AN A.S. PRATT PUBLICATION
JULY 2018
VOL. 4 • NO. 7

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis®

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 4 NUMBER 7 JULY 2018

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

(2018–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.

A New GSA Effort to Regulate Contractor Cybersecurity

By Charles A. Blanchard, Ronald D. Lee, Nicholas L. Townsend, and E. Christopher Beeler*

The General Services Administration is planning to formalize cybersecurity rules for its government contractors. The authors of this article discuss the proposed rule and current rules, which provide guideposts on how the Administration may draft its proposed cybersecurity rules.

The General Services Administration's ("GSA") newest regulatory agenda[1] includes a plan to formalize cybersecurity rules for its government contractors. The anticipated proposed rule will impact a significant number of government contractors. Indeed, as recently as fiscal year 2016, 18,313 entities held GSA Schedules and received over $45 billion from government agencies.[2] The GSA's anticipated action follows years of an increased effort by the U.S. government to impose cybersecurity safeguard requirements on contractors, something this Advisory briefly summarizes below. Moreover, GSA rulemaking on this issue may create momentum to promulgate a Federal Acquisition Regulation ("FAR") rule to standardize the designation and treatment of Controlled Unclassified Information ("CUI") as required by the National Archives and Record Administration ("NARA") in its September 2016 final rule.[3] This rule, among other things, provides that the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171, "Protecting Controlled Unclassified Information Systems and Organizations," establishes the requirements for contractors to protect CUI. Not only does the GSA regulatory agenda specifically reference NIST SP 800-171 as part of the substantive requirements in its anticipated proposed rule, but a forthcoming FAR rule would also likely incorporate the NIST requirement.

---

* Charles A. Blanchard (charles.blanchard@arnoldporter.com), a partner at Arnold & Porter who previously served as the General Counsel of the Air Force and the Army, works with clients in the contracting and national security communities. Ronald D. Lee (ronald.lee@arnoldporter.com) is a partner at the firm representing clients in national security, cybersecurity and privacy, and government contracts matters. Nicholas L. Townsend (nicholas.townsend@arnoldporter.com) is counsel at the firm maintaining an international trade and national security practice. E. Christopher Beeler (chris.beeler@arnoldporter.com), an associate at the firm, practices at the intersection of national security, government contracting, and litigation.

1 https://www.gpo.gov/fdsys/pkg/FR-2018-01-12/pdf/2017-28236.pdf.

2 http://gsa.federalschedules.com/resources/gsa-schedule-sales-2016/.

3 https://www.gpo.gov/fdsys/pkg/FR-2016-09-14/pdf/2016-21665.pdf.

GSA's regulatory plan envisions an update to the General Services Administration Acquisition Regulation ("GSAR") that requires contractors to:

- Protect the confidentiality, integrity, and availability of unclassified GSA information and information systems from cybersecurity threats and vulnerabilities; and
- Report cyber incidents that could potentially affect GSA or its customer agencies.

The GSA will initiate a formal rulemaking process later in 2018, which will provide a formal public comments period for each proposed new rule.

BACKGROUND AND CURRENT CYBERSECURITY REQUIREMENTS

The stated mission of the GSA is to deliver the best value in real estate, acquisition, and technology services to the government and the American people. To do so, GSA plays the role of the centralized procurement arm for the federal government. GSA already imposes cybersecurity requirements on its contractors. For example, as of July 31, 2017, GSA issued an order[4] requiring that contractors responsible for managing personally identifiable information ("PII") and with access to federal information report all "suspected or confirmed breaches" of PII.

The current GSAR[5] makes contractors "responsible for information technology (IT) security, based on . . . GSA risk assessments, for all systems connected to a GSA network or operated by the Contractor for GSA, regardless of location."[6] Other requirements include the submission of an IT Security Plan to the Contracting Officer. The IT Security Plan must currently "describe the processes and procedures that will be followed to ensure appropriate security of IT resources" developed and used for each particular contract. In addition, GSA contractors are required to develop a continuous IT monitoring strategy that includes:

(1) A configuration management process for the information system and its constituent components;

(2) A determination of the security impact of changes to the information system and environment of operation;

(3) Ongoing security control assessments in accordance with the organi-

---

[4] https://www.gsa.gov/directives-library/gsa-information-breach-notification-policy-92972c-cio.

[5] http://farsite.hill.af.mil/reghtml/regs/other/gsar/552237.htm#P259_45700.

[6] GSAR 552.239-71(a).

zational continuous monitoring strategy;

(4) Reporting the security state of the information system to appropriate GSA officials; and

(5) Compliance with NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

PROPOSED CYBERSECURITY REQUIREMENTS

GSA's current regulatory agenda states that it intends to expand the scope of current cybersecurity requirements on contractors by promulgating two new regulations.

