AN A.S. PRATT PUBLICATION
MAY 2019
VOL. 5 • NO. 5

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis®

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 5 **NUMBER 5** **MAY 2019**

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.

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

MATTHEW BENDER

(5/2019–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, 646.539.8300. 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 Continues to Up the Ante on Cybersecurity Compliance for Contractors

By Susan B. Cassidy and Ian Brekke*

The Department of Defense's evolving cybersecurity requirements present new challenges to contractors that are still working to fully implement all 110 controls in National Institute of Standards and Technology Special Publication 800-171. The authors of this article discuss the issues and recommend that contractors update their subcontract forms and develop an approach for meeting the new requirements.

Compliance with the security controls in National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171 is only the beginning for contractors that receive controlled defense information ("CDI") in performance of Department of Defense ("DoD") contracts and subcontracts.

Faced with an evolving cyber threat, DoD contractors have experienced an increased emphasis on protecting DoD's information and on confirming contractor compliance with DoD cybersecurity requirements. This includes audits by the DoD Inspector General ("IG") "to determine whether DoD contractors have security controls in place" to protect CDI and enhanced security controls for certain high risk contractor networks. And, on September 28, 2018, the Navy issued a policy memorandum calling for enhanced cybersecurity requirements, including some that have generated opposition within the defense community such as the installation of network sensors by the Naval Criminal Investigative Service on contractor systems. Other requiring activities are reportedly requiring similar enhanced protections and NIST was expected to issue a revision to NIST SP 800-171 in the spring, with additional enhanced controls.

On November 6, 2018, the DoD issued final guidance to requiring activities for assessing contractors' System Security Plans ("SSPs") and their implementation of the security controls in NIST SP 800-171. Since then, DoD has issued two additional guidance memoranda; one that includes contractual language for implementing the November 6th guidance and one that explains how DoD

---

* 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. Ian Brekke is an associate at the firm advising clients on issues arising from their participation or connection to government contracting. The authors may be contacted at scassidy@cov.com and ibrekke@cov.com, respectively.

plans to confirm contractor oversight of subcontractor compliance with the Defense Federal Acquisition Regulation Supplement ("DFARS") 252.204-7012 cybersecurity requirements.

FAHEY MEMORANDUM

On December 17, 2018, Kevin Fahey, the assistant secretary of defense for acquisition, issued a policy memorandum,[1] which provides contractual language that requiring activities can use in conjunction with the November 6th guidance. This language addresses (i) access to and delivery of contractors' and subcontractors' SSPs (or extracts thereof); (ii) access to and delivery of a contractor's plan to track flow down of CDI to subcontractors and a restriction on unnecessary sharing/flowing down of CDI; and (iii) the requirement for a prime contractor to flow down (ii) and (iii) to its first-tier subcontractors. The added language is necessary because these requirements are not explicitly reflected in DFARS 252.204-7012.

One of the contractual excerpts addresses the submission of SSPs and Plans of Action and Milestones ("POA&M"). Although NIST SP 800-171 does address the production of the prime's SSP to the government, the DFARS cyber clause does not explicitly require it and it was not until the November 6th guidance that DoD indicated it would require delivery of subcontractors' SSPs and POA&Ms.[2]

Potentially problematic in the new contractual language is the requirement for the prime contractor to ensure government access to the SSP and POA&Ms of its first—and second-tier subcontractors, vendors and suppliers, given the sensitivity of this information and the competitive nature of the defense industry. Contractors will need to ensure that their subcontract, vendor and supplier forms cover this requirement.

The second excerpt covers the identification and tracking of CDI flowed down to first-tier subcontractors, vendors and suppliers. This language anticipates a "post-award" conference where the government and contractor will "identify and affirm marking requirements for all covered defense information." The language also contemplates that the post-award conference will address restrictions on unnecessary sharing or flow down of CDI. There is a requirement for contractors to track all CDI and "document, maintain, and provide to the government, a record of tier 1 level subcontractors, vendors, and/or suppliers who will receive or develop covered defense information" in

---

[1] https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA003377-18%20ASD(A)%20Signed%20Memo%20w%20attach.pdf.

[2] DFARS 252.204-7012 requires contractors to "implement" NIST SP 800-171.

performance of the subcontract. Each of these requirements must be flowed down to first-tier subcontractors, vendors, and suppliers.

Given the broad use of "subcontractor, vendor and supplier," it seems clear that DoD's focus is on any entity to whom CDI is provided in the performance of a DoD contract, regardless of whether that entity is defined as a subcontractor subject to the myriad of other procurement requirements. DoD is plainly concerned with the CDI being passed along and DoD's requirements for protecting that information from improper disclosure.

Again, the tracking and documentation requirements are beyond the current DFARS cyber clause requirements and contractor agreements with relevant subcontractors, vendors, and suppliers should be reviewed to confirm compliance in anticipation of this new requirement.

LORD MEMO

On January 21, 2019, Ellen Lord, the under secretary of defense for acquisition and sustainment, issued a second memorandum[3] focused on assessing contractor compliance with the DFARS cyber clause via audits of a contractor's purchasing system. Much like the DoD IG audits that many contractors have been subject to in the past few months, the intent of this guidance is to have DCMA "validate, for contracts for which they provide contract administration and oversight, contractor compliance with the requirements of DFARS clause 252.204-7012."

However, the memorandum states that this would be done as part of a review of a contractor's purchasing system in accordance with DFARS 252.244-7001. Because the need for a contractor purchasing system review is triggered when sales to the government are expected to exceed $25 million during the next 12 months (excluding certain firm fixed priced contracts and contracts for commercial items), it is unclear how contractors outside these parameters will be reviewed.

The DCMA review is focused on contractor oversight of its first-tier subcontractors. Pursuant to the memorandum, DCMA review will include the following:

- Review contractor procedures to ensure contractual DoD requirements for marking and distribution statements on DoD CUI flow down appropriately to their Tier 1 Level Suppliers.
- Review contractor procedures to assess compliance of their Tier 1 Level

[3] https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19%20TAB%20A%20USD(AS)%20Signed%20Memo.pdf.

Suppliers with DFARS Clause 252.204-7012 and NIST SP 800-171.[4]

Notably, there is no specific requirement in the DFARS cyber clause for documented procedures to flow down CDI to first-tier subcontractors. Nor is there any explicit requirement to assess compliance of first-tier subcontractors with the DFARS cyber clause. These requirements, however, will ostensibly be imposed by the new contractual language that appeared in the December 17 Fahey memorandum.

IMPACT ON CONTRACTORS

DoD's evolving cybersecurity requirements present new challenges to contractors that are still working to fully implement all 110 controls in NIST SP 800-171. Although DoD will rightfully note that the DFARS cyber clause requires contractors to provide "adequate security" and that compliance with NIST SP 800-171 is the minimum requirement, the reality is that the ever-changing approach and the use of guidance issued in a piecemeal fashion has the potential to cause more confusion rather than less. Contractors will need to update their subcontract forms and develop an approach for meeting these requirements, as they are likely to begin appearing in solicitations and DCMA will be expanding its review of contractor purchasing systems with the above requirements.

---

[4] Neither the November 6 guidance nor the January 21 Lord memorandum define "Tier 1 Level Supplier," but from the context of the December 17 Fahey memorandum it appears that DoD intends it to be interpreted broadly to include first-tier subcontractors, vendors, and other suppliers.