THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 59, No. 13 April 5, 2017

Focus

¶ 87

FEATURE COMMENT: Achieving Cyber-Fitness In 2017: Part 3—Proving Compliance And The Role Of Third-Party Auditors

The Department of Defense final rule for safeguarding covered defense information requires contractors to implement the security controls in National Institute of Standards and Technology Special Publication (SP) 800-171 by December 31. See 81 Fed. Reg. 72986 (Oct. 21, 2016); Chierichella, Bourne and Biancuzzo, Feature Comment, "Achieving Cyber-Fitness In 2017: Part 1—Planning For Compliance," 59 GC ¶ 25. In enacting the final rule, the drafters created "[n]o new oversight paradigm" or certification requirement. 81 Fed. Reg. 72990. More recently, in response to questions from industry on compliance with NIST SP 800-171, DOD stated,

> *The rule does not require "certification" of any kind*, either by DoD or any other firm professing to provide compliance, assessment, or certification services for DoD or Federal contractors. *Nor will DoD give any credence to 3rd party assessments or certifications—by signing the contract, the contractor agrees to comply with the terms of the contract. It is up to the contractor to determine that their systems meet the requirements.*
>
> Some companies with limited cybersecurity expertise may choose to seek outside assistance in determining how best to meet and implement the NIST SP 800-171 requirements in their company. *But, once the company has implemented the requirements, there is no need to have a separate entity assess or certify that the company is compliant with NIST SP 800-171.*

DOD FAQs Regarding Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), Defense Federal Acquisition Regulation Supplement subpt. 204.73 and Procedures, Guidance and Information subpt. 204.73, and DFARS subpt. 239.76 and PGI subpt. 239.76 (Jan. 27, 2017), available at *http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf* (emphasis added).

Thus, DOD expects the contractor to demonstrate compliance and, without any Government audit and approval of the contractor's systems, and without any "safe harbor" arising out of prophylactic third-party audits, DOD will serve as judge and jury on the sufficiency of contractor safeguards. So, how should contractors assess and demonstrate their compliance with NIST SP 800-171? This part of our series focuses on best practices and strategies for demonstrating compliance and reducing potential liability or lost business should a cyber incident occur.

Proving Compliance—First, check the DOD solicitation—it may be your lucky day! In industry guidance, DOD stated that agencies *may* include in sections L and M of a solicitation "what constitutes acceptable/unacceptable compliance with NIST SP 800-171" or "how offeror compliance with NIST SP 800-171 will be evaluated." DOD FAQs, supra at A21.

Thus, in some cases the path to NIST SP 800-171 compliance may be spelled out. Solicitation guidance, however, may arrive too late to be of general utility in framing a compliance plan and, in the end, it will be strictly applicable only to the contract that results from that solicitation. If your customer has not addressed compliance in the solicitation, the next best option is to focus on other compliance regimes.

Note: Revision 1 of NIST SP 800-171 provides that a companion publication likely to be published this year "will provide assessment procedures to help organizations determine compliance to the security requirements." NIST SP 800-171 (Rev. 1) at n. 10.

Lessons Learned from Other Compliance Regimes—As discussed in Part 2 of our series, contractors may be subject to various cybersecurity requirements depending on their agency customers and the data with which they work. See Chierichella, Jehl, Bourne and Biancuzzo, Feature Comment, "Achieving Cyber-Fitness In 2017: Part 2—Looking Beyond The FAR And DFARS—Other Safeguarding And Reporting Requirements," 59 GC ¶ 43. NIST SP 800-171 is not significantly different from any other compliance regime—it is a checklist of minimum security requirements.

Drafters of the DFARS final rule made it clear that compliance with NIST SP 800-171 does not preempt other cybersecurity requirements (or vice versa). See 81 Fed. Reg. 72987. "DFARS 204.7300(b) states that the rule 'does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information.'" Although contractors must be mindful of other security obligations, and recognize that compliance with one regime does not necessarily guarantee compliance with others, they still can—and should—leverage documentation and agency guidance under other compliance regimes to support their response to the requirements of NIST SP 800-171.

FISMA/FedRAMP: The Federal Information Security Management Act (FISMA) requires federal agencies to implement programs to provide security for information and information systems. Organizations under contract to process, store or transmit Government data must comply with the minimum security requirements in Federal Information Processing Standards Publication 200 as well as appropriate security controls in NIST SP 800-53 (see Part 1, supra, discussing the interrelationships between NIST SP 800-171, FIPS 200 and NIST SP 800-53).

