Bloomberg BNA

Federal Contracts Report™

VOL. 106, NO. 9 SEPTEMBER 12, 2016

Cybersecurity

At first glance, the changes stemming from Revision 1 to the National Institute of Standards and Technology's Special Publication 800-171 seem few in number and modest in consequence. But Revision 1 has significance that merits recognition by government contractors and by federal agencies planning to use their acquisition tools to improve the protection of Controlled Unclassified Information when provided to or furnished by their contractors.

BNA INSIGHTS: NIST Proposes Requirements for System Security Plans

By Robert S. Metzger

Robert S. Metzger, rmetzger@rjo.com, heads the Washington, D.C., office of Rogers Joseph O'Donnell, PC, a boutique law firm specializing in public contracts. A frequent contributor to Federal Contracts Report, Bob was named a 2016 ''Federal 100'' awardee by Federal Computer Week for his contributions to cyber and supply chain security. This article reflects Mr. Metzger's personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated.

The National Institute of Standards and Technology (NIST) created Special Publication (SP) 800-171 specifically to protect Controlled Unclassified Information (CUI) in nonfederal information systems and organizations.[1] NIST SP 800-171 identifies 109 security safeguards in 14 families. These safeguards were developed to protect all forms of CUI, including the four types of Covered Defense Information (CDI) that are subject of cybersecurity regulations implemented by the Defense Department (DOD) in the Network Pen-

[1] National Institute of Standards and Technology, Special Publication 800-171, June 2015.

 ISSN 0014-9063

etration Defense Federal Acquisition Regulation Supplement.[2]

In August 2016, NIST released a proposed ''Revision 1'' to SP 800-171. [3] At first glance, the changes seem few in number and modest in consequence. Upon further examination, however, Revision 1 has significance that merits recognition by government contractors and by federal agencies planning to use their acquisition tools to improve the protection of CUI when provided to or furnished by their contractors.

SSPs and POAMs

The most important change is the addition of guidance on the use of system security plans (SSPs) and plans of action and milestones (POAMs) to ''demonstrate the implementation or planned implementation of CUI requirements by nonfederal organizations.''[4] Specifically, new guidance is added, as follows:

> Nonfederal organizations describe in a system security plan (SSP), how the CUI requirements are met or how organizations plan to meet the requirements. The SSP describes the boundary of the information system; the operational environment for the system; how the security requirements are implemented; and the relationships with or connections to other systems. When requested, the SSP and any associated plans of action and milestones (POAM) for any planned implementations or mitigations should be submitted to the responsible federal agency or contracting officer to demonstrate the nonfederal organization's implementation or planned implementation of the CUI requirements. Federal agencies may consider the submitted SSPs and POAMs as critical inputs to an overall risk management decision to process, store, or transmit CUI on an information system hosted by a nonfederal organization and whether or not to pursue an agreement or contract with the nonfederal organization.[5]

A new Basic Security Requirement is added to the SP 800-171 controls, under the Security Assessment family:

> 3.12.4 Develop, document, periodically update, and implement system security plans for organizational information systems that describe the security requirements in place or planned for the systems.[6]

With this addition, the number of requirements stated by SP 800-171 increases to 110. Should it remain in the final revision to SP 800-171, companies required by regulation to safeguard CUI will have the additional requirement of preparing a SSP.[7] Today, only DOD contractors who have CDI are subject to SP 800-171 requirements. However, the National Archives and Records Administration (NARA) is working to complete — perhaps this year — the final federal regulation to establish governmentwide requirements for designation and safeguards of all forms of CUI.[8] As explained in Rev. 1 to SP 800-171, NARA also plans to sponsor, in 2017, a single FAR clause to apply the requirements contained in the federal CUI regulation and SP 800-171 to all contractors (and to other nonfederal enterprises that are entrusted with CUI). Thus, within the foreseeable future, hundreds of thousands of entities that possess, use or transmit CUI will find themselves subject to federal requirements that they prepare a SSP and the accompanying POAM, which has the purpose, as explained in the Revision, to present ''associated plans of action and milestones (POAM) for any planned implementations or mitigations.''[9]

Considered from a holistic perspective, it makes sense that the federal government would expect nonfederal holders of CUI to prepare a SSP and a POAM. Indeed, the initial version of SP 800-171 could be characterized either as ''partially complete'' or even ''incomplete'' because it articulated required controls without explicit obligation for the affected enterprise to describe how it intends to satisfy the requirements or what actions or schedule will accompany those intentions.

