Published on *The National Law Review* https://natlawreview.com

DoD Issues Final Guidance for Assessing Contractor Compliance with NIST SP 800-171

Article By:

Susan B. Cassidy

Ian Brekke

The Department of Defense (DoD) recently issued final guidance for requiring activities to assess contractors' System Security Plans (SSPs) and their implementation of the security controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. A draft of this guidance was made available for public comment in April 2018. As noted in our original post on the draft guidance, DoD's proposed approach raised significant questions as to what role offerors' implementation of the security controls in NIST SP 800-171 would play in bid protests, contract performance, and post award audits. In the memorandum accompanying the final guidance documents, DoD notes that it has incorporated comments it received from the public into the final guidance. As discussed below, although the DoD has addressed some of the issues raised by the April draft, the final guidance adds some additional concerns and ambiguities.

The final guidance consists of two documents. The first document is "Guidance for Assessing Compliance of and Enhancing Protections for a Contractor's Internal Unclassified Information System," which provides direction to requiring activities for including evaluation criteria in solicitations and in contracts for assessing contractor compliance with NIST SP 800-171. The second document is "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented," which addresses how DoD should assess the impact and risk of NIST SP 800-171 security controls that a contractor has not yet implemented.

DoD components are "strongly encouraged" to implement the guidance.

Guidance For Assessing Compliance Of And Enhancing Protections For A Contractor's Internal Unclassified Information System (Compliance Guidance)

This document provides guidance to requiring activities for assessing contractor implementation of the security controls in NIST SP 800-171, both pre- and post-award. Although the Compliance Guidance does not provide explicit direction as to *how* DoD should conduct these assessments, it does reference NIST SP 800-171A with regard to the on-site assessments described below. NIST SP 800-171A provides a generalized framework for assessing compliance with NIST SP 800-171. DoD may draw from this document to help develop the criteria when using implementation of NIST

SP 800-171 as an evaluation factor.

Pre-Award. The Compliance Guidance addresses three objectives pre-award: (1) requiring a self-attestation of implementation of NIST SP 800-171 in all proposals; (2) imposing enhanced security controls beyond those in NIST SP 800-171 in certain situations; and (3) providing alternatives for using compliance with NIST SP 800-171 as an evaluation factor.

Self-Attestation. DFARS 252.204-7008, "Compliance With Safeguarding Covered Defense Information Controls," is required in every solicitation, except for those solely for the acquisition of commercially available off-the-shelf (COTS) items. When an offeror submits a proposal to DoD where DFARS 252.204-7008 was included in the solicitation, the offeror represents that "By submission of this offer, the Offeror represents that it will implement the security requirements specified by [NIST SP 800-171] that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017." DoD has interpreted "implementation" of NIST SP 800-171 as having a completed SSP and a plan of action and milestones (POA&M) for the relevant covered contractor information systems.

Enhanced Security Requirements. If a requiring activity believes that enhanced security controls are required beyond those in NIST SP 800-171, the Compliance Guidance provides direction for adding the requirements to a solicitation. The guidance does not define what constitutes "enhanced controls." NIST recently announced that it was developing a new appendix to NIST SP 800-171 in response to increased advanced persistent threats.[1] This appendix will provide additional optional security controls when contractors are handling very sensitive DoD information on their internal networks. It may be that these revisions are the enhanced controls referenced in the Compliance Guidance. However, the guidance does not specify any limitations on the security controls that DoD could impose contractually on contractors in specific instances.

Evaluation Factors. The Compliance Guidance also provides insight into how DoD will evaluate compliance with NIST SP 800-171, both pre-award as part of the source selection decision and post-award as part of contract performance. For pre-award evaluations, the Guidance lists four evaluative approaches. The first is a "Go/ No Go" criterion, which would require delivery of the contractor's SSP(s) and POA&M(s) to evaluate against criteria included in Section M as to what would be "acceptable." The second approach would rely on a separate technical evaluation factor, which would also require delivery of the SSP(s) and POA&M(s) with a more detailed description of how compliance would be judged in Section M. The third approach would be for DoD to conduct on-site assessments of the contractor's internal information systems using NIST SP 800-171A. Finally, contractors could be asked to identify Tier 1 suppliers[2] and their plans for flowing down the requirements of the DFARS Cyber Rule and for assuring subcontractor compliance.

Post Award. The Compliance Guidance envisions three post-award objectives: (i) delivery of the SSP(s) and POA&M(s) via a Contract Data Requirements List (CDRL) requirement; (ii) conduct of on-site assessments of a contractor's covered defense systems; and (iii) identification of CDI requiring protection under DFARS 252.204-7012, including at the subcontractor level.

