AN A.S. PRATT PUBLICATION
JANUARY 2020
VOL. 6 • NO. 1

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 6 **NUMBER 1** **January 2020**

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)
ISSN: 2688-7290

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

(2020-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. Direct any editorial inquiries 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.

CISA Information and Communications Technology Supply Chain Risk Management Task Force Issues New Interim Report

By Susan B. Cassidy and Ryan Burnette*

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's Information and Communications Technology Supply Chain Risk Management Task Force recently released an interim public report describing the Task Force's efforts to develop recommendations for securing the government's supply chain, and outlining the potential focus areas of each of its working groups over the coming year. The authors of this article discuss the interim report.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's ("CISA") Information and Communications Technology ("ICT") Supply Chain Risk Management Task Force (the "Task Force") recently released an interim public report.[1] The report describes the Task Force's efforts over the last year to develop recommendations for securing the government's supply chain, and outlines the potential focus areas of each of its working groups over the coming year.

The report is particularly relevant to contractors that either sell ICT related products or services to the government, or that sell ICT related components to higher tier contractors, because it offers some insight into potential supply chain risk management ("SCRM") best practices, as well as requirements that the government may seek to impose on contractors in the future.

OVERVIEW OF THE TASK FORCE AND THE INTERIM REPORT

The Task Force was established in 2018 to provide a means to allow for "the collaboration of private sector owners and operators of ICT critical infrastructure" and to "provide advice and recommendations to DHS on means for assessing and managing risks associated with the ICT supply chain." It is chaired by CISA, the US Telecom Communications Sector Coordinating

---

* Susan B. Cassidy 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. Ryan Burnette is an associate at the firm advising clients on a range of issues related to government contracting. The authors may be reached at scassidy@cov.com and rburnette@cov.com, respectively.

[1] https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.

Council, and the Information Technology Sector Coordinating Council. Its members include 60 representatives from 17 different defense and civilian agencies that have been focused on assessing and protecting security vulnerabilities in their supply chains, including the Department of Defense, the Federal Bureau of Investigation, the Department of Justice, the Office of the Director of National Intelligence, and the National Security Agency. The Task Force also includes industry representatives across the information technology and communications sectors.

Collective actions of the Task Force have involved assisting with ongoing government supply chain efforts, including by coordinating with the Federal Acquisition Security Council and by providing input to the ICT criticality assessment contemplated by EO 13873.

The Task Force is divided into four working groups, each of which focuses on one of the following issue areas:

(1) Information Sharing;

(2) Threat Evaluation;

(3) Qualified Bidder Lists ("QBLs") and Qualified Manufacturer Lists ("QMLs"); and

(4) Policy Recommendations to Incentivize Purchase of ICT from Original Equipment Manufacturers ("OEM") & Authorized Resellers.

The efforts and status of the Task Force's working groups are generally summarized below:

- *Information Sharing Working Group*: This working group is tasked with "developing a common framework for the bidirectional sharing of actionable supply chain risk information across the community." To achieve this goal, the group focused on identifying the supply chain information that would be most valuable in mitigating risk, and assessing the barriers that might exist to accessing this information. The group identified inherent challenges with sharing potentially "derogatory" information, and has concluded that further legal guidance is needed to fully evaluate the risks of information sharing and how such risks can be mitigated.
- *Threat Evaluation Working Group*: This group has principally focused on developing an inventory of threats and cataloging the threats' sources and event descriptions. These threats have been divided into the same "threat group" categories discussed above. The working also created illustrative "threat scenarios" for ICT suppliers, intended to provide supporting guidance under various situations. The group noted

that in the coming year, it will continue to build these scenarios, and may expand more broadly to cover ICT products and services.

- *QBL & QML Working Group*: The group has focused on the appropriate use of Qualified Bidder Lists and Qualified Manufacturer Lists, working to identify how QBL and QML lists already are used in government procurement, developing factors for helping organizations determine when they should create their own QBLs or QMLs, and identifying use cases where QBLs and QMLs are appropriately leveraging SCRM criteria. The group has created an initial list of factors for when these types of QBL and QML can be used. These factors include addressing whether a product is commoditized, the relative importance of a product to an organization's mission, the relative level of control the organization can exhibit over its sources for products, and the existence of standards applicable to the article (e.g., ISO or NIST). Over the coming year, the group plans to finalize the factors for when these types of lists are appropriate.
- *Policy Recommendations for Purchase of ICT from Original Equipment Manufacturers or Authorized Resellers Working Group*: To achieve the working group's goal of developing recommendations, it has, among other things, looked at extending certain policy requirements of the DFARS 252.246-7007 (Contractor Counterfeit Electronic Part Detection and Avoidance System) clause to apply to civilian agencies. The group also developed a policy recommendation that ICT be purchased only from OEMs or from authorized resellers, and has made recommendations for defining the term "authorized reseller" to the Federal Acquisition Security Council. The group will shift its focus over the coming year to try and identify SCRM educational opportunities and develop standardized templates for vendors to describe or attest to their SCRM practices.

This year, the Task Force as a whole will continue to identify new topic areas for the working groups, and will look for further opportunities to coordinate with the Federal Acquisition Security Council.

IMPACT TO CONTRACTORS

Although the efforts of the Task Force to date have not yet resulted in immediate changes to official government procurement regulations or requirements, the efforts of the Task Force are informative to contractors, in part, for the following reasons:

- *Clear Commitment to Supply Chain Risk Mitigation Efforts*. The scope and scale of the questions being addressed by the Task Force confirms

the government's concerns with managing and securing its ICT supply chain. The activities of the Task Force, in combination with recent government measures such as the issuance of EO 13873 and the passage of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (the "SECURE Technology Act"), demonstrates that the government is focused on ensuring the security of its supply chain and that additional requirements for contractors are forthcoming in this space.

- *Involvement of Civilian Agencies*. The widespread representation from agencies, in addition to involvement from the National Security Council and the Office of Management and Budget, in the Task Force indicates that government attention in this space is not just limited to the Defense market. Indeed, one of the working groups has considered whether aspects of the DFARS counterfeit parts clause should apply more broadly than to just the Department of Defense. Thus, contractors with a relationship to the ICT industry that primarily do business in the civilian agency market should take note of the government's focus.
- *Best Practices*. At this relatively early stage, much of the efforts of the various working groups have appeared to focus on compiling best practices, including a lengthy list of various industry and government standards relating to supply chain risk mitigation in the ICT industry. This inventory of standards are categorized into nine "Threat Groups," including Cybersecurity, System Development Life Cycle ("SDLC") Processes and Tools and Insider Threats. These resources could prove helpful to contractors charged with designing their own SCRM programs.