Akin®

New Cybersecurity Controls for Government Contractors: NIST Revises SP 800-171

June 11, 2024

Reading Time : **3 min**

By: Natasha G. Kohne, Angela B. Styles, Michael J. Vernick, Ryan Dowell, Joseph Hold

In May, the National Institute of Standards and Technology (NIST) issued updated recommendations for security controls for controlled unclassified information (CUI) that is processed, stored or transmitted by nonfederal organizations using nonfederal systems, (NIST Special Publication 800-171 (SP 800-171), Revision 3). These security requirements are "intended for use by federal agencies in contractual vehicles or other agreements that are established between those agencies and nonfederal organizations."[1] While these new controls are only applicable to nonfederal entities that agree to comply with the new issuance, Revision 3 signals the next phase of expected security for government contractors.

The Revised Guidelines

The latest revision aligns the SP 800-171 guidelines more closely with NIST's comprehensive catalog of security and privacy controls for federal information systems, SP 800-53, and recommends SP 800-171A, which was also updated, as the companion document for assessing security requirements.

The revised SP 800-171 guidelines removed or combined some existing CUI cybersecurity controls, streamlining the total controls from 110 to 97. Before discussing the requirements themselves, the revised guidelines first describe the assumptions and methodology used to develop the security requirements for safeguarding the confidentiality of CUI (including the categorization of "Security Requirement Families" reproduced below), the format for the requirements and the tailoring criteria applied to the NIST guidelines for the security requirements. The security requirements include: access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident

response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment and monitoring, system and communications protection, system and information integrity, planning, system and services acquisition, and supply chain risk management.[2]

The tailoring criteria are included so that CUI security requirements can be developed according to what controls are best suited for a particular context. The revised guidelines also include a number of "organization-defined parameters" (ODPs), which provide organizations with the flexibility to define CUI requirements according to their mission, business functions, operational environments and risk tolerance. ODPs also support consistent security assessments, determining whether specific security requirements were satisfied.[3]

Impact on Federal Cybersecurity

SP 800-171 is a foundation of federal cybersecurity rules such as the U.S. Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) program, the upcoming iteration of which (CMMC 2.0) will borrow heavily from SP 800-171 requirements and principles.[4] On May 2, the DoD issued a Defense Federal Acquisition Regulation Supplement (DFARS) class deviation for cybersecurity standards required for covered contractor information systems. This class deviation will require contractors subject to DFARS clause 252.204-7012 to comply with SP 800-171 Revision 2, instead of Revision 3. This deviation is intended to give contractors time to adjust to the new version, and the DoD time to align their supporting mechanisms, which demonstrates the influence of these guidelines on federal cybersecurity practices.[5]

Looking Ahead

NIST has also announced plans to revise SP 800-172 in the near future. SP 800-172 is distinguished from SP 800-171 in that it sets forth more stringent security requirements for particularly important CUI associated with critical programs and high-value assets.[6] This forthcoming revision, along with other updates to supporting publications, is expected in the coming months and will continue to influence how important sensitive information is secured across various sectors.

Takeaways

The third revision of SP 800-171 by NIST marks a significant step towards refining the security framework for protecting CUI outside of federal systems. By providing clearer guidelines and allowing for customizable security measures, NIST is enabling federal agencies to have a more easily navigated roadmap for federal contractors handling sensitive information. Because very few civilian agencies have a clear incorporation of NIST requirements in standard contract clauses, federal contractors should be alert to specific contractual requirements that may incorporate this Revision

---

1 Dep't of Com., National Institute of Standards and Technology, NIST SP 800-171r3: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (May 14, 2024), available at https://csrc.nist.gov/pubs/sp/800/171/r3/final.

2 *Id*. at 4.

3 *Id*.

4 *See CMMC Model Structure*, Chief Information Officer, U.S. Dep't of Defense, available at https://dodcio.defense.gov/CMMC/Model/.

5 Press Release, Dep't of Defense, *Department of Defense Issues Class Deviation on Cybersecurity Standards for Covered Contractor Information Systems* (May 2, 2024) available at https://www.defense.gov/News/Releases/Release/Article/3763953/department-of-defense-issues-class-deviation-on-cybersecurity-standards-for-cov/.

6 *Id*. at 1.

Categories

Cybersecurity, Privacy & Data Protection

Government Contracts

Consumer Privacy

© 2024 Akin Gump Strauss Hauer & Feld LLP. All rights reserved. Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.