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

# Draft DoD Guidance on SSPs and NIST SP 800-171 – Impact on Bid Protests and Ongoing Contract Performance

Article By:

Susan B. Cassidy

Jason A. "Jay" Carey

Kayleigh Scalzo

On April 24, 2018, the Department of Defense (DoD) issued a Notice and Request for Comment on draft guidance that DoD proposes for assessing contractors' System Security Plans (SSPs) and their implementation of the security controls in NIST Special Publication (SP) 800-171. This includes assessments as part of source selection decisions and during contract performance. DFARS 252.204-7012 requires defense contractors to provide "adequate security" for networks where covered defense information (CDI) is processed, stored, or transmitted. Adequate security means, "at a minimum," implementing NIST SP 800-171. To demonstrate implementation or planned implementation of the security controls in NIST SP 800-171, contractors must describe in a SSP how the security requirements have been implemented and develop plans of action and milestones (POA&M) that describe how any unimplemented security requirements will be met.

DoD issued two draft guidance documents. The first, "Assessing the State of a Contractor's Information System," provides guidance to requiring activities on four objectives: (1) assessing the risks presented by a contractor's internal network in a pre-award setting by evaluating compliance with NIST SP 800-171; (2) assessing an offeror's implementation of security requirements in addition to the security controls imposed by NIST SP 800-171; (3) assessing implementation of NIST SP 800-171 after award as part of contract performance; and (4) confirming a contractor's self-attestation of compliance. For each objective, DoD sets forth, as applicable, the information that must be included in an RFP, how the source selection authority would evaluate the requirement, what resources are available for that evaluation, and the contract provisions that will be needed to implement the requirement during performance.

The second draft guidance document, "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented," was developed by DoD to "facilitate the consistent review and understanding of" SSPs and POA&Ms. In particular, the guidance is intended to help requiring activities assess the risks that a security control left unimplemented has on an information system and to prioritize which unmet controls should be addressed first. The document is not intended to assess the quality of a contractor's implementation or to assess a

company's approach to implementing a particular security requirement.

DoD will assess the risk of unimplemented controls by assigning a "DoD Value" for each security requirement ranging from 5 (highest impact on the information system and the highest priority for implementing ) to 1 (representing the lowest impact and priority for implementation). The priority ranking is tied to the priority codes that NIST assigns to the NIST SP 800-53 Revision 4 security controls that are used for government information systems and which form the basis for NIST SP 800-171. Finally, in the comments section of the matrix, methods of implementation – such as IT configuration, software, policy/process – are noted. An example of one security control within the assessment document is set forth below:

It is unclear how DoD will use this calculation either pre-award or during contract performance. Although the guidance provides contractors with some insight into how DoD views the security requirements of NIST 800-171, the guidance lacks sufficient clarity as to how DoD will use these assessments. Further explanation on their use would be beneficial to both DoD and its contractors.

## Impact on Contractors

**Bid Protests –** The guidance raises questions about what role offerors' implementation of NIST SP 800-171 — and their SSPs and POA&Ms — may play in bid protests. The first draft guidance document — "Assessing the State of a Contractor's Information System" — lists two alternatives for evaluating offerors' implementation of NIST SP 800-171 at the source selection stage: (1) making an acceptable/unacceptable determination based on implementation status (a "Go/No Go decision") or (2) evaluating implementation "as a separate technical evaluation factor." It also contemplates solicitations requiring protections beyond NIST SP 800-171.

In the pre-award context, prospective offerors may consider protesting solicitation terms where a solicitation's treatment of NIST SP 800-171 implementation is inconsistent with the objectives and approach laid out in the guidance. And in the post-award context, disappointed offerors may consider challenging their own exclusion or non-award — or the award to another offeror — where the agency's assessment of the protester's or awardee's implementation of NIST SP 800-171 is inconsistent with the guidance documents.

The viability and success of such protest grounds likely will depend on how DoD writes solicitations moving forward — particularly, whether and how it incorporates the guidance into solicitations — and whether DoD takes the position that its assessment of NIST SP 800-171 implementation is a matter

of contractor responsibility subject only to limited protest.

**Termination Risk** – To evaluate compliance with their SSPs and POA&Ms, the draft guidance states that solicitations and contracts must include contract data requirements (CDRLs) to "require delivery of System Security Plan and any Plans of action after contract award." Thus, the accuracy of the SSPs and POA&Ms and a contractor's follow through on its POA&Ms are crucial. By making the SSP and POA&M a contractual obligation, failure to comply may provide a basis for termination if actions are not completed or if the SSP does not accurately reflect the status of the contractor's information system security.

**DCMA Audits –** DoD has stated in various industry meetings and in its updated FAQs that as part of its audit function, DCMA will verify that the contractor has an SSP and POA&M. DCMA will not be charged with a technical assessment of the system security plan against the NIST 800-171 security requirements. It is unclear, however, whether DCMA would leverage any of this guidance in its review.

**False Claims Act** – The use of the SSP as an evaluation criterion and/or deliverable under a government contract, also could increase the potential risk of a False Claims Act violation. For example, if an SSP misrepresents a contractor's actual cybersecurity status, DoD may be able to bring an action based on fraud in the inducement. Although it would depend on the language in the solicitation and the particular facts, DoD may be able to establish that the actual cybersecurity status of a contractor's internal network was material to the Department's award decision. If DoD were successful in this argument, this could potentially put all earnings under the contact at risk.

Comments are due by May 31, 2018.



National Law Review, Volumess VIII, Number 115