PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 9 **NUMBER 9** **September 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call or email:

Heidi A. Litman at 516-771-2169
Email: ..... heidi.a.litman@lexisnexis.com

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
LexisNexis® Support Center . . . . https://supportcenter.lexisnexis.com/app/home/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (518) 487-3385

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

(2023–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.

Secure Software Regulations and Self-Attestation Required for Federal Contractors

By Guillermo S. Christensen, Sheila A. Armstrong, Tara D. Hopkins and Brian J. Hopkins*

In this article, the authors discuss a new federal requirement that will require software vendors to attest to new security controls in the design of code used by the federal government.

Government contractors providing software across the federal government's supply chain soon will be required to comply with a new Secure Software Design Framework (SSDF). The SSDF requires software vendors to attest to new security controls in the design of code used by the federal government.

CYBERSECURITY COMPROMISES OF GOVERNMENT SOFTWARE ON THE RISE

In the aftermath of the cybersecurity compromises of significant enterprise software systems embedded in government supply chains, the federal government has increasingly prioritized reducing the vulnerability of software used within agency networks. Recognizing that most of the enterprise software that is used by the federal government is provided by a wide range of private sector contractors, the White House has been moving to impose a range of new software security regulations on both prime and subcontractors.

One priority area is an effort to require government contractors to ensure that software used by federal agencies incorporates security by design. As a result, federal contractors supplying software to the government now face a new set of requirements to supply secure software code. That is, to provide software that is developed with security in mind so that flaws and vulnerabilities can be mitigated before the government buys and deploys the software.

THE SSDF AS A GOVERNMENT RESPONSE

In response, the White House issued Executive Order 14028, "Executive Order on Improving the Nation's Cybersecurity" (EO 14028), on May 12, 2021. EO 14028 requires the National Institute of Standards and Technology (NIST) to develop standards, tools, and best practices to enhance the security of the software supply chain. NIST subsequently promulgated the SSDF in special publication NIST SP 800-218. EO 14028 also mandates that the

* The authors, attorneys with K&L Gates LLP, may be contacted at Guillermo.Christensen@klgates.com, Sheila.Armstrong@klgates.com, Tara.Hopkins@klgates.com and Brian.Hopkins@klgates.com, respectively.

director of the Office of Management and Budget (OMB) take appropriate steps to ensure that federal agencies comply with NIST guidance and standards regarding the SSDF. This resulted in OMB Memorandum M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" (M-22-18).

The OMB memo provides that a federal agency may use software subject to M-22-18's requirements only if the producer of that software has first attested to compliance with federal government-specified secure software development practices drawn from the SSDF. Meaning, if the producer of the software cannot attest to meeting the NIST requirements, it will not be able to supply software to the federal government. There are some exceptions and processes for software to gradually enter into compliance under various milestones for improvements, all of which are highly technical and subjective.

In accordance with these regulations, the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security issued a draft form for collecting the relevant attestations and associated information. CISA released the draft form on April 27, 2023, and accepted comments until June 26, 2023.[1]

SSDF IMPLEMENTATION DEADLINE AND REQUIREMENTS FOR GOVERNMENT SUPPLIERS

CISA initially set a deadline of June 11, 2023, for critical software and September 13, 2023, for non-critical software to comply with SSDF. Press reports indicate that these deadlines will be extended due to both the complexity of the SSDF requirements and the fact that the comment period remained open until June 26, 2023. However, CISA has not yet confirmed an extension of the deadline.

ATTESTATION AND COMPLIANCE WITH THE SSDF

Based on what we know now, the attestation form generally requires software producers to confirm that:

- The software was developed and built in secure environments.
- The software producer has made a good-faith effort to maintain trusted source code supply chains.
- The software producer maintains provenance data for internal and third-party code incorporated into the software.
- The software producer employed automated tools or comparable

[1] 88 Fed. Reg. 25,670.

processes that check for security vulnerabilities.

Software producers that must comply with SSDF should move quickly and begin reviewing their approach to software security. The SSDF requirements are complex and likely will take time to review, implement, and document. In particular, many of the requirements call for subjective analysis rather than objective evaluation against a set of quantifiable criteria, as is usually the case with such regulations. The SSDF also includes numerous ambiguities. For example, the SSDF requires versioning changes in software to have certain impacts in the security assessment, although the term "versioning" does not have a standard definition in the software sector.

NEXT STEPS AND RISK OF NONCOMPLIANCE

Critically, the attestations on the new form carry risk under the civil False Claims Act for government contractors and subcontractors. Given the fact that many of the attestations require subjective analysis, contractors must take exceptional care in completing the attestation form. Contractors should carefully document their assessment that the software they produce is compliant.