**Technical Amendment**

**May 2024**

**PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES**

**\* \* \* \* \***

**SUBPART 252.2—TEXT OF PROVISIONS AND CLAUSES**

**\* \* \* \* \***

**252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.**

As prescribed, in 204.7304(c), use the following clause:

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (~~JAN 2023~~**[MAY 2024]**)

\* \* \* \* \*

(b) *Adequate security.* \* \* \*

(2) \* \* \*

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (available via the internet at ~~http://dx.doi.org/10.6028/NIST.SP.800-171~~**[*https://csrc.nist.gov/publications/sp800*]**) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii) \* \* \*

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (~~https://www.fedramp.gov/resources/documents/~~**[*****https://www.fedramp.gov/documents-templates/*]**) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

\* \* \* \* \*