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.

Issues for Government Contractors and the Private Sector Under the Cybersecurity Executive Order

By Steven G. Stransky, Mona Adabi, Tom Mason, and Thomas F. Zych*

The authors of this article discuss President Biden's "Executive Order on Improving the Nation's Cybersecurity," which creates several new cyber and data protection requirements that will impact organizations providing, directly or indirectly, cloud services, software solutions, and other information technology to the federal government.

In response to a series of cyberattacks against the United States and its critical infrastructure, including the SolarWinds breach, President Biden recently issued "Executive Order on Improving the Nation's Cybersecurity" ("EO").[1] The EO creates several new cyber and data protection requirements that will impact organizations providing, directly or indirectly, cloud services, software solutions, and other information technology to the federal government. Compliance with the EO, and the resulting changes to the Federal Acquisition Regulation ("FAR") and Defense Federal Acquisition Regulation Supplement ("DFARS"), will significantly influence whether an organization is determined to be a "responsible contractor" as required by FAR Part 9. Some of the EO's key issues are set forth below.

INFORMATION SHARING REQUIREMENTS

A cornerstone of the U.S. government's cybersecurity policy is to encourage and, in some instances, mandate cyber threat information sharing[2] between private sector entities and the government. The EO recognizes that technology-related government contractors "have unique access to and insight into cyber threat and incident information" pertaining to the federal government's networks and systems, but that government contracts limit the sharing of such data to federal agencies.

In turn, the EO mandates updates to the FAR and DFARS to ensure that government contracts include clauses requiring contractors to collect and preserve data relevant to cybersecurity events, share such data with the agency

---

* The authors, attorneys with Thompson Hine LLP, may be contacted at steve.stransky@thompsonhine.com, mona.adabi@thompsonhine.com, tom.mason@thompsonhine.com, and tom.zych@thompsonhine.com, respectively.

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

2 *See* Steven G. Stransky, "Enhancing Cyber Threat Information Sharing," *Pratt's Privacy & Cybersecurity Law Report* (July/Aug. 2018 at 182 et. seq.).

with which they have contracted *and* other federal agencies (as may be determined in the future), collaborate with federal agencies as they investigate and respond to cyber incidents, and share cyber threat and incident information with federal agencies.

BREACH NOTIFICATION OBLIGATIONS

The EO mandates that all information and communications technology contractors report to their contracting agency and certain other federal departments "when they discover a cyber incident involving a software product or service provided to such agencies or involving a support system for a software product or service provided to such agencies." The EO requires the FAR and DFARS to be updated to clarify the scope and nature of this reporting. The FAR and DFARS must also address the time periods within which contractors must report cyber incidents based on a graduated scale of severity, with reporting on the most severe cyber incidents to be within three days after initial detection.

CLOUD SERVICE PROVIDERS

A significant portion of the EO is dedicated to cloud service providers ("CSP"), the Federal Risk and Authorization Management Program ("FedRAMP"), and requiring the adoption of a zero trust architecture within the federal government.[3]

In particular, the EO requires certain federal agencies to issue a federal cloud security strategy, cloud security technical reference architecture documentation, and a cloud service governance framework. It also requires federal agencies to "establish a framework to collaborate on cybersecurity and incident response activities" related to certain federal cloud technology to "ensure effective information sharing among agencies and between agencies and CSPs."

The EO also includes requirements addressing automating and standardizing communications between CSPs and federal agencies; automation throughout the FedRAMP lifecycle; digitizing and streamlining compliance documentation; and identifying relevant compliance frameworks, mapping those frameworks into the FedRAMP authorization process, and allowing them to be used as a substitute for the relevant portion of the authorization process.

---

[3] According to the National Institute of Standards and Technology ("NIST"), "zero trust" is "the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources" and "zero trust architecture" uses these the "zero trust principles to plan industrial and enterprise infrastructure and workflows." *See* NIST, SP 800-207, Zero Trust Architecture (Aug. 2020), *available at* https://csrc.nist.gov/publications/detail/sp/800-207/final.

SOFTWARE SUPPLY CHAIN SECURITY

The EO includes several technically detailed provisions addressing risks, threats, and new requirements pertaining to the government's procurement of software.

In particular, it 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 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 issue related guidance that addresses, among other issues:

- Securing software development environments;
- Generating artifacts that demonstrate compliance with the 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 (i.e., origin) of all software components;
- Providing a Software Bill of Materials ("SBOM") for each product directly or by publishing it on a public website;
- Participating in a vulnerability disclosure program that includes a reporting and disclosure process;
- Identifying minimum standards for vendors' testing of their software source code; and
- Attesting to conformity with secure software development practices.

The EO also requires that certain agencies more thoroughly examine and define the term "critical software" to which these requirements will apply. In addition, federal agencies must furnish recommendations on amendments to the FAR requiring "suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements" that are issued pursuant to the EO. After such FAR amendments become final, federal agencies must remove software products that do not meet the requirements of the amended FAR from all federal supply schedules, federal government-wide acquisition contracts, blanket purchase agreements, and multiple award contracts.

However, the EO creates separate rules for agencies employing software developed and procured prior to the date of the EO (i.e., legacy software).

SOFTWARE PRODUCT LABELING

The EO mandates that certain federal agencies initiate pilot programs (informed by existing consumer product labeling programs) to educate the public on the security capabilities of IoT devices and software development practices; identify IoT cybersecurity criteria for a consumer labeling program; and identify secure software development practices for a consumer software labeling program. The criteria for IoT devices must reflect the levels of testing and assessment that the product may have undergone and be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products. The practices for software must consider whether a labeling program may align with any similar existing government programs and reflect a baseline level of secure practices and increasingly comprehensive levels of testing and assessment that the software may have undergone.

CONCLUSION

It will be important for government contractors to assess the upcoming changes to the FAR and DFARS to ensure they are compliant with these new requirements. Government contractors should also consider participating in the government's rulemaking process to ensure any new cybersecurity requirements are practical and reasonable in light of the government's compelling need for greater information protection.