FISMA also applies to cloud service providers (CSPs). The Federal Risk and Authorization Management Program (FedRAMP) provides a standard process for ensuring the security of CSPs for use by the Government. The process and resources for securing Government authorization to operate under FedRAMP are well defined, and include (1) a readiness assessment phase; (2) an initial authorization phase, which involves creating a system security plan (SSP), a security assessment plan, a security assessment report, a plan of action and milestones; and (3) a continuous monitoring phase. See *www.fedramp.gov/resources/templates-2016/*. Resources and a security assessment framework are available for both low and moderate impact level systems, which are subject to different control levels under NIST SP 800-53.

Independent assessors, including third-party assessment organizations (organizations vetted and approved to conduct FedRAMP assessments of CSPs), are an integral part of this process. A CSP is required to create a security assessment plan with an independent assessor describing the assets to be reviewed and the methodology for the assessment, including testing. Following the security assessment, the independent assessor is required to provide a final security assessment report that includes

- a system overview,
- description of tests performed,
- identification of system vulnerabilities,
- a risk analysis,
- recommended corrective actions,
- identification of known risks, and
- an authorization recommendation.

The CSP then develops a plan of action and milestones with planned dates as well as a point of contact responsible for each weakness identified. The CSP may receive provisional authority to operate from the Joint Authorization Board (JAB), which consists of the chief information officers from the Department of Homeland Security, General Services Administration and DOD, or an individual agency may provide its own authority to operate. A provisional authority to operate from JAB indicates the CSP has met FedRAMP requirements and may be used Government-wide; individual agencies may grant authority to operate on the basis of the provisional authority to operate from JAB.

Under DFARS clause 252.239-7010, Cloud Computing Services, CSPs must comply with the Cloud Computing Security Requirements Guide, with which many companies already may comply. A contractor using an external CSP to store or transmit covered defense information must ensure that the CSP meets security requirements equivalent to those established by the Government for the FedRAMP "moderate" baseline at the time award. DFARS clause 252.204-7012(b)(2)(ii)(D); see 81 Fed. Reg. 72994.

As discussed more fully below, in taking steps to prove compliance under the DFARS rule, contractors might hire an accredited FedRAMP third-party assessment organization with demonstrated technical experience with NIST SP 800-53 assessments. Because NIST SP 800-171 is a subset of the NIST SP 800-53 security controls, an audit conducted by a third-party assessment organization should face less resistance from the Government.

HIPAA/HITECH: The Health Information Technology for Economic and Clinical Health Act requires the Department of Health and Human Services, Office for Civil Rights (OCR) to audit covered entity and business associate compliance with the Health Insurance Portability and Accountability Act (HIPAA) privacy, security and breach notification rules. Currently in Phase 2, the HIPAA audit program has matured considerably from the 2011 pilot program, and provides a useful resource for proving compliance.

The HIPAA audit process is document-intensive, and is intended to ensure that covered entities and business associates (a) have appropriate written policies and (b) follow them. During the audit process, OCR sends an initial request asking entities to identify and provide applicable policies, procedures and evidence of HIPAA implementation, or an explanation for any deficiency.

Generally, the documents requested include privacy policy and procedure manuals, workforce training documentation, incident response plans (including breach response) and risk analyses, as well as associated documented risk mitigation plans. The final audit report results in one of four findings: (1) no major compliance gaps are found and a compliance action plan is presented; (2) significant issues are found and the report proposes a remediation plan; (3) a serious deficiency is found and the OCR conducts further review; or (4) willful neglect is found and an OCR enforcement action may be brought, resulting in fines or penalties.

Contractors demonstrating compliance with the DFARS rule can use the HIPAA audit process as a guide to best practices, especially where a NIST SP 800-171 control is vaguely worded or DOD balks at the contractor's proof of compliance. A third-party auditor experienced with HIPAA can help identify corollary controls; alternatively, contractors looking to "go it alone" can cross reference the requirements using Appendix D of NIST SP 800-171 and the OCR HIPAA Security Rule Crosswalk, available at *www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf*.

Where a contractor maintains a clear file of all plans, procedures and compliance documentation for each security control (or a documented rationale explaining why a control is not applicable or why an alternate control is sufficient), a Government reviewer should be more likely to find that the contractor has taken reasonable steps to protect and secure data, and the legal and business consequences of any breach should be less severe. Furthermore, contractors already proving compliance under HIPAA may be able to repurpose much of the documentation if it is tailored to specific controlled unclassified information (CUI) under NIST SP 800-171.

Contractor Documentation—Proving compliance requires a solid trail of documentation demonstrating the contractor's understanding of, and efforts to implement, each of the security controls outlined in NIST SP 800-171. (Table 1 at the end of this article lists NIST SP 800-171 security controls warranting specific documentation.)

