DoD Specifies Implementation Requirements for NIST 800-171 Cyber Standard

Client Alert | 2 min read | 05.15.25

The Department of Defense (DoD) has **released a memorandum** establishing the DoD Organization-Defined Parameters (ODPs) for use in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision (Rev) 3. Currently, DoD's cybersecurity regimes require government contractors to comply with NIST SP 800-171 Rev. 2. However, the release of this memorandum may indicate DoD's intention to soon incorporate Rev. 3 into DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting* (DFARS 7012) as well as the forthcoming Cybersecurity Maturity Model Certification (CMMC).

NIST SP 800-171 Rev. 3 was released in May 2024. Rev. 3 introduced new controls and control families, increased specificity for certain security requirements, and introduced Organization-Defined Parameters into 800-171. ODPs are "fill-in-the-blanks" to be filled by federal agencies to create tailored requirements for each agency's specific needs.

DoD's selected ODPs range from time-based requirements, such as requiring inactive user accounts to be terminated within 24 hours, to specific technical requirements, such as the use of Federal Information Processing Standard (FIPS) validated cryptography. The ODPs will also require flowing down certain protections to subcontracts, through requiring external service providers to meet NIST SP 800-171 Rev 2 and requiring integration of supply chain risk management into procurement policies.

The ODPs will not take immediate effect. Shortly after the release of NIST SP 800-171 Rev. 3, **DoD issued a class deviation** to clarify that NIST SP 800-171 Rev. 2 would continue to be used for the DFARS 7012 Safeguarding Clause. However, this new memorandum indicates that companies should begin preparing for Rev. 3, as it suggests that DoD is gearing up for Rev. 3 implementation in both the DFARS 7012 and CMMC requirements.

Recommendation

Companies should review the new security requirements and DoD-specific ODPs to determine what technical and administrative revisions would be required to meet these emerging requirements.

Contacts

Michael G. Gruden
Partner
Washington, D.C. D | +1.202.624.2545
mgruden@crowell.com

Alexis Ward
Associate
She/Her/Hers

Los Angeles D | +1.213.271.2797
award@crowell.com

Jacob Harrison
Associate
He/Him/His

Washington, D.C. D | +1.202.624.2533
jharrison@crowell.com

