Deloitte.

5x5 series: Insights and actions

NIST SP 800-171 Revision 3 Draft: Five notable updates and five actions

The National Institute of Standards and Technology (NIST) is updating NIST Special Publication (SP) 800-171, which provides recommended security requirements for protecting controlled unclassified information (CUI) that resides in nonfederal information systems and organizations.

NIST released a draft of NIST SP 800-171 Revision 3 (Rev 3), which includes some significant updates. In our 5x5 series, we explore five notable updates and five actions federal contractors can take to prepare.

Note: Revision 2 remains the standard for federal contractors handling CUI until Revision 3 is finalized and published. Per Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, contractors are subject to the requirements in NIST SP 800-171 in effect at the time the solicitation is issued or such other version that is authorized by the contracting officer.[1]

***5** updates you should know*[2]		***5** actions you can take*
For certain security requirements, Rev 3 introduced **organization-defined parameters (ODPs)**, intended to "rightsize" requirements based on the protection needs of the respective organization. For example, the number of unsuccessful system logon attempts during a certain period of time may differ across organizations.	1	**Familiarize yourself with the proposed controls with ODPs and consider how you may need to adapt to possible changes**—particularly if you support multiple federal agencies with different ODP requirements. Additionally, consider if efficiencies can be gained through the tailoring of security requirements related to ODPs, which can also reduce costs and decrease the burden of compliance.
Requirements that pertain to external system services, such as third-party providers and vendors, which fall under the new System and Services Acquisition control family.	2	**Take an inventory of your third-party system service providers and perform a risk assessment** to (1) identify critical providers; (2) evaluate potential gaps in compliance for those providers; (3) determine the possible impact these new requirements could have on your organization; and (4) develop a plan to address gaps and requirements. With that in mind, also consider implementing shared responsibility matrices with third-party providers.
New Supply Chain Risk Management (SCRM) control family, which includes various requirements intended to identify, address, and manage supply chain risks within a system, component, or service.	3	**Revisit your existing supply chain risk management program (or create one if needed) and evaluate if it sufficiently addresses the new proposed SCRM requirements**—including having (1) a SCRM plan; (2) strategies, tools, and methods to identify and mitigate supply chain risks; (3) controls and processes for identifying and addressing supply chain vulnerabilities; and (4) proper CUI disposal methods. As needed, **develop an actionable plan to address any potential gaps in your SCRM program.**
Additional details provided for various security requirements to clarify requirements and to help improve the effectiveness of implementation by organizations. For example, the requirement that personnel are trained to carry out their duties now explicitly mentions role-based security training and requires such trainings before authorizing access to the system or CUI.	4	It is important to review the additional details related to the documentation and implementation of controls, as assessors will evaluate your compliance with them. For example, **provide role-based security training to relevant personnel before they perform assigned duties or are granted access to the system or CUI.** Role-based trainings can include policies, procedures, tools, and artifacts for the defined security roles.
Organizations are required to document and disseminate policies and procedures needed to implement security requirements, which include the rules and expected behavior for handling CUI and system usage.	5	**Review existing policies and procedures** to determine if they address the respective requirements and are sufficiently documented. Additionally, **identify relevant roles and responsibilities in order to appropriately disseminate policies and procedures** to the applicable personnel and stakeholders.

Click *here* or connect with us to learn more.

Connect with us:

Alan Faver
Partner | Deloitte & Touche LLP
afaver@deloitte.com

Charan Ahluwalia
Principal | Deloitte & Touche LLP
cahluwalia@deloitte.com

Jeff Lucy
Managing Director | Deloitte & Touche LLP
jlucy@deloitte.com

Keith Thompson
Senior Manager | Deloitte & Touche LLP
keithompson@deloitte.com

Mika Alexoudis
Senior Manager | Deloitte & Touche LLP
malexoudis@deloitte.com

1. US Department of Defense, Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, September 21, 2017.
2. National Institute of Standards and Technology (NIST), NIST SP 800-171 Rev. 3 (Final Public Draft) – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, November 9, 2023.