SSP: NIST SP 800-171 requires contractors to develop, document and periodically update their SSP. Although there is "no prescribed format or specified level of detail" required, the SSP must at a minimum "describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems." NIST SP 800-171 (Rev. 1), 3.12.4, n. 26 (Dec. 20, 2016).

Aside from the 14 control families listed in NIST SP 800-171, other items to address in the SSP are:

- <u>Governance</u>: There should be a designated individual or group charged with overseeing data security. A charter should establish the individual or group's authority, outline objectives, and provide procedures for change control and obtaining approvals.
- <u>Supply Chain Management</u>: In addition to the flowdown requirements under the DFARS clause, supply chain risks should be addressed in the policies and procedures. For example, incident response should be tested with key subcontractors.
- <u>Incident Reporting</u>: There should be documented escalation processes for complaints and incidents to get the right attention at the right levels in the organization. Training should include incident reporting as well.
- <u>Insider Threats</u>: Insider threat training is required under NIST SP 800-171, 3.2 (distinct from the more specific insider threat requirements for cleared contractors under the National Industrial Security Program Operating Manual). Policies should address how insider threat indicators are monitored, identified, handled and communicated internally.

- Monitoring: At least 11 security controls in NIST SP 800-171 expressly require monitoring activities. However, contractors also should monitor high-risk areas, focusing on risks that can have the greatest impact, and leverage risk assessments across different compliance areas if there are common controls. Contractors should document assumptions and define metrics that provide visibility into the program's effectiveness, including early indicators of security risks and compliance issues. Metrics should be reassessed periodically.

In developing their plans, contractors should consider the NIST cybersecurity framework, available at *www.nist.gov/cyberframework/draft-version-11*. This voluntary framework provides guidance on managing cybersecurity risk. More importantly, the framework allows organizations to demonstrate compliance with the CUI security requirements in the context of their established information security programs. NIST SP 800-171 notes:

> Organizations that have implemented or plan to implement the NIST Framework for Improving Critical Infrastructure Cybersecurity can find in Appendix D of this publication, a direct mapping of the Controlled Unclassified Information (CUI) security requirements to the security controls in NIST Special Publication 800-53 and ISO/IEC 27001. Once identified, those controls can be located in the specific categories and subcategories associated with Cybersecurity Framework core functions: Identify, Protect, Detect, Respond, and Recover. The security control mapping information can be useful to organizations that wish to demonstrate compliance to the CUI security requirements in the context of their established information security programs, when such programs have been built around the NIST or ISO/IEC security controls.

NIST 800-171 at vii; Appendix D at D-1; see Cybersecurity Framework Draft Version 1.1, available at *www.nist.gov/cyberframework/draft-version-11* (note: Comments on the proposed updates in version 1.1 are due by April 10 and should be sent to *cyberframework@nist.gov*).

Compliance Matrix/Plan of Action: As discussed in Part 1, supra, a compliance matrix is a useful tool for tracking what has been done and what is being done for each security control. The matrix should address how the controls are implemented by the contractor, e.g., "*What mechanisms does the company employ to ensure requirement [XX] is properly implemented and sustained?*" A thorough compliance matrix can help guide the contractor through the compliance process, and is an accessible tool to provide to the Government if questions about the contractor's compliance arise. For security controls or mitigation actions not yet implemented, NIST SP 800-171 provides that contractors should create plans of action. NIST SP 800-171, 3.12.2.

- Plan of Action and Milestones—Contractors may look to the plan of action and milestones developed under FedRAMP or other Government programs for guidance in drafting a solid compliance matrix. These plans of action and milestones are likely to be familiar to many Government customers and, thus, more likely to be accepted as evidence of a viable compliance approach. See, e.g., DSS Job Aid: POA&M, available at *www.dss.mil/documents/rmf/Plan_of_Action_and_Milestones_POAM_Job_Aid.pdf.*

Security Assessment Report/Report of Compliance: Contractors can benefit from creating a comprehensive report on the methodology employed for determining security compliance. As noted above, under FedRAMP, the report should include consideration of risks and contractor vulnerabilities as well as corrective action plans. If a third-party auditor is used, a report of compliance from the auditor (even if not required or given "credence" by DOD) adds to the contractor's compliance arsenal and can bolster credibility if there are any security issues. If a DOD contractor feels a control is inapplicable, or an adequate alternate exists, the contractor may provide a written explanation, which will be presented to the DOD CIO and adjudicated.