This ''gap'' is illustrated by a feature of the Network Penetration DFARS. The Safeguarding clause obligates ''covered companies'' (those that hold CDI and have contracts subject to this DFARS clause) to conform to NIST SP 800-171, by no later than Dec. 31, 2017, *but* it also requires a contractor to notify the chief information officer of DOD within 30 days of contract award ''of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.''[10] Under the DFARS, therefore, an obligation

---

[2] *See* DFARS 252.204-7008, ''Compliance with Safeguarding Covered Defense Information Controls,'' December 2015; DFARS 252.204-7012, ''Safeguarding Covered Defense Information and Cyber Incident Reporting,'' December 2015.

[3] The proposed revision (Rev. 1, hereafter), is available at http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-171-Rev-1.

[4] *See* Rev. 1, ''Notes to Reviewers,'' at p. v.

[5] Rev 1, Ch. 3 (''Requirements''), at p. 8.

[6] Rev. 1, Requirement 3.12, at p. 14.

[7] *See* National Institute of Standards and Technology, Special Publication 800-18, Rev. 1, ''Guide for Developing Security Plans for Federal Information Systems,'' February 2006.

[8] NARA acts as the ''executive agent'' to produce a new Federal Acquisition Regulation, of general application, to govern designation, dissemination controls, and safeguards for all forms of ''Controlled Unclassified Information.'' *See* ''Controlled Unclassified Information,'' (Proposed Rule), 80 Fed. Reg. 26501, May 8, 2015. NARA maintains a ''Registry'' of CUI, which identifies 23 categories and 82 subcategories of CUI. ''Controlled Technical Information'' and ''Export Control'' are two of the 23 categories.

[9] The specific language proposed by NIST speaks to ''planned implementation or mitigations.'' Rev. 1, Ch. 3, at p. 8. This recognizes that some companies will need time to meet SP 800-171 requirements.

[10] DFARS 252.204-7012(b)(1)(ii)(A).

  FCR ISSN 0014-9063

now is in place to inform DOD of the ''fit'' and ''gaps'' versus SP 800-171 — but there was no requirement to articulate any plan to close those ''gaps,'' or commit to any schedule to get it done, or to document the accomplishment of future actions.

The government's interest in protecting CDI, as well as other forms of CUI, is an important national objective, reflecting years of painful experience with compromise of the confidentiality of sensitive and valuable unclassified federal information. While the federal government wisely has shown, through SP 800-171, a willingness to accommodate ''nonfederal'' methods to achieve security objectives, that does not mean the federal government can or even should entirely *trust* all contractors to provide security as they may promise by taking a contract with the Network Penetration DFARS or future FAR equivalent. Beyond the ''promise'' of the contractors, it is reasonable for federal agencies, at least for those procurements that implicate especially sensitive agency functions, to ask their contractors to document their security plan and to provide the milestones to demonstrate to their federal customers that confidence is justified.

Not all agencies and not all contracts present information security risks that will justify the active agency administration of contractor achievement of CUI cybersecurity obligations. However, an obligation to prepare SSPs and POAMs must be seen as a preparatory step to other actions, in the nature of federal assurance, oversight and even enforcement.[11]

Industry should consider how DOD components are obligated to apply security practices for DOD information systems. A key document is DOD Instruction (DODI) 8510.01, the ''Risk Management Framework'' (RMF).[12] The RMF describes six security steps:

- Categorize System
- Select Security Controls
- Implement Security Controls
- Assess Security Controls
- Authorize System, and
- Monitor Security Controls.

