5001-06-P

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

[Docket DARS-2018-0023]

DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented

AGENCY: Department of Defense (DoD).

ACTION: Notice and request for comment.

SUMMARY: DoD has drafted guidance for procurements requiring implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, and is making the draft guidance available to the public.

DATES: Comments are due by May 31, 2018.

ADDRESSES: You may submit comments, identified by docket DARS-2018-0023, by any of the following methods:

- Federal eRulemaking Portal: http://www.regulations.gov. Search for "DARS-2018-0023." Select "Comment Now" and follow the instructions provided to submit a comment. Please include "DARS-2018-0023" on any attached documents.
- Mail: Defense Procurement and Acquisition Policy, Attn: Ms. Mary Thomas, OUSD(A&S) DPAP/PDI, Room 3C958, 3060 Defense Pentagon, Washington, DC 20301-3060.

FOR FURTHER INFORMATION CONTACT: Ms. Mary Thomas, DPAP/PDI, at mary.s.thomas.civ@mail.mil or by mail at: Defense Procurement and Acquisition Policy, Attn: Ms. Mary Thomas, OUSD(A&S) DPAP/PDI, Room 3C958, 3060 Defense Pentagon, Washington, DC 20301-3060.

SUPPLEMENTARY INFORMATION:

The Defense Federal Acquisition Regulation Supplement clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors to provide "adequate security" for "covered defense information" that is processed, stored, or transmitted on the contractor's internal information system or network. To provide adequate security, the contractor must, at a minimum, implement NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." NIST SP 800-171 states that in order to demonstrate implementation or planned implementation of the security requirements in NIST SP 800-171, nonfederal organizations should describe in a System Security Plan how the specified security requirements are met, or how organizations plan to meet the requirements, and should develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. NIST SP 800-171 further states that, when requested, the System Security Plan and any associated Plans of Action for any planned

implementations or mitigations should be submitted to the responsible Federal agency/contracting officer to demonstrate the nonfederal organization's implementation or planned implementation of the security requirements.

DoD developed the document "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented" to facilitate the consistent review and understanding of System Security Plans and Plans of Action, the impact that NIST SP 800-171 Security Requirements that are "not yet implemented" have on an information system, and to assist in prioritizing the implementation of security requirements not yet implemented. The document "Assessing the State of a Contractor's Internal Information System in a Procurement Action" illustrates how "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented" may be used during a procurement for which DoD must assess the state of a contractor's internal information system.

"DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented" provides a "DoD Value" to assess the risk that a security requirement left unimplemented has on an information system, to assess the risk of a security requirement with an identified deficiency, and to address the priority for which an unimplemented requirement

should be implemented. The guidance also addresses the method(s) to implement the security requirements, and, when applicable, provides clarifying information for security requirements that are frequently misunderstood.

The matrix "Assessing the State of a Contractor's Internal Information System in a Procurement Action" is provided to illustrate how DoD may choose to assess submitted System Security Plans and Plans of Action in procurement actions that require the implementation of NIST SP 800-171.

To access the documents entitled "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented" and "Assessing the State of a Contractor's Internal Information System in a Procurement Action," go to the Federal eRulemaking Portal at www.regulations.gov, search for the docket "DARS-2018-0023" click "Open Docket," and view "Supporting Documents."

Jennifer Lee Hawes,

Regulatory Control Officer,

Defense Acquisition Regulations System.

[FR Doc. 2018-08554 Filed: 4/23/2018 8:45 am; Publication Date: 4/24/2018]