AN A.S. PRATT PUBLICATION
JUNE 2019
VOL. 5 • NO. 6

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis®

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 5 NUMBER 6 JUNE 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

(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.

Senate Armed Services Subcommittee on Cybersecurity Holds Hearing to Discuss the Responsibilities of the Defense Industrial Base

By Susan B. Cassidy, Samantha L. Clark, Zachary Mears, and Weiss Nusraty*

The authors of this article report on a recent Senate Armed Services Subcommittee on Cybersecurity hearing where testimony was given on how the Department of Defense's cybersecurity policies and regulations have affected the Defense Industrial Base.

The Senate Armed Services Subcommittee on Cybersecurity recently held a hearing to receive testimony assessing how the Department of Defense's ("DoD") cybersecurity policies and regulations have affected the Defense Industrial Base ("DIB").

THE HEARING

To gain a better understanding of the DIB's cybersecurity concerns, the Subcommittee invited William LaPlante, Senior Vice President and General Manager of MITRE's National Security Sector; John Luddy, Vice President for National Security Policy at the Aerospace Industries Association; Christopher Peters, Chief Executive Officer of the Lucrum Group; and Michael MacKay, the Chief Technology Officer of Progeny Systems Corporation.

In their opening remarks, the Chairman of the Subcommittee, Senator Mike Rounds (R-SD), and Ranking Member Joe Manchin (D-WV) acknowledged industry concerns about the DoD's lack of clarity and disparate implementation of cybersecurity regulations, such as guidance relating to DFARS 252.204-7012 ("DFARS Cyber Rule" or "Rule") and National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171.

Senator Rounds stated that he "expects [DoD] to come up with measured policies to make improvements in [cybersecurity]" and he "hope[s] DOD takes

---

* Susan B. Cassidy (scassidy@cov.com) is a partner at Covington & Burling LLP advising clients on the complex rules and regulations imposed on government contractors, with a special emphasis on the defense and intelligence sectors. Samantha L. Clark (sclark@cov.com) is special counsel practicing in the firm's Public Policy, CFIUS, and Government Contracts groups. Zachary M. Mears (zmears@cov.com) is a senior advisor at the firm helping companies in the aerospace, defense, and national security sector navigate policy and regulatory challenges. Weiss Nusraty (wnusraty@cov.com) is an associate at the firm advising clients on cybersecurity and national security matters.

seriously the concerns of the DIB." He further noted that DoD "cannot simply apply increasingly stringent cybersecurity requirements on its contractors" and that "doing so without subsidy or assistance is unlikely to particularly improve cybersecurity [for] the DIB" and would likely drive the most innovative small businesses out of the supply chain. Senator Rounds called for putting a program in place to ensure the best possible protections for contractors regardless of size and referred to the "Achilles heel" of this issue as the desire to use a large number of small contractors while still needing to protect sensitive government information. Later in the hearing, Senator Manchin expressed great concern over the cyber incidents experienced by DoD contractors and urged the witnesses to "tell [the Subcommittee] what you need . . . [the Subcommittee] is here to fix it and you're here to tell us what's broken."

KEY POINTS

Summarized below are key points discussed during the hearing:

- *Clear, Scalable, and Consistent Cybersecurity Policy*: Witnesses representing the DIB agreed that the future of the defense industry is dependent on robust cybersecurity and, to that end, expressed the need for DoD to clarify critical aspects of existing policy. For instance, the identification and definition of Controlled Unclassified Information and its subset, Covered Defense Information ("CDI") was highlighted as an area of concern. DIB witnesses testified that the current definition of CDI in the DFARS Cyber Rule has become very broad. They suggested that DoD collaborate with the DIB to identify critical information so contractors are not protecting mundane data, but focusing on securing truly sensitive information. John Luddy noted that "with limited resources, if [contractors] try to protect everything that is currently considered CDI, we may under-protect the really important things."
- *Unified DoD Approach*: All of the witnesses emphasized the need for DoD to take a unified approach to cybersecurity that helps to minimize the burden on industry. The industry witnesses were clear that, together with large prime contractors, DoD can help support the middle and lower-tier suppliers to be cyber secure, but clear guidance and programs must first be in place. Currently, DoD has taken an "ad hoc, service-by-service" approach as it works towards developing actionable regulations that has resulted in segmented and overlapping contractor infrastructure, and increased costs. The DIB witnesses commended recent memoranda issued by Ellen Lord, the Under Secretary of Defense for Acquisition and Sustainment, that clarified requirements for contracts overseen by the Defense Contract Management Agency, but they also noted that the memoranda "raised issues that need to be

collaboratively assessed." The witnesses made plain the need for more opportunities to contribute to future standards and guidance by DoD.

- *Measuring and Certifying Cybersecurity Compliance*: The DIB witnesses highlighted the numerous NIST SP 800-171 controls and the need to develop an approach using "real, objective metrics" that helps industry measure their cybersecurity performance against those controls. Defense contractors have been frustrated with the lack of clear metrics for compliance, which has resulted in the perception of DoD's uneven enforcement of standards. The witnesses urged DoD to adopt a standard interpretation of NIST SP 800-171 as a useful baseline and starting point. They would prefer that DoD "set the bar high and set it once to hold all [companies] accountable, not only to spare companies from the cost, but also the need to adjudicate between different and potentially conflicting direction."
- *Information Sharing*: The witnesses also drew attention to the need for greater information sharing. One idea raised by the DIB witnesses included the formation of a centralized DoD threat sharing initiative that distributes relevant and timely data to the DIB to bolster cybersecurity efforts. The representatives acknowledged the tension between information sharing that is aimed at identifying and addressing threats and information that is competitive or business sensitive. But, there was a consensus that progress on information sharing has been made within the DIB and that further improvements would be welcome.

Throughout the hearing, members of the Subcommittee and representatives from the DIB seemed to agree that greater collaboration with DoD on contractor cybersecurity issues and supply chain issues would be necessary to address systemic concerns. While there was a broad focus on DFARS requirements and NIST SP 800-171, a number of related issues were raised with the goal of helping businesses prioritize investments and meet DoD's cybersecurity standards. As the cybersecurity efforts by DoD and the DIB continue, there was consensus during the hearing for a considered approach to partitioning cybersecurity responsibility among DoD, prime contractors, and their subcontractors so that no single entity shoulders the entire burden.