First, GSA intends to propose a rule regarding Information and Information Systems Security that updates GSAR 552-239-70, Information Technology Security Plan and Security Authorization, and GSAR 552.239-71, Security Requirements for Unclassified Information Technology Resources. GSA envisions that the updated rule will "mandate contractors protect the confidentiality, integrity, and availability of unclassified GSA information and information systems from cybersecurity vulnerabilities and threats." This updated rule would likely flow down to the contractor compliance requirements with the Federal Information Security Modernization Act of 2014.

GSA has also said that this new rule will require that Contracting Officers include the applicable GSA cybersecurity requirements in statements of work in order to ensure compliance. In addition, the new rule may require that statements of work incorporate best practices for preventing cyber incidents. Finally, GSA's regulatory agenda demonstrates an intent to expand cybersecurity requirements to a contractor's *internal systems*, *external systems*, *cloud systems*, and *mobile systems*. Such an expanded mandate could require significant investment and overhaul of a contractor's current IT environment.

Second, GSA intends to propose a rule regarding Cyber Incident Reporting to update GSA Order CIO 9297.2[7] and to incorporate the order into the GSAR. As mentioned above, this order requires contractors to report all "suspected or confirmed breaches" of PII whether in electronic or physical form. But this proposed rule will likely expand cyber incident reporting to situations beyond breaches involving PII. For instance, GSA said that the proposed rule will require contractors to report any cyber incident where the confidentiality, integrity, or availability of GSA information or information systems are

[7] https://www.gsa.gov/directives-library/gsa-information-breach-notification-policy-92972c-cio.

potentially compromised, or where the confidentiality, integrity, or availability of information or information systems owned or managed by or on behalf of the U.S. government is potentially compromised. Such a proposed rule for GSA contractors would expand the scope of cyber incidents that require notification. The proposed Cyber Incident Reporting will also likely include authority for the government to access a contractor's information systems after a cyber incident. Other expected requirements include:

- Contractors must preserve images of infected or breached systems and may require mandatory employee training regarding cybersecurity.
- A cyber incident reporting clause in all GSA contracts and those orders placed against GSA multiple award contracts.
- A timetable for reporting cyber incidents.
- A delineation of roles and responsibilities regarding cyber incident reporting among GSA contracting officers, contractors, and the agencies ordering from a GSA contract.
- Rules regarding how the government will protect attributional information and a contractor's proprietary information provided in a cyber incident report.

GSA has indicated that the public comments period will open in August 2018 and close in October 2018.

These anticipated proposed rules would augment current cybersecurity rules already in place for government contractors. Moreover, current cybersecurity rules indicate potential requirements that GSA may likewise impose. For instance, where a contractor or subcontractor may have Federal Contract Information ("FCI") residing in or transiting through its information system, then Federal Acquisition Regulation 52.204-21 requires the contracting officer to insert the Basic Safeguarding of Covered Contractor Information Systems clause. This clause is meant to protect "federal contract information," which the FAR defines as "information, not intended for public release, that is provided by or generated for the Government under the contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public."

If applicable, the clause requires that the contractor and subcontractor apply 15 basic safeguarding requirements and procedures to protect the covered information systems. These requirements include, but are not limited to:

- limiting access to authorized users;
- limiting the functions of authorized users;

- authenticating or verifying users and devices prior to granting access to an information system;
- destroying FCI media prior to disposal;
- controlling physical access to information system equipment;
- monitoring and controlling organizational communications at the boundaries of the covered information system;
- maintaining virus protections; and
- performing periodic network scans.

Using these requirements as a touchstone, GSA could implement similar security requirements on GSA contractors.

Department of Defense FAR Supplement ("DFARS") clause 252.204-7012,[8] titled Safeguarding Covered Defense Information and Cyber Incident Reporting, also outlines certain cybersecurity requirements that GSA may find relevant. For example, DFARS 7012 requires that contractors provide "adequate security." This includes any network operated on behalf of the government, including cloud-based services and any other IT system. Further, DFARS 7012 incorporates the security requirements listed in NIST SP 800-171. Finally, DFARS 7012 also imposes a mandatory cyber incident reporting requirement, similar to the one GSA anticipates to include in its proposed rule. Under the DFARS rules, after discovery of a cyber incident, contractors must review for evidence of compromised covered defense information, must preserve and protect images of all known affected systems, and if requested, provide the Department of Defense with access to information.

These current rules provide guideposts on how GSA may draft its proposed cybersecurity rules. Contractors should begin compiling their compliance lessons learned from DFARS 7012, NIST SP 800-171, and FAR 52.204-21, so that lessons learned can be incorporated into comments to the proposed new rules.

---

[8] DFARS 7012; https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012.