AN A.S. PRATT PUBLICATION
DECEMBER 2017
VOL. 3 • NO. 12

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis®

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 3 **NUMBER 12** **DECEMBER 2017**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Heidi A. Litman at 516-771-2169
Email: ..... heidi.a.litman@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

Library of Congress Card Number:

ISBN: 978-1-6328-2705-0 (print)

Cite this publication as:

[author name], [article title], [vol. no.] PRATT'S GOVERNMENT CONTRACTING LAW REPORT [page number] (LexisNexis A.S. Pratt);
Michelle E. Litteken, GAO Holds NASA Exceeded Its Discretion in Protest of FSS Task Order, 1 PRATT'S GOVERNMENT CONTRACTING LAW REPORT 30 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

An A.S. Pratt® Publication

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2017–Pub.4938)

Editor-in-Chief, Editor & Board of Editors

PRATT'S GOVERNMENT CONTRACTING LAW REPORT is published twelve times a year by Matthew Bender & Company, Inc. For subscription information and customer service, call 1-800-833-9844. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to government contractors, attorneys and law firms, in-house counsel, government lawyers, and senior business executives. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher. POSTMASTER: Send address changes to *Pratt's Government Contracting Law Report*, LexisNexis Matthew Bender, 630 Central Avenue, New Providence, NJ 07974.

DOD Issues Further Guidance on Implementation of DFARS Cyber Rule

By Susan B. Cassidy and Calvin Cohen*

The Director of the Defense Pricing/Defense Procurement and Acquisition Policy recently issued guidance to Department of Defense acquisition personnel in anticipation of the December 31, 2017 date for contractors to implement the security controls of National Institute of Standards and Technology Special Publication 800-171. The authors of this article discuss the guidance, which represents a forward leaning approach to addressing industry concerns and questions with regard to the Defense Federal Acquisition Regulation Supplement Cyber Rule.

The Director of the Defense Pricing/Defense Procurement and Acquisition Policy ("DPAP") recently issued guidance[1] to Department of Defense ("DOD") acquisition personnel in anticipation of the December 31, 2017 date for contractors to implement the security controls of National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171. The guidance outlines (i) ways in which a contractor may use a System Security Plan ("SSP") to document implementation of NIST SP 800-171; and (ii) provides examples of how DOD organizations could leverage a contractor's SSP and related Plan of Action and Milestones ("POA&M") in the contract formation, administration, and source selection processes.

COVERED DEFENSE INFORMATION ("CDI")

The guidance states that DOD "must mark, or otherwise identify in the contract, any covered defense information that is provided to the contractor, and must ensure that the contract includes the requirement for the contractor to mark covered defense information developed in performance of the contract." Although the requirement for DOD to mark data provided to the contractor during performance is clear, the guidance is less clear as to information developed in performance of the contract. In particular, noting a "requirement for the contractor to mark" information developed during performance, without specifying which information needs to be marked (i.e.,

---

* Susan B. Cassidy is a partner at Covington & Burling LLP advising clients on the rules and regulations imposed on government contractors, with a special emphasis on the defense and intelligence sectors. Calvin Cohen is an associate in the firm's Government Contracts and Data Privacy and Cyber Security practice groups. The authors may be reached at scassidy@cov.com and ccohen@cov.com, respectively.

[1] http://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf.

specifying a particular Contract Data Requirements List ("CDRL") presents a compliance challenge and increases the opportunity for miscommunications between DOD and its contractors. The DOD's slides and statements at the June 2017 Industry Day were more explicit, noting that the DOD must

> [d]ocument in the contract (e.g., Statement of Work, CDRLs) information, including covered defense information, that is required to be developed for performance of the contract, and specify requirements for the contractor to mark, as appropriate, information to be delivered to DoD. (see, e.g., MIL-Handbook 245D, and Contract Data Requirements List (CDRL) (DD Form 1423)).[2]

Contractors may see additional clarification of this point in the Frequently Asked Questions that DOD is expected to issue soon. Otherwise, contracting personnel may take a narrow view of their responsibilities to identify CDI that will be developed during performance.

