Hogan Lovells

ADG Insights

NIST set to "enhance" contractor cybersecurity duties

September 2019


Speed
Link/Act
Speed
Link/Act

Federal agencies have taken numerous actions to protect against the threat of cyberattacks. Those actions include measures designed to protect Controlled Unclassified Information (CUI) held on information systems outside the federal government.

Standards promulgated by the National Institute of Standards and Technology (NIST) in Special Publication (SP) 800-171 have been incorporated in regulations and government contracts as the baseline standards for protecting CUI on non-federal (i.e., contractor or grantee) systems. This past spring, I in response to concerns about emerging and existent advanced persistent threats (APT), NIST released a new set of standards in SP 800-171B. SP 800-171B will supplement the baseline requirements contained in SP 800-171 by enhancing cybersecurity requirements for a small number of businesses — those that handle high value assets or participate in critical programs on a contract-by-contract basis.

But if history is an indication of the future, more companies may find themselves bound by these additional cybersecurity requirements. The public comment period for SP 800-171B concluded on August 2, 2019 and an updated version of that publication may be forthcoming soon.

Background

On September 14, 2016, the National Archives and Records Administration (NARA) released its CUI Final Rule (the CUI regulation)[1], prescribing how federal agencies must safeguard CUI. The CUI regulation also created the CUI Registry, the official online repository for information, guidance, policy, and requirements related to the handling of CUI, and required the application of NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, to CUI residing on non-federal information systems.

Since then, NIST standards have undergone several updates and revisions:

- On December 20, 2016, NIST released Revision 1 to SP 800-171 that included, among other changes, a requirement for contractors to develop and implement a System Security Plan (SSP) for systems containing CUI.
- On June 7, 2018, NIST issued an erratum update of SP 800-171 with new references and definitions. A new Appendix F provided "discussion" on each CUI requirement and NIST made minor editorial changes to the 110 security requirements as written. This is the version of SP 800-171 relied upon by the ADG industry today.
- On June 13, 2018, NIST released the final version of SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*, to serve as a companion piece to SP 800-171. This publication provided "assessment procedures and a methodology" to help both federal and nonfederal entities "conduct efficient, effective, and cost-effective assessments" of the CUI security requirements in SP 800-171.
- On October 18, 2018, NIST announced at a CUI Security Requirements Workshop that it would enhance "CUI security requirements" in the next revision of SP 800-171 to address APT and to prevent the theft or compromise of highly sensitive federal information.
- In the spring of 2019, NIST officials developed SP 800-171B, a companion publication to SP 800-171, to put additional protections in place for CUI in critical programs or high-value assets on a case-by-case basis.

Application of these standards to ADG companies

Today, SP 800-171 serves as the baseline standards for protecting CUI on non-federal systems. However, the government has seen that when CUI is part of a critical program or a high value asset, it can become a significant target for high-end, sophisticated adversaries making it subject to an ongoing barrage

1. 81 Fed. Reg. 63,324 (Sept. 14, 2016), codified at 32 C.F.R. Part 2002.

of serious cyberattacks (*i.e.*, APT). This concern prompted the Department of Defense (DoD) to request additional guidance from NIST, which NIST provided in the form of SP 800-171B. The NIST standards found in both SP 800-171 and 171B flow to ADG companies through contractual provisions. Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 requires that SP 800-171 requirements be contractually placed on contractors and subcontractors that process, store, or transmit CUI.

All CUI, which is broadly defined as unclassified information that requires "safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies," as discussed here, are subject to, at a minimum, the security measures in SP 800-171. The CUI regulation mandates that SP 800-171 provides the baseline of security requirements that should be employed to protect CUI when contracting with nonfederal organizations and systems. The standards apply only to "components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components" and apply only when nonfederal organizations do not collect or maintain information on behalf of a federal agency, do not use or operate a system on behalf of a federal agency, and no "[more] specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government wide policy for the CUI category or subcategory listed in the CUI Registry" exist.[2]

In addition, contractors operating in the ADG industry sector should expect systems that process, store, or transmit CUI within a critical program or high value asset may become subject to SP 800-171B. The enhanced security requirements of SP 800-171B will only be applicable to an ADG company when a federal agency so mandates through a contract, grant, or other agreement.