> The rule allows for the contractor to identify situations in which a required control might not be necessary or for an alternative to a required control. In such cases, the contractor should provide a written explanation in their proposal describing the reasons why a control is not required or adequate security is provided by an alternative control and protective measure. The contracting officer will refer the proposed variance to the DoD CIO for resolution. The DoD Chief Information Officer (CIO) is responsible for ensuring consistent adjudication of proposed non-applicable or alternative security measures.

See DOD FAQs at A18, A19. There is no guarantee an alternate will be approved, however, and the proposal could be deemed noncompliant for failure to meet requirements and be ineligible for contract award. Documentation and a clear rationale for contractor assessments (whether demonstrating compliance or asserting a certain control does not apply) are key. Contractors should be proactive and include this information in their compliance matrices and compliance reports, and should inform the customer as soon as possible to allow for resolution of any issues.

Third-Party Audits—Although DOD will not require a third-party assessment or certification under the DFARS rule, and will not regard such an assessment or certification as determinative, engaging a third party to assess and audit your systems can be beneficial, particularly where it leads to an independent finding that your systems have adequate security controls, and your processes and plans are sufficient.

An auditor can review the contractor's current level of compliance, provide a gap analysis, assist in generating solutions and provide documentation confirming contractor compliance. A third-party auditor also may be able to facilitate use of penetration testers—individuals who will attempt to gain access to your systems to test whether appropriate security controls are in place *prior* to beginning an audit. (For movie fans among you, think of Robert Redford's team in *Sneakers*.) Contractors may also consider licensing third-party tools that will set systems within a specific compliance framework for testing.

- ***Practitioner's Note***: If you choose to bring in penetration testers, these individuals should *not* be the same team you hire for the audit. To preserve the final report's integrity, there needs to be an arms-length distance from the final audit team. Additionally, consider having outside counsel retain the penetration testers so that their findings may be protected as attorney work product.

Because third-party audits are typically longer than a self-assessment, it is important to determine as soon as possible whether your company will use a third-party auditor. As noted in Part 1 of this series, experts estimate that an assessment could take between three to six months for a contractor with 600 employees and 30 servers (located within the contiguous U.S.). However, timing can be negotiated depending on how many resources the auditor can bring to bear during the requisite time period, and how much the contractor is willing to pay.

Pre-Audit Considerations—Before beginning an audit (either a self-assessment or a third-party audit), the contractor should conduct a thorough review to define the applicable contractor systems and security standards for the audit, and a security assessment plan should be created. As noted above, contractors may be subject to more than just the security controls in NIST SP 800-171 under the DFARS rule, and 2017 is a good time to ensure the sufficiency of controls and compliance under all applicable regimes. Also, it is important to review applicable contracts to ensure customers do not specify additional controls.

Even where the contractor identifies the systems to be audited, the contractor should review this finding with the auditor. According to Christopher Pogue, a veteran third-party auditor and chief information security officer (CISO) at Nuix, an international cybersecurity software company, "nine times out of ten the contractor is unclear about which systems actually house data that should be included."

What should contractors look for when hiring a third-party auditor? Neither the regulation nor the NIST standard specifies a standard for auditors. In fact, DOD's frequently asked questions make it clear that the agency is taking a hands-off approach in this regard. According to Pogue, "The most important considerations are who will have 'fingers on the keyboard' during the audit, and what is that person's experience?"

Aside from having an information technology degree (or the equivalent), it is recommended that auditors have between three to five certifications, such as Certified Information Systems Security Professional, GIAC Security Essentials Certification (entry-level certification), Certified Information Systems Auditor, and Certified Ethical Hacker (pen-testing techniques and technologies). Finally, the terms of the third-party auditor agreement should include data protection clauses, a nondisclosure agreement, and terms that clearly define the scope of the audit (with potential room for expansion if the auditor determines that additional scope is necessary).

The Audit—Although each audit is unique, below are common steps in an audit that contractors should anticipate.

1. The audit leader (or audit mediator) will meet with you to discuss goals, explain the audit process and identify how long it should take.
2. The audit team will ask a series of questions about the nature of your business, the com-

puter systems, data dispensation and the business processes. These questions help the team determine whether all areas of your network have been appropriately included within the scope of the audit.

3. The team will audit your system against specific controls. The team will ask you to show it specific aspects of your system and processes, which requires the appropriate personnel within your organization to be available and responsive to facilitate the audit. Note: Your team should be prepared to explain if there are "compensating controls" in place (i.e., alternate but equally effective controls).
4. The audit team will compile a report on its findings (sometimes known as a report of compliance) that establishes what systems were audited and that the systems were compliant as of the date of the assessment.
5. If there are any noncompliances or deficiencies identified, you should communicate a date by which you will get the issue fixed so that the final report can reflect that you are compliant. The auditor will reassess and issue the final report.