IMPLEMENTATION OF NIST 800-171 SECURITY CONTROLS

The guidance recognizes that NIST SP 800-171 provides latitude to contractors for how they choose to implement applicable security controls and for how contractors assess their own compliance with those requirements. DOD recognizes that compliance with NIST SP 800-171 involves both policy/procedures and technical controls. To the extent that a contractor seeks additional clarification as to the interpretation of NIST SP 800-171 security controls, the guidance points contractors to the corresponding NIST SP 800-53 security controls, as well as the 800-53 Supplemental Guidance.

DOCUMENTING COMPLIANCE WITH AN SSP

Under 252.204-7012(b)(2)(ii)(A), contractors "shall implement 800-171, as soon as practical, but not later than December 31, 2017." Key to that implementation is the 110th security control, which was added in Revision 1 to NIST SP 800-171. This control requires contractors to create an SSP, which "describe[s] the boundary of [a contractor's] information system; the operational environment for the system; how the security requirements are implemented; and the relationships with or connections to other systems."

At the June 23, 2017 Industry Day, DOD clarified that if a contractor is not in compliance with all 110 security controls by December 31, 2017, but has an SSP and POA&M that accurately reflect the status of its compliance with those

---

[2] *See* Cybersecurity Challenges, Protecting DoD's Unclassified Information, June 23, 2017 Industry Day at Slide 27, *available at* http://dodcio.defense.gov/Portals/0/Documents/Public Meeting-Jun 23 2017 Final.pdf?ver=2017-06-25-022504-940.

controls, that contractor has "implemented" 800-171 for purposes of the 7012 clause.[3] In the guidance, DOD further noted that in addition to a POA&M, the SSP should "describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems." DOD again noted that there is no required format for an SSP and that it may be separate or combined documents.

ROLE OF THE SSP AND POA&M IN CONTRACT FORMULATION, ADMINISTRATION, AND SOURCE SELECTION

Revision 1 to NIST SP 800-171 provides that federal agencies may consider a contractor's SSP and POA&Ms as "critical inputs to an overall risk management decision to process, store or transmit CUI [controlled unclassified information]" on a contractor's internal networks. Although not mandatory, agencies will be permitted to use implementation of NIST SP 800-171 as an evaluation criteria. The guidance notes the following examples:

- "Using proposal instructions and corresponding evaluation specifics" as to the implementation of NIST SP 800-171 to permit DOD to determine "whether it is an acceptable or unacceptable risk to process, store, or transmit" CDI on a contractor's system;
- "Establishing compliance with [Defense Federal Acquisition Regulation Supplement ("DFARS")] 252.204-7012 as a separate technical evaluation factor";
- Identifying any NIST SP 800-171 security requirements not implemented at the time of the award and including associated POA&Ms implementation; and/or
- "Identifying in the solicitation that all security requirements in NIST SP 800-171 must be implemented at the time of award."

Because contractors have objected that SSPs contain highly sensitive data about their networks, the guidance suggests that contracting officers incorporate the SSPs by reference as part of the contract. Thus, the accuracy of the SSPs and compliance with the POA&Ms are crucial because by incorporating these documents, DOD would make compliance with those documents a contractual obligation. This contractual obligation is further exacerbated by DFARS 252.204-7008, which provides that by submitting the offer, a contractor is representing that it has implemented the 800-171 security controls, including the requirement for an SSP.

---

[3] *See, id.,* Cybersecurity Challenges, Protecting DoD's Unclassified Information, June 23, 2017 Industry Day at Slide 46.

This guidance represents DOD's forward leaning approach to addressing industry concerns and questions with regard to the DFARS Cyber Rule. The next iteration of Frequently Asked Questions is expected soon and should provide further guidance to contractors.