph "As of October 2016, DFARS 252.204-7012 is required in all DoD contracts and grants." to read, "As of October 2016, DFARS 252.204-7012 is required in all DoD contracts."

The report is a summary of previously issued audit reports and does not include findings and recommendations; therefore, we are not requesting comments on these revisions. As previously stated, the revisions do not impact the findings, conclusions, and recommendations of the summarized reports.

Please reference the attached page as a replacement page 1 for any copy of the subject report in your possession. We revised only the page indicated and modified no other information in the report.

If you have any questions on the revision, please contact me at [redacted] or [redacted].

FOR THE INSPECTOR GENERAL:

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Attachment:
As Stated

Distribution:

SECRETARIES OF THE MILITARY DEPARTMENTS
UNDER SECRETARIES OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

Background

As of October 1, 2023, the DoD had 183,562 active contracts with organizations for goods and services that ranged from laboratory equipment and supplies to management support for weapon systems. To support the delivery of those goods and services, many DoD contractors process, store, and transmit controlled unclassified information (CUI) on their networks and systems.[1] CUI is information created or possessed for the Government that requires safeguarding or dissemination controls according to applicable laws, regulations, and Government-wide policies. CUI is not classified information as defined in Executive Order 13526, "Classified National Security Information," December 29, 2009. The responsibility of Federal agencies to protect CUI does not change when such information is shared with or used by contractors in the course of their contracts. Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by contractors on their networks and systems.

The Defense Pricing and Contracting Office, a Component within the Office of the Under Secretary of Defense for Acquisition and Sustainment, establishes DoD contracting and procurement policy and provides updates to the Defense Federal Acquisition Regulation Supplement (DFARS), which requires contractors to safeguard DoD information.[2] Contractors and grantees that maintain CUI are required by DFARS 252.204-7012 and DoD Instruction 8582.01, as applicable, to implement security controls specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, which lists security requirements for safeguarding sensitive information on non-Federal information networks and systems.[3] As of October 2016, DFARS 252.204-7012 is required in all DoD contracts.

NIST SP 800-171 provides contractors with security requirements for protecting the confidentiality of DoD CUI. Specifically, contractors must implement or develop a plan to implement 110 security requirements to comply with NIST SP 800-171. The 110 security requirements are grouped into 14 categories that are defined in Table 1.

[1] An example of CUI is controlled technical information, or CTI. CTI is a category of CUI that includes technical information with military or space application that is subject to access, use, reproduction, modification, performance, display, release, disclosure, or dissemination controls.

[2] The Defense Pricing and Contracting Office was formerly known as the Defense Pricing Office and as the Defense Procurement and Acquisition Policy Office.

[3] DFARS Part 252, "Solicitation Provisions and Contract Clauses," Subpart 252.2, "Text of Provisions and Clauses," Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting.

DoD Instruction 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," December 9, 2019.

NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," Revision 1, December 2016 (Updated June 7, 2018).