AN A.S. PRATT PUBLICATION
MARCH 2017
VOL. 3 • NO. 3

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis®

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 3 **NUMBER 3** **MARCH 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
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) 487-3000
Fax Number . . . . . (518) 487-3584
Customer Service Web site . . . . . 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 . . . . . (518) 487-3000

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.

More Cybersecurity Changes Expected for Contractors in 2017

By Susan B. Cassidy and Anuj Vohra*

The authors of this article highlight some of the key regulatory actions taken in 2016 to further the goal of protecting government data from cyber-attacks and describe the government's cybersecurity focus for the year ahead.

In 2016, the dangers presented by an increasingly digital world clearly were on display. A cyber-attack using an army of "Internet of Things" devices interfered with the operations of major commercial websites. And the U.S. Presidential Election was plagued with allegations of state-sponsored cybersecurity hacking (for which the Obama Administration issued sanctions against the Russian government). Cybersecurity threats are unlikely to cede the spotlight in the coming year. Indeed, Marcel Lettre, the former Undersecretary of Defense for Intelligence recently described cybersecurity as a "political, economic, diplomatic and military challenge" that is "evolving and growing more acute over time."[1]

As repositories for some of the government's most sensitive data, contractors face increasing regulatory obligations for protecting that data from cyber-attacks. Highlighted below are some of the key regulatory actions taken in 2016 to further this goal. And, as described further below, cybersecurity remains a focus for the government for the year ahead.

KEY CYBERSECURITY REGULATORY ACTIONS OF 2016

Some of the key cybersecurity regulatory actions impacting contractors in 2016 included the following:

- On February 9, 2016, President Obama unveiled his Cybersecurity National Action Plan and two related Executive Orders, to "enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower

---

* 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. Anuj Vohra is special counsel in the firm's Government Contracts practice advising clients in a range of contracting issues during all stages of the procurement process and litigating bid protests before federal agencies. The authors may be reached at scassidy@cov.com and avohra@cov.com, respectively.

[1] https://www.defense.gov/News/Article/Article/1019404/intel-undersecretary-describes-cyber-threat-steps-to-combat-it.

Americans to take better control of their digital security."

- On May 16, 2016, the Federal Acquisition Regulatory ("FAR") Council issued a final rule adding a new subpart and contract clause (52.204-21) to the FAR "for the basic safeguarding of contractor information systems that process, store, or transmit Federal contract information." The rule imposed a set of 15 "basic" security controls for contractor information systems upon which "Federal contract information" transits or resides.
- On September 14, 2016, the National Archives and Record Administration ("NARA") issued a final rule, effective November 13, 2016, establishing cross-agency practices and procedures for safeguarding, disseminating, controlling, destroying, and marking Controlled Unclassified Information. This rule should pave the way for a final FAR clause that will impose contractor safeguarding requirements (and potentially cyber incident reporting requirements) across the government.
- On October 4th, the Department of Defense ("DoD") issued a final rule implementing mandatory cyber incident reporting requirements for DoD contractors and subcontractors that have "agreements" with DoD. The final rule also highlighted DoD's desire to encourage greater participation in the voluntary Defense Industrial Base cybersecurity information sharing program.
- On October 21, 2016, DoD issued a long-awaited, immediately effective final rule and revised Defense Federal Acquisition Regulation Supplement ("DFARS") clause imposing safeguarding and cyber-incident reporting obligations on defense contractors whose information systems process, store, or transmit covered defense information.
- On October 31, 2016, DoD issued a proposed rule[2] calling for the revocation of access and implementation of an initial disqualification process for contractors where DoD has "substantial and credible information" of export-control violations. As noted above, DoD contractors are required to report cyber incidents involving covered defense information. Because such incidents could involve export-controlled information, contractors have expressed concern that DoD may use them as a basis for disqualification. Hopefully, DoD will clarify this point in its final rule.

---

[2] https://www.federalregister.gov/documents/2016/10/31/2016-26236/withholding-of-unclassified-technical-data-and-technology-from-public-disclosure.

- On December 20, 2016, the National Institute of Standards and Technology ("NIST") published Revision 1 to Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.[3] The Revision added a new control requiring a System Security Plan ("SSP"), which must "describe 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." If requested, contractors will be required to provide the government with its SSP and any associated Plans of Action and Milestones ("POAM"). Federal agencies may consider the submitted SSPs and POAMs as critical inputs when deciding whether to award a contract that requires the processing, storing, or transmitting of CUI on a contractor information system.[4]

LOOKING AHEAD

The government's emphasis on cybersecurity demonstrated by all of the above also is apparent in the Fiscal Year 2017 National Defense Authorization Act ("NDAA"), which contains a number of cybersecurity-focused provisions. These provisions, which could impact contractors, include the following:

- Section 1647 requires the Secretary of Defense to establish an advisory committee to make recommendations for the protection of information and networking systems of cleared defense contractors, including "information security and cyber defense policies, practices, and reporting relating to the unclassified information and networking systems of defense contractors." The advisory committee will be composed of six to ten members appointed by the Secretary of Defense, split between government and industry representatives.
- Section 1650 requires the Secretary of Defense to submit "a plan for the evaluation of the cyber vulnerabilities of the critical infrastructure of the Department of Defense."
- Section 1652 requires the Director of the Defense Information Systems Agency ("DISA"), in consultation with the Pentagon's Acquisitions Chief, to develop a "strategic plan" for evaluating and testing the

[3] https://insidecybersecurity.com/daily-news/defense-bill-sets-strict-deadlines-trump-assess-vulnerabilities-deter-cyber-attacks.

[4] Notably, Rev. 1 of NIST SP 800-171 also indicated that the anticipated FAR clause that will apply to all federal contractors in protecting CUI (and presumably will impose NIST SP 800-171 safeguarding requirements government-wide) will not be issued until 2017.

"adequacy" of efforts for protecting DISA's IT systems. This plan must be updated every two years.

- Section 1654 requires the Secretary of Defense to report to Congress and the President on the "military and nonmilitary options" for deterring cyber-attacks by foreign governments and terrorist organizations. Among the topics in the report would be an integrated priorities list for cyber-deterrence capabilities. This portion of the report could provide contractors with insight into DoD procurement priorities as the Department seeks to shore up its cybersecurity capabilities and defenses.

The government's concerns about cybersecurity are also on display in its Unified Agenda of Federal Regulatory and Deregulatory Actions, published on December 23, 2016. In it, DoD identifies cybersecurity as one of its six priorities and indicates an intent to continue to sharpen its regulatory requirements in this area, including further revisions to its final rule regarding participation in its Defense Industrial Base program. Although the exact parameters of the changes that DoD will make in the cybersecurity area remain to be seen, DoD's significant emphasis on protecting its own systems should provide a warning to contractors about the importance that DoD and other government agencies place on the protection of government information—whether stored on government or contractor systems.