AN A.S. PRATT PUBLICATION
JULY 2019
VOL. 5 • NO. 7

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 5 NUMBER 7 JULY 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.

Significant Changes to Supply Chain Compliance

By Eric S. Crusius*

The 2019 National Defense Authorization Act and the SECURE Technology Act passed by the government demonstrate that supply chain compliance will grow in importance. The author of this article discusses the changes and advises contractors to take responsibility for supply chain monitoring and compliance or risk being excluded from doing business with the federal government.

The 2019 National Defense Authorization Act ("NDAA")[1] and a supply chain bill passed soon thereafter (the SECURE Technology Act[2]) foretell significant changes to how government contractors will be required to monitor their supply chains. The provisions include requirements to voluntarily disclose vulnerabilities, prohibitions on utilizing certain Chinese companies for contractor deliverables and the establishment of a new Federal Acquisition Security Council ("FASC") that will be able to recommend the exclusion of companies that pose an unreasonable supply chain risk.

SECTION 889 OF THE OF 2019 NDAA

Section 889 of the 2019 NDAA prohibits the procurement of certain technologies and services from companies connected with the People's Republic of China ("China"). Subsection (f)(3) lists the covered telecommunications equipment of services:

- Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).
- For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure and other national security purposes, video surveillance, and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company or Dahua Technology Company (or any subsidiary or affiliate of such entities).

---

* Eric S. Crusius is a partner at Holland & Knight LLP focusing his practice on a wide range of government contract matters, including bid protests, claims and disputes, compliance issues and sub-prime issues. He may be reached at eric.crusius@hklaw.com.

1 https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

2 https://www.congress.gov/bill/115th-congress/house-bill/7327/text.

- Telecommunications or video surveillance services provided by the above entities or using such equipment.
- Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country (which is China).

Section 889's prohibition is not as all-encompassing as it would seem at first glance because it is not absolute and does not cover all procurements. As noted in Subsection (a) of the provision, the prohibition only extends to situations where the covered equipment and services are a "substantial or essential component of any system, or as critical technology as part of any system." Because of that, there are situations where such equipment or services can be used. However, contractors should proceed with care: "substantial," "essential," and "critical technology" are not defined in Section 889 (though that may be subject to agency interpretation or further regulations).

Further, there is nothing in Section 889 that prohibits a contractor from using equipment from a covered company in its manufacturing process so long as the covered company's product is not included in the final deliverable to the government. In addition, there is nothing prohibiting a contractor from utilizing covered products and services outside of its supply chain directed at the U.S. government. Finally, as noted above, a covered product or service can even be an ancillary part of the deliverable to the government (though extreme caution should be used due to a lack of definitions). That being said, there may be other laws or regulations that restrict the use of materials or services impacted by Section 889. For instance, the SECURE Act, discussed below, will give agencies additional flexibility in excluding sources or particular products.

Contractors potentially impacted by this provision should consider whether covered products are in their supply chains and, if so, whether the products or services are (or could be) sold to the federal government.

The above will be effective on August 13, 2019 with respect to procured products and on August 13, 2020 with respect to covered services.

SECTION 881 OF THE 2019 NDAA

With respect to procurements involving national security systems (or IT that is purchased for inclusion within a national security system), Section 881 of the 2019 NDAA allows the U.S. government to shroud them in secrecy, elevates the importance of supply chain as an evaluation factor and limits bid protests challenging the determination that a procurement is covered under this

provision. "National security systems" are defined in 44 USC § 3542(b)(2)(A) to include, among other things, systems involving intelligence agencies, command and control of armed forces and equipment that is "integral" to a weapons system.

More specifically, with respect to covered procurements, this provision of the NDAA allows the government to:

- Exclude contractors that fail to meet certain standards defined by the agency;
- Exclude contractors that fail to achieve an "acceptable" rating in an evaluation factor concerning supply chain risk; and
- "Withhold consent" from a contractor's request to subcontract with an entity.

If the government acts against a contractor, a contractor is to be notified "only to the extent necessary to effectuate the covered procurement action." This language permits the government to withhold from the prime contractor the reason the subcontractor was excluded or not notify the proposed subcontractor at all. This provision will surely impact prime/subcontractor relations at some point.

OTHER NOTABLE PROVISIONS

A few other notable provisions in the 2019 NDAA impact supply chain management:

- *Section 252* authorizes up to $42,800,000 to be utilized by the Air Force on "nontraditional technologies and sustainment practices" to, among other things, increase availability of aircraft, decrease part manufacturing backlog reduce supply chain risk and "advance . . . additive manufacturing into the Air Force supply chain."
- *Section 843* establishes a pilot program "to test the feasibility and reliability of using machine-vision technologies to determine the authenticity and security of microelectronic parts in weapons systems." This pilot program began on April 1, 2019 and will run through December 31, 2020 and is being managed by the Undersecretary of Defense for Research and Engineering. Under this provision, the Undersecretary may consult with industry, including trade associations, manufacturers, nontraditional defense contractors, and federal laboratories.
- *Section 845* requires the Department of Defense to submit a report regarding the health of the defense electronics industrial base.

SECURE TECHNOLOGY ACT

Perhaps even more significant than the supply chain provisions in the NDAA was Congress' passage of the SECURE Technology Act in the final days of the

previous Congress. The SECURE Technology Act (which is short for the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act) is actually a combination of what had been two separate bills. The first part of the Act concerns the Department of Homeland Security's information and supply chain vulnerabilities while the second part concerns federal acquisition supply chain vulnerabilities and establishes a Federal Acquisition Security Council.

The SECURE Act offers important context to how the government is looking at supply chain issues in the 2019 NDAA. If followed faithfully, the Act will completely alter the way the government evaluates supply chain issues and whether to buy from certain contractors.

As noted above, Title II of the Act establishes the FASC. The FASC, which will be comprised of representatives from agencies across the Executive branch, will be chaired by a senior Office of Management and Budget official. The FASC will have wide-ranging responsibilities which include:

- Identifying and recommending which supply chain standards, guidelines and best practices should be addressed by NIST;
- Identifying executive agencies to provide shared acquisition services such as reviewing products and common contract solutions that would support "supply chain risk management activities"; and
- Developing criteria for sharing information among executive and non-executive Federal agencies, and non-federal agencies "with respect to supply chain risk."

Perhaps most significant, the FASC will create standards for excluding companies or products that pose an unreasonable supply chain risk. Following the creation of those standards, the FASC will utilize those standards to recommend the exclusion of sources or products from the supply chain. A recommendation can be challenged by a company that is the subject of an exclusion recommendations. After that process, exclusion or removal orders may be issued by: the Department of Homeland Security (for civilian agencies), the Department of Defense, and the Director of National Intelligence (for intelligence agencies and "sensitive compartmented information systems"). Any party that is subject to the exclusion or removal order must be notified of the decision and the decision to remove or exclude is required to be reviewed annually by the original exclusion official. This process standardizes and streamlines what some viewed as an ad hoc process that led to the removal of Kaspersky from the supply chain last year.

If company is on the receiving end of an exclusion or removal order, it may file a petition for judicial review with the U.S. Court of Appeals for the District of Columbia Circuit.

CONCLUSION

The recent actions by the government demonstrate that supply chain compliance will grow in importance in 2019. Contractors will need to take responsibility for supply chain monitoring and compliance or risk being excluded from doing business with the federal government.