AN A.S. PRATT PUBLICATION
DECEMBER 2018
VOL. 4 • NO. 12

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis®

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 4 NUMBER 12 DECEMBER 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.

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.

White House's New National Cyber Strategy: Dramatic Changes for Government Contractors

By Norma M. Krayem and Mary Beth Bosco*

President Trump recently unveiled a new National Cyber Strategy that centers on four pillars of priority. In addition, the U.S. Department of Defense rolled out a cybersecurity strategy which focuses on government contractors in the defense industrial base. The authors of this article explain these developments and the impact on government contractors.

President Donald Trump recently unveiled a new National Cyber Strategy[1] ("Strategy"). This Strategy follows the release of the May 2017 White House Cybersecurity Executive Order ("EO") 13800.[2] The EO addressed key issues and areas related to federal networks as well as a focus on critical infrastructure sectors.[3] Key U.S. Department of Homeland Security ("DHS") officials also rolled out the new cybersecurity strategy[4] at a recent State of Cybersecurity Conference. The new Strategy includes four main pillars of priority, including the need to:

- *Pillar I*: *Protect the American People, the Homeland, and the American Way of Life* by securing our information systems and combating cybercrime;
- *Pillar II*: *Promote American Prosperity* by pursuing cyberspace as an engine of economic growth, innovation and efficiency;

---

* Norma M. Krayem is a senior policy advisor at Holland & Knight LLP and chair of the firm's Global Cybersecurity and Privacy Policy and Regulation Team, as well as a member of the Public Policy & Regulation Group. She works on cybersecurity and privacy issues for global companies including those in the defense and critical infrastructure sectors and civilian and defense contractors. Mary Beth Bosco, a partner at the firm and a member of the Board of Editors of *Pratt's Government Contracting Law Report*, works with new and experienced government contractors, and focuses her practice on advising such organizations in contract compliance, transactional matters, and how to navigate the federal marketplace. The authors may be contacted at norma.krayem@hklaw.com and marybeth.bosco@hklaw.com, respectively.

[1] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[2] https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[3] https://www.dhs.gov/what-critical-infrastructure.

[4] https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/.

- *Pillar III*: *Preserve Peace through Strength* by identifying, countering, disrupting, degrading and deterring bad behavior in cyberspace; and
- *Pillar IV*: *Advance American Influence* by preserving the long-term openness, security and reliability of the internet.

IMPACT OF CYBER STRATEGY ON GOVERNMENT CONTRACTORS

The Strategy continues to reinforce the role of DHS in securing federal departments and agency networks, other than those run by the U.S. Department of Defense ("DoD") and U.S. Intelligence Community ("IC") systems. Pillar I includes two main areas of impact to government contractors—"Strengthen Federal Contractor Cybersecurity" and "Improve Federal Supply Chain Risk Management."

Under this first area, implementation of the National Cyber Strategy will affect federal contractors in important ways. It envisions a more proactive government role in assuring that contractors' information systems are adequately protected. The Strategy explicitly states that "The United States cannot afford to have sensitive government information on systems inadequately secured by contractors." It requires federal contracts to contain provisions authorizing the government to review contractor cyber protections by "testing, hunting, sensoring, and responding to incidents on contractor systems." It therefore contemplates government officials accessing and testing contractor systems, rather than its previous primary reliance on contractors to attest to the security of their systems. Present DoD and civilian agency contracts for the most part depend on contractors to evaluate and test their own systems, or use a third-party consultant. The Strategy focuses on "acute concerns" for defense-related contractors as well.

The Strategy also calls for the consolidation of cyber acquisition strategies to reduce the costs of utilizing contract provisions that differ from agency to agency. At present, DoD has its own cybersecurity regulations and contract clauses ("DFARS"), and individual civilian agencies supplement the Federal Acquisition Regulation ("FAR") cyber provisions with their own requirements. As this complex and sometimes conflicting set of requirements on federal contractors doing business with multiple agencies has been a significant compliance challenge, a more unified approach to cyber regulations and contract clauses may be a benefit to the contracting community.

The second area of importance for government contractors includes a focus on supply chain security. Supply chain security has been a growing risk and concern by the federal government for some time. The Strategy calls for the creation of a brand new "supply chain risk assessment shared service" that will centralize information about supply chain threats.

Of more direct relevance to federal contractors, the document requires implementation of new and "more streamlined" authorities to exclude risky vendors, products and services. It does not, however, specify whether these authorities will be in addition to, or integrated in, current debarment and suspension regulations. Federal contractors should monitor implementation of these provisions carefully as they could significantly impact how companies are excluded from the procurement process.

Certainly, any federal contractors who are also part of the 16 critical infrastructure sectors[5] will also find themselves subject to new cybersecurity priority action items, including where DHS and other federal agencies will lay out expectations on the private sector and where "[t]he Administration will develop a comprehensive understanding of national risk by identifying national critical functions . . . related to cybersecurity risk management."

DEPARTMENT OF DEFENSE ALSO ROLLS OUT NEW CYBERSECURITY STRATEGY

In addition to the White House National Cyber Strategy, the DoD also rolled out a cybersecurity strategy[6] that focuses on government contractors in the defense industrial base ("DIB"). The report explicitly states:

> Our focus working with DIB entities is to protect sensitive DoD information whose loss, either individually or in aggregate, could result in an erosion of Joint Force military advantage. As the Sector Specific Agency (SSA) for the DIB and a business partner with the DIB and DCI, the Department will: set and enforce standards for cybersecurity, resilience, and reporting; and be prepared, when requested and authorized, to provide direct assistance, including on non-DoD networks, prior to, during, and after an incident.

CONCLUSION

It is clear that both civilian federal contractors and defense-related contractors can expect a much more robust set of contracting standards and requirements than in the past.

---

[5] https://www.dhs.gov/what-critical-infrastructure.

[6] https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.