PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 7 **NUMBER 11** **November 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.

U.S. Government Defines "Critical Software" for Supply Chain Security Purposes

By Steven G. Stransky*

This article explains President Biden's Executive Order 14028, "Improving the Nation's Cybersecurity," which mandates federal agencies implement certain measures to enhance the security and integrity of the software supply chain.

In response to a series of cyberattacks against the United States and its critical infrastructure, President Biden issued Executive Order 14028, "Improving the Nation's Cybersecurity" (the "Cyber EO"). The Cyber EO mandates federal agencies implement certain measures to enhance the security and integrity of the software supply chain. In particular, the Cyber EO requires certain federal agencies to both publish a definition of the term "critical software" and identify a list of categories of software that satisfy this definition, which will be used to limit how the federal government procures such software products. Consequently, the Cyber EO will significantly impact organizations selling, directly or indirectly, cloud services, software solutions, and other information technology to the federal government.

BACKGROUND

The Cyber EO includes several provisions that address risks, threats, and new requirements pertaining to the federal government's procurement of third party products and services containing software solutions or programs. In particular, Section 4(a) of the Cyber EO notes 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" and "[t]here is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended." To address these concerns, the Cyber EO mandates that certain federal agencies, in conjunction with the private sector and academia, identify existing or develop new standards, tools, and best practices for developing and procuring secure software solutions and to issue guidance ("Cyber Guidance") that addresses, among other issues:

---

* Steven G. Stransky is a partner at Thompson Hine LLP and vice chair of its Privacy & Cybersecurity practice group, and a member of its Government Contracts practice group. Mr. Stransky primarily assists clients in devising strategies to assess and mitigate cybersecurity risks and with maintaining compliance with federal, state, and foreign laws and regulations governing data privacy and information security. He previously served as a Deputy Legal Adviser on the President's National Security Council and as an Attorney (Intelligence Law) at the U.S. Department of Homeland Security. Mr. Stransky may be reached at steve.stransky@thompsonhine.com.

- Securing software development environments;
- Auditing trust relationships;
- Generating artifacts that demonstrate compliance with this Cyber Guidance;
- Employing automated tools to maintain trusted source code supply chains and that check for known and potential vulnerabilities;
- Publishing data on the software security life cycle;
- Maintaining accurate and up-to-date data, provenance of all software components;
- Providing a Software Bill of Materials for each product directly or by publishing it on a public website;
- Participating in certain vulnerability disclosure programs;
- Identifying minimum standards for vendors' testing of their software source code; and
- Attesting to conformity with secure software development practices.

The Cyber EO requires that certain agencies furnish recommendations on drafting amendments to federal acquisition processes and regulations to ensure compliance with this Cyber Guidance and the other requirements set forth in the Cyber EO.

DEFINING AND IDENTIFYING CRITICAL SOFTWARE

The Cyber EO mandates that the Director of the National Institute of Standards and Technology ("NIST"), in consultation with the Director of the National Security Agency ("NSA"), the Director of the Cybersecurity and Infrastructure Security Agency ("CISA"), the Director of the Office of Management and Budget, and the Director of National Intelligence, publish a definition of the term "critical software" to which the Cyber Guidance described above would apply. This definition must, according to the Cyber EO, "reflect the level of privilege or access required to function, integration and dependencies with other software, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised." In addition, the Cyber EO provides that the Director of CISA "use this published definition of critical software to develop a list of software categories and products that are in scope for that definition and thus subject to the further requirements of the [Cyber] EO."

On June 25, NIST published a white paper[1] that defines the term "critical software" in the context of the Cyber EO and sets forth a preliminary list of software that meets the definition. For clarity purposes, NIST uses the term "EO-critical software" to refer to "critical software" and avoid conflating it with similar terminology used in other existing definitions and frameworks. In turn, NIST defines EO critical software as:

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

The definition of EO-critical software "applies to software of all forms (e.g., standalone software, software integral to specific devices or hardware components, cloud-based software) purchased for, or deployed in, production systems and used for operational purposes." On the other hand, software solely used for research or testing that is not deployed in production systems, are considered outside of the scope of this definition and therefore not subject to the Cyber Guidance.

The NIST white paper provides the following preliminary list of software categories that satisfy the definition of EO-critical software:

- *Identity, credential, and access management*: software that centrally identifies, authenticates, manages access rights for, or enforces access decisions for organizational users, systems, and devices.
- *Operating systems, hypervisors, container environments*: software that establishes or manages access and control of hardware resources (bare metal or virtualized/containerized) and provides common services such as access control, memory management, and runtime execution environments to software applications and/or interactive users.
- *Web browsers*: software that processes content delivered by web servers over a network and is often used as the user interface to device and service configuration functions.
- *Endpoint security*: software installed on an endpoint, usually with elevated privileges which enable or contribute to the secure operation of

[1] The NIST white paper is accessible at www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf.

the endpoint or enable the detailed collection of information about the endpoint.

- *Network control and protection*: software that implements protocols, algorithms, and functions to configure, control, monitor, and secure the flow of data across a network and products that prevent malicious network traffic from entering or leaving a network segment or system boundary.
- *Network monitoring and configuration*: Network-based monitoring and management software with the ability to change the state of—or with installed agents or special privileges on—a wide range of systems.
- *Operational monitoring and analysis*: software deployed to report operational status and security information about remote systems and the software used to process, analyze, and respond to that information.
- *Remote scanning*: software that determines the state of endpoints on a network by performing network scanning of exposed services.
- *Remote access and configuration management*: software for remote system administration and configuration of endpoints or remote control of other systems.
- *Backup/recovery and remote storage*: software deployed to create copies and transfer data stored on endpoints or other networked devices.

The NIST white paper identifies the types of software products and solutions that align to these categories and NIST's rationale for including these categories therein. However, the NIST white paper also notes that CISA is ultimately responsible for providing "the authoritative list of software categories" that satisfy the definition of EO-critical software, which will be included in the initial phase of the Cyber EO's implementation.

PHASED IMPLEMENTATION

NIST recommends that the federal government implements the requirements set forth in the Cyber EO in a phased approach. According to NIST, such an incremental manner will provide the software industry the opportunity to furnish feedback to the federal government and better enable improvements to NIST's processes with each additional phase. Accordingly, NIST formally recommends that the initial implementation phase "focus on standalone, on-premises software that has security-critical functions or poses similar significant potential for harm if compromised." In addition, subsequent phases, according to NIST, may address other categories of software, such as:

- Software that controls access to data;

- Cloud-based and hybrid software;
- Software development tools (e.g., code repository systems), development tools, testing software, integration software, packaging software, and deployment software;
- Software components in boot-level firmware; or,
- Software components in operational technology.