If shortcomings are too complex to correct before the audit is complete, the contractor's CISO should document these items in a compliance matrix—or plan of action—and develop a roadmap for achieving

Table 1: NIST SP 800-171 (Rev. 1): Security Controls Warranting Specific Documentation

Control Family	Security Control		
AUDIT & ACCOUNTABILITY	Basic	3.3.1	Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.
	Derived	3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
	Derived	3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.
CONFIGURATION MANAGEMENT	Basic	3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
	Basic	3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.
	Derived	3.4.3	Track, review, approve/disapprove, and audit changes to organizational systems.
	Derived	3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
INCIDENT RESPONSE	Basic	3.6.2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.
SECURITY ASSESSMENT	Basic	3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
	Basic	3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
SYSTEM & INFORMATION INTEGRITY	Basic	3.14.1	Identify, report, and correct information and system flaws in a timely manner. ***Note**: This is the only documentation requirement that correlates to one of the 15 "basic" requirements for safeguarding Federal contract information under FAR 52.204-21.*

compliance. The matrix provides critical documentation if an issue ever emerges later regarding whether the contractor took reasonable steps to remedy deficiencies in a timely manner.

Post-Audit Considerations—After the audit is complete and the final report is on file, congratulations—time to "Netflix and chill" with a few of those Oscar-winning movies you missed, right? WRONG! "Security is not a destination, it's the beginning," explains Nuix's Pogue. He cautions clients:

> The problem inherent to any compliance regime is that people assume that if every box is checked, they are secure. However, you cannot check-box your way to security. You have an enemy that is proactive—spending between 1-5 hours per week improving their craft—and you need to match their enthusiasm. This requires preemptively "threat hunting" and "proactive forensics."

Nuix's "The Black Report 2017: Decoding the Minds of Hackers" identifies a few alarming statistics in this regard. Of the penetration testers and hackers interviewed:

- *88 percent* could compromise a target *in less than 12 hours*, and *81 percent* said they could identify and exfiltrate your data *in less than 12 hours*.
- *50 percent* changed their attack methodologies *with every target*.
- *64 percent* said their biggest frustration was that organizations did not fix the things they knew were broken.

An effective compliance program is required to ensure not only that you currently satisfy the security requirements, but that you *continue* to satisfy them. While DOD currently has no intention of auditing contractors for compliance, that may not always be the case.

For example, HHS has only recently implemented audits for HIPAA compliance. Contractors who implement robust compliance plans should be less likely to see their proposals deemed noncompliant with cybersecurity requirements, or their contracts terminated for lack of adequate security. Documentation identifying compliance with contractor controls, including a report from a third-party auditor, can prove to be useful evidence in the face of any Government inquiries.

Conclusion—The age-old adage that you should not put off until tomorrow what you can do today was never truer. Like a healthy lifestyle, cybersecurity is not a destination—it is a journey. Some days you meet all of your goals, other days you uncover an area that needs improvement. Organizations must understand and embrace the fact that cybersecurity is not a static process—it encompasses prevention *and* continuous improvement.

✦

This Feature Comment was written for The Government Contractor by* John Chierichella, Laura Jehl, Townsend Bourne *and* Melinda Biancuzzo. *Mr. Chierichella is a partner in the Washington, D.C. office of Sheppard, Mullin, Richter & Hampton, a member of the firm's Government Contracts, Investigations, and International Trade practice group, and co-leader of the firm's Aerospace and Defense Industry team. Ms. Jehl is a partner in the Washington, D.C. office of Sheppard, Mullin, Richter & Hampton, a member of the firm's Business Trials practice group, and leader of the firm's Cybersecurity and Privacy team. Ms. Bourne and Ms. Biancuzzo are associates in Sheppard Mullin's Washington, D.C. office and members of the Government Contracts, Investigations, and International Trade practice group. They can be reached at jchierichella@sheppardmullin.com, ljehl@sheppardmullin.com, tbourne@sheppardmullin.com and mbiancuzzo@sheppardmullin.com, respectively. Special thanks to Christopher Pogue for his invaluable contributions to this article. Mr. Pogue is the chief information security officer at Nuix, an international cybersecurity software company, where he oversees all aspects of cybersecurity for the company. He also oversees the services organization, which performs Incident Response, Penetration Testing, Malware Reverse Engineering, and other security-related projects for external customers.