NIST SP 800-171B's enhanced CUI protection requirements

NIST designed the new enhanced requirements in SP 800-171B to combat APTs by creating a resilient, survivable, penetration resistant architecture with the ability to limit the damage from inevitable incidents. A non-exhaustive list of SP 800-171B's enhanced cybersecurity requirements include:

- Providing employees with awareness training targeted at APT actors and scenarios
- Establishing and maintaining a full-time security operations center capability
- Establishing and maintaining a deployable cyber incident response team that can be on-site within twenty-four hours
- Conducting enhanced personnel screening for trustworthiness
- Reassessing personnel trustworthiness on an ongoing basis
- Establishing a cyber threat hunting capability
- Employing automation techniques to predict and identify risks
- Reassessing the effectiveness of cybersecurity controls at least annually

Which contractors and subcontractors must comply with NIST SP 800-171B

SP 800-171B applies only to contractors and subcontractors that handle high value assets or participate in critical programs and are therefore likely targets for APTs. The enhanced cybersecurity requirements of SP 800-171B should only flow to subcontractors that independently meet that requirement. The fact that a prime contractor handles high value assets or participates in critical programs does not necessarily mean that their subcontractors do so as well. Those subcontractors, or their lower tier subcontractors, may only be subject to the baseline SP 800-171 requirements, or none at all.

However, the draft publication does not define high value assets or critical programs. The Department of Homeland Security, in conjunction with NIST, has

2 . National Institute of Standards & Technology, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST Special Publication 800-171 Rev.1*, COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY LABORATORY (Dec. 2016) (as updated 06/07/2018), available here.

defined high value assets elsewhere as "those assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests."[3] But the draft publication itself explicitly states that the enhanced requirements are only applicable when mandated by a federal agency in a contract, grant, or other agreement.[4] Absent a clear definition of these key terms, contractors may challenge an agency's effort to mandate the enhanced requirements through contract provisions by persuading the agency that they do not handle high value assets or participate in critical programs.

Subcontractors should be aware that federal agencies, especially DoD, are increasingly considering cybersecurity an important factor when selecting prime contractors[5] and that prime contractors tend to "flow down the relevant clauses out of an abundance of caution."[6] Prime contractors are astutely aware that the consequences for violating the requirements of SP 800-171 and 171B can be grave. These consequences could include damages under the False Claims Act, termination of the contract, and suspension of the ability to secure future contracts, among other consequences.[7] Failure to comply can materially affect a contractor's business. Given these risks, prime contractors have little incentive to ensure their subcontracts only include the minimum provisions required. Instead, prime contractors do, and are likely to continue to, include the SP 800-171 contract provisions almost by default. Prime contractors subject to the enhanced requirements of SP 800-171B may similarly attempt to impose these obligations on their subcontractors even if that subcontractor should not be subject to the enhanced requirements based on the work the subcontractor is actually performing for the prime. Subcontractors should thus take care not to agree to implement the enhanced controls required by SP 800-171B merely because their prime contractors are required to do so.

Takeaway

As the risk of cyberattacks grows throughout the ADG industry, companies operating in this sector should closely monitor the ever changing cybersecurity requirements and safeguards. For now, companies can look to SP 800-171 as the baseline of safeguards necessary to protect CUI. However, companies involved in critical programs or working with high value assets may find themselves subject to additional security requirements found in SP 800-171B. DoD contractors should expect to see these additional requirements applied on a contract by contract, program by program basis. DoD contractors should also pay special attention to how these requirements will correlate with the DoD's new Cybersecurity Maturity Model Certification (CMMC) program. That program requires that DoD contractors demonstrate they have the appropriate levels of cybersecurity practices and processes in place to protect CUI. Thus, companies that ensure they understand and comply with all applicable CUI controls will be well-positioned for the CMMC audit and certification process that DoD plans to roll out in 2020.

3. U.S. Department of Homeland Security, *NIST-DHS High Value Asset Control Overlay 3* (June 1, 2017), available here.

4. National Institute of Standards & Technology, *Draft NIST Special Publication 800-171B*, (June 2019) at 11, available here.

5. *Pentagon to See DoD Contractor Cyber Security as a Competitive Advantage*, SYSARC (Aug. 20, 2018), available here.

6. Stacy Hadeka & Michael Scheimer, *DoD Amends its DFARS Safeguarding and Cyber Incident Reporting Requirements with a Second Interim Rule*, FOCUS ON REGULATION (Jan 7, 2016), available here.

7. United States v. Aerojet Rocketdyne Holdings, Inc., 381 F. Supp. 3d 1240 (E.D. Cal. 2019); *Understanding NIST SP 800-171*, COMPLYUP (Last visited July 25, 2019), available here.

Authors

Stacy Hadeka
Senior Associate
Global Regulatory
Washington, D.C.
+1 202 637 3678
stacy.hadeka@hoganlovells.com

Michael Scheimer
Senior Associate
Global Regulatory
Washington, D.C.
+1 202 637 6584
michael.scheimer@hoganlovells.com

Jonathan Stulberg
Associate
Litigation, Arbitration, and Employment
Los Angeles
+1 310 785 4630
jonathan.stulberg@hoganlovells.com

Rebecca Umhofer
Knowledge Lawyer
Litigation, Arbitration, and Employment
Washington, D.C.
+1 202 637 6939
rebecca.umhofer@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices
Legal Services Center: Berlin

www.hoganlovells.com