Delivery of SSP and POA&M. The Compliance Guidance anticipates that the prime contractor's SSP and POA&M can be delivered as a CDRL and that DoD will incorporate these deliverables into the contract. Thus, a contractor's SSP arguably becomes a contractual requirement, as does the contractor's POA&M. Failure to comply with either could result in contract performance and/or breach issues. In addition, contractors must provide a SSP that meets the requirements of the Data Item Description (DID) that is included in the guidance. Consistent with previous DoD guidance, the

Compliance Guidance again notes that there is no prescribed format for the SSP or POA&M. However, the Data Item Description (DID) for the SSP requires a contractor to include specific information in the SSP that is similar to the SSP template that NIST includes on its website.

On-Site Assessments. The Compliance Guidance also envisions on-site assessments of a contractor's covered contractor information systems via contractual agreement. The scope, timing, and auditors for these assessments remain undefined. In June 2018, the DoD Office of Inspector General (OIG) announced it was conducting an audit at the request of the Secretary of Defense with the objective to "determine whether DoD contractors have security controls in place to protect the DoD controlled unclassified information maintained on their systems and networks from internal and external cyber threats." Numerous contractors have received notice from the DoD OIG that they would be subject to such an audit. These OIG audits may be the template for the audits addressed in the Compliance Guidance.

Identification of CDI Including Tier 1 Suppliers. The Compliance Guidance provides that DoD must identify CDI that requires protection by references in the SOW and require prime contractors to identify which Tier 1 suppliers will be receiving or developing CDI in performance of their subcontracts. The DID included in the Compliance Guidance requires prime contractors to do the following for each Tier 1 supplier: (i) provide basic identification information, (ii) verify that it has flowed down the substance of DFARS 252.204-7012 to the supplier, as well as any additional security requirements; (iii) state whether the supplier has done a self-assessment in accordance with NIST SP 800-171A; and (iv) provide a copy of the supplier's SSP(s) and POA&M(s). Given the sensitivity of this information and the competitive nature of the defense industry, this last requirement for production of an SSP and POA&M is likely to cause significant concerns among contractors that often compete in one program only to team in another.

DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented (Impact Guidance)

Whereas the Compliance Guidance focuses on evaluating a contractor's level of compliance with the NIST SP 800-171 security controls, the Impact Guidance focuses on the "potential consequences" that could result if a specific security control is not yet implemented. DoD notes that the Impact Guidance should "not to be used to assess implemented security requirements, nor to compare or score a company's approach to implementing a security requirement."

The Impact Guidance eliminates the confusing NIST "Priority" and "DoD Value" columns that were present in the April draft. In their place are three columns. The first lists the NIST SP 800-171 security control. The second column is a description of the security impact if that control is not implemented. The third column is implementation guidance. As an example, for control 3.1.19 "Encrypt CUI [controlled unclassified information] on mobile devices and mobile computing platforms," the Impact Guidance describes the impact of non-implementation as putting "any CUI on the devices at risk for unauthorized access if there is a loss of control of the device." The implementation method is described as "Software." In addition, the implementation column sometimes includes DoD clarifying information to address requirements that are "often over-analyzed and/or misunderstood." For security control 3.1.19, DoD notes that cryptography used to protect the confidentiality of CUI must use modules tested and validated to meet FIPS 140-1 or -2 requirements. The implementation methods, however, do not appear mandatory as the guidance describes them as "approach[es] a company *might use* to implement the NIST SP 800-171 security requirements …." The Impact Guidance also recommends that if a contractor indicates that a control is not yet implemented that a requiring activity should consider "a follow-up to ensure the company

understands the requirement."

Impact on Contractors

Now that the deadline for implementation of NIST SP 800-171 is long past, DoD is seeking to assure itself that contractors are in compliance with those requirements. Under DFARS 252.204-7012, contractors are required to provide "adequate security," which includes ***"at a minimum"*** implementation of NIST SP 800-171. Given recent breaches of DoD data reported in the news, and the increased and evolving threat, DoD is looking even more carefully at how contractors protect its data and seeking to impose even greater security requirements. At a minimum, contractors should be reviewing their SSPs and POA&Ms for completeness and for how they would be viewed in a competitive procurement, as well as carefully reviewing solicitations and contract amendments to identify any new cyber-related requirements. Similarly, if DoD incorporates the SSP and POA&M into the contract, a failure to comply with either could be a breach of the contract. To the extent that either document is inaccurate or a contractor fails to comply with the requirements of its own SSP and/or POA&M, a contractor also opens itself up to false statements and false claim allegations.

---

[1] On October 18, 2018, NIST co-sponsored a "Controlled Unclassified Information Security Requirements Workshop" with DoD and the National Archives and Records Administration (NARA). Dr. Ron Ross, a NIST Fellow and one of the authors of NIST SP 800-171, announced this update during the conference.

[2] Both guidance documents refer to "Tier 1 suppliers" without defining that term. If Tier 1 is equivalent to "first-tier" as that term is used in other provisions of the DFARS, then it likely refers to those subcontractors with whom the prime contractor has direct privity for a particular prime U.S. Government contract.

National Law Review, Volume VIII, Number 333