PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 7 **NUMBER 10** **October 2021**

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.

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub.4938)

Editor-in-Chief, Editor & Board of Editors

Pratt's Government Contracting Law Report is published 12 times a year by Matthew Bender & Company, Inc. For customer support, please contact LexisNexis Matthew Bender, 9443 Springboro Pike, Miamisburg, OH 45342 or call Customer Support at 1-800-833-9844. 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, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. 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, 230 Park Ave. 7th Floor, New York NY 10169.

Recent Developments Under the Executive Order on Improving the Nation's Cybersecurity

By Susan B. Cassidy, Robert K. Huffman, and Ryan Burnette*

The authors discuss recent developments in connection with the Biden administration's cybersecurity order.

The Biden administration has issued an "Executive Order on Improving the Nation's Cybersecurity" ("EO").[1] Among other things, the EO sets out a list of deliverables from a variety of government entities. This article discusses a number of these deliverables that recently were due, including a definition of "critical software," the minimum requirements for a software bill of materials, and certain internal actions imposed on various federal agencies.

DEVELOPMENTS AFFECTING ENHANCEMENT OF SOFTWARE SUPPLY CHAIN SECURITY

Definition of Critical Software

Section 4 of the EO stated that the "development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors." The EO cites a "pressing need" for mechanisms to ensure the "security and integrity" of "critical software." The EO broadly defines critical software as "software that performs functions critical to trust" and tasks the Secretary of Commerce, through the National Institute of Standards and Technology ("NIST") to develop a definition of critical software that could be used in forthcoming regulations and guidance—including guidance required by the EO on identifying practices that enhance the security of the software supply chain.

---

* Susan B. Cassidy, a partner in Covington & Burling LLP, advises government contractors on compliance with the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement and conducts internal investigations when allegations of violations of those requirements arise. Robert K. Huffman, senior of counsel with the firm, represents defense, health care, and other companies in contract matters and in disputes with the federal government and other contractors. Ryan Burnette, an associate at the firm, advises defense and civilian contractors on a range of issues related to government contracting. Resident in the firm's office in Washington, D.C., the authors may be contacted at scassidy@cov.com, rhuffman@cov.com, and rburnette@cov.com, respectively.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

On June 25, 2021, NIST issued a white paper[2] providing a definition of critical software. The white paper followed a workshop that NIST held on June 2–3, 2021 with over 1,400 participants and 150 position papers submitted for NIST's consideration. In addition to private industry, NIST solicited input from the public as well as reportedly from several government agencies—including the Cybersecurity and Infrastructure Security Agency, the Office of Management and Budget ("OMB"), the Office of the Director of National Intelligence ("ODNI") and the National Security Agency—to help define what critical software means.

NIST's definition is broad and defines critical software as:

> any software that has or has direct software dependencies upon, one or more components with at least one of these attributes:
>
> - Software that is designed to run with elevated privilege or manage privileges;
> - Software that has direct or privileged access to networking or computing resources;
> - Software that is designed to control access to data or operational technology;
> - Software that performs a function critical to trust; or operates outside of normal trust boundaries with privileged access.

According to NIST, this definition preliminarily includes operating systems, web browsers, hypervisors, endpoint security tools, identity and access management applications, network monitoring tools, backup, recovery, and remote storage tools, and other categories of software.

In explaining the definition, NIST expressed its view that the EO's implementation "must take into consideration how the software industry functions, including product development, procurement, and deployment." Further, NIST explained that the term "critical" as used in the EO is not based not on the context of use, "but instead focuses on critical functions that address underlying infrastructure for cyber operations and security." Some limited use cases—such as software solely used for research or testing that is not deployed in production systems—are outside of the scope of this definition.

Finally, although the definition applies to all forms of software, NIST recommends that the initial EO implementation phase focus on standalone, on-premises software that has security-critical functions or poses similar

---

[2] https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf.

significant potential for harm if compromised. NIST indicated that later implementation of the EO could expand to other forms of software such as software that controls access to data, cloud-based and firmware to name a few.

OTHER DEVELOPMENTS

Software Bill of Materials Minimum Requirements

Section 4(f) of the EO requires the National Telecommunications and Information Administration ("NTIA") to publish the minimum elements of a Software Bill of Materials ("SBOM"), which the EO defines as "a formal record containing the details and supply chain relationships of various components used in building [the] software." In preparing to meet the July 11, 2021 deadline for publishing the minimum elements for SBOMs, NTIA issued a request for public comment[3] on the minimum elements for SBOMs and the factors that should be considered in requesting, producing, distributing, and consuming such items.

NTIA's request notes that an SBOM is similar to a "list of ingredients" and thereby promotes transparency in the software supply chain. NTIA proposed a definition of the minimum elements of an SBOM that encompasses three broad, inter-related features:

- Required data fields;
- Operational considerations; and
- Support for automation.

Data fields suggested include "supplier name," "component name," and "cryptograph hash of the component," among others. Operational considerations include a set of operational and business decisions and actions that establish the practice of requesting, generating, sharing, and consuming SBOMs, including "frequency," "depth," and "delivery." Automation support relates to whether the SBOM can be automatically generated and is machine-readable, which is "[a] key element for SBOM to scale across the software ecosystem."

Over 86 written comments were submitted in response to NTIA's request by the June 17, 2021 deadline for such comments.

Other EO Deadlines

The EO imposed other deadlines that may have been met, but for which there is no public access to the results. These included:

---

[3] https://www.federalregister.gov/documents/2021/06/02/2021-11592/software-bill-of-materials-elements-and-considerations.

- Section 2(g)(i) of the EO requires the Department of Homeland Security ("DHS"), in consultation with the Department of Defense ("DoD"), the Attorney General, and OMB, to recommend to the FAR Council contract language regarding the reporting of cyber incidents. The EO requires such contract language to identify:
  (1) The nature of the cyber incidents that require reporting;
  (2) The types of information that must be reported;
  (3) Appropriate and effective protections for privacy and civil liberties;
  (4) The time periods within which contractors must report cyber incidents based on a graduated scale of severity (with reporting of the most severe cyber incidents not to exceed three days from initial detection);
  (5) National Security Systems ("NSS") reporting requirements; and
  (6) The types of contractors and associated service providers to be covered by the proposed contract language. As of this writing, we have not yet been able to confirm whether DHS submitted any recommended contract language to the FAR Council or whether, if it did, what such language says.
- Section 7(c) of the EO requires DHS to provide OMB with recommendations on options for implementing an Endpoint Detection Response initiative to support proactive detection of cyber incidents. A senior Biden administration official publicly confirmed that DHS had provided such recommendations to OMB, but declined to state what those recommendations are.
- Section 7(g) of the EO requires NSA to recommend to DOD, ODNI, and the Committee on NSS by June 26, 2021, appropriate actions for improving detection of cyber incidents affecting NSS. Whether those recommendations have been issued has not been publicly disclosed as of this writing.