The RMF requires as well as a ''plan of action and milestones (POA&M) . . . to address known vulnerabilities'' of information systems.[13]

NIST SP 800-171, which describes the safeguards, works in conjunction with regulations, such as the Network Penetration DFARS, that impose SP 800-171 upon contractors by contract. As matters stand today, the combination of NIST SP 800-171 (present version) and the Network Penetration DFARS address the first two of the RMF security steps and requirement achievement of the third (''Implement Security Controls'') by no later than Dec. 31, 2017. *However, the combination of SP 800-171 and the Network Penetration DFARS contains no government requirement for assessment, authorization or monitoring.* No doubt, this ''forbearance'' reflects a considered decision, taking into account limited resources of both the government and its contractors, likely costs, and the potential difficulty of implementation across a universe of thousands of contractors. Yet, the same restraint is accompanied by risk, as (today) the government has neither the tools nor the method to obtain positive demonstration that contractors deliver the required security.

The new obligations, to prepare SSPs and POAMs, are significant because they will inform and enable the government to review the contractor's plans, if requested, and then assess whether the contractors have performed in accordance with those plans. This is explicitly anticipated by new language in Revision 1 to SP 800-171: ''Federal agencies may consider the submitted SSPs and POAMs as critical inputs to an overall risk management decision to process, store, or transmit CUI on an information system hosted by a nonfederal organization and whether or not to pursue an agreement or contract with the nonfederal organization.'' At the same time, it is important that NIST (or procuring agencies) clarify the requirements so that companies are not obliged to submit multiple SSPs and POAMs or held to different review standards by different agencies.

How Should Industry Respond?

Comments to the proposed Revision 1 to SP 800-171 are due Sept. 16, 2016.[14] Industry will face some difficult choices. There is no doubt that preparation of SSPs and POAMs will add to burden and expense, and there will be many companies in the DOD supply chain, and more generally among federal suppliers to civilian agencies, who will balk at these additional obligations. At the same time, the federal government has interests that are both legitimate and important in assuring that its contractors provide minimum cyber safeguards to protect the confidentiality of the many forms of federal CUI. All government contractors know that that ''responsibility'' is a fundamental prerequisite to receipt of contracts from the federal government. [15] Among the requirements of ''responsibility'' is that a contractor:

> Have the necessary organization, experience, accounting ***and operational controls***, and technical skills, or the ability to obtain them (including, as appropriate, such elements as production control procedures, property control systems, quality assurance measures, and safety programs applicable to materials to be produced or services to be performed by the prospective contractor and subcontractors).[16]

Contractor ''responsibility'' should be a dynamic concept, reflecting changes in the performance environment and contemporary risks. In the contemporary contracting environment, cybersecurity is essential to the

[11] At the same time, the composition of SSAs and POAMs should not impose excessive burdens or cost. In the Definitions, Rev. 1 defines a ''system security plan'' by reference to NIST SP 800-18. This is not the ideal reference to establish the content for a SSP, since SP 800-18 is intended for *federal* information systems. Companies should be permitted to choose their own form of SSP.

[12] DODI 8510.01, ''Risk Management Framework (RMF) for DoD Information Technology (IT),'' Mar. 12, 2014, incorporating Change 1, effective May 24, 2016.

[13] DODI 8510.01, at 3(i). To note, the RMF also states that ''[c]ontinuous monitoring capabilities will be implemented to the greatest extent possible.'' *Id.*, at 3(j).

[14] The NIST announcement advises that comments are to be e-mailed to sec-cert@nist.gov (Subject: ''Comments on Draft SP 800-171 Rev. 1'').

[15] FAR 9.104-1.

[16] FAR 9.104-1(e) (emphasis added).

business interests of commercial enterprises and to the mission fulfillment of government customers. It is in this context that Revision 1 to SP 800-171 should be understood.

  FCR ISSN 0014-9063