PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 7 **NUMBER 9** **September 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.

President Biden Issues Executive Order to Overhaul Cyber and Software Supply Chain Security and Expand Incident Reporting for Contractors

By Natasha G. Kohne, Michael J. Vernick, Scott M. Heimberg, Molly E. Whitman, Michelle A. Reed, Angela B. Styles, and Chris Chamberlain*

The authors suggest that contractors and other stakeholders should closely monitor the various timelines and releases laid out in President Biden's executive order on improving the nation's cybersecurity.

On May 12, 2021, President Biden issued Executive Order ("EO") 14028 on "Improving the Nation's Cybersecurity."[1] As noted in the administration's accompanying Fact Sheet,[2] the EO is a direct response to recent high-profile cybersecurity incidents (e.g., SolarWinds).

More broadly, the EO responds to years of increasing concern about, and efforts to enhance, cyber and supply chain security within the federal government, its contracting base and the U.S. information and communications technology and services ("ICTS") industry.

Building on initiatives such as Section 889, the Department of Commerce's ICTS supply chain regulations,[3] Federal Acquisition Regulation ("FAR") and the Defense Federal Acquisition Regulation Supplement ("DFARS") cybersecurity and incident reporting standards, and the Department of Defense's ("DOD") Cybersecurity Maturity Model Certification ("CMMC"), among other efforts, the EO seeks to harmonize, enhance, and extend existing security

---

* The authors, attorneys with Akin Gump Strauss Hauer & Feld LLP, may be contacted at nkohne@akingump.com, mvernick@akingump.com, sheimberg@akingump.com, mwhitman@akingump.com, mreed@akingump.com, astyles@akingump.com, and cchamberlain@akingump.com, respectively. Akin Gump counsel Molly Whitman and summer associate Miguel Bacigalupe also contributed to this article.

[1] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

[2] https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/.

[3] https://www.ecfr.gov/cgi-bin/text-idx?SID=259a81022ebe4cf2c0cf81ad8a8ce21a&mc=true&tpl=/ecfrbrowse/Title15/15cfr7_main_02.tpl.

requirements across the government sector while operationalizing several new programs to address existing and emerging threats.

Consequently, the EO and related rulemakings will significantly impact government contractors, software companies and other ICT service providers, most notably through adding or enhancing incident reporting requirements and attestations related to software development and acquisition practices.

EO OVERVIEW

The EO contains 10 sections, eight of which address specific areas or issues in federal cyber and supply chain security:

- Section 1: Policy;
- Section 2: Removing Barriers to Sharing Threat Information;
- Section 3: Modernizing Federal Government Cybersecurity;
- Section 4: Enhancing Software Supply Chain Security;
- Section 5: Establishing a Cyber Safety Review Board;
- Section 6: Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents;
- Section 7: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks;
- Section 8: Improving the Federal Government's Investigative and Remediation Capabilities;
- Section 9: National Security Systems; and
- Section 10: Definitions.

While the EO targets U.S. federal agencies and their cyber and supply chain policies, several sections will quickly reach beyond the government into the federal contracting community, as well as the wider ICTS, cloud, software and cybersecurity services ecosystem. In the near term, government contractors and other stakeholders should pay close attention to developments flowing from EO Sections 2 and 4, while monitoring the longer term implications of other efforts under the EO for business and compliance considerations.

INCIDENT REPORTING AND CYBERSECURITY STANDARDS FOR FEDERAL CONTRACTORS

Incident Reporting

Section 2 of the EO, "Removing Barriers to Sharing Threat Information," lays the groundwork for a federal government-wide incident reporting framework for certain information technology ("IT") and operational technology

("OT") "service providers" and "cloud service providers" (terms that the administration has not yet defined). As a first step, the EO directs the Office of Management and Budget ("OMB") to review and recommend updates to the FAR and DFARS contract requirements and language for "contracting with IT and OT service providers." Notably, the EO recommends that FAR and DFARS contracts specifically include descriptions of contractors (i.e., the "service providers") to be covered by the proposed updates.

In the EO, the administration also states its expectation that the proposed language will address and ensure that these providers adequately collect and share cybersecurity incident information and collaborate with federal agencies in incident response and investigation—including by "monitoring networks for threats *in collaboration with agencies* they support, as needed."[4] In addition, the EO previews several minimum standards that will likely manifest in forthcoming rulemakings, including that:

- ICT service providers must "promptly" report cyber incidents involving software or services provided to their federal customers or involving a support system for such software or services; and
- ICT service providers must also directly report to the Department of Homeland Security's ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") whenever they report an incident to another federal agency.

The EO does not define the term "promptly," "support system," or other key terms. It similarly leaves open the specific scope of this new incident reporting regime and criteria that would trigger the requirement to report, and instead directing DHS, in consultation with the National Security Agency, the Attorney General, and OMB, to recommend contract language to the FAR Council ("FAR Council")—the body generally charged with overseeing federal acquisition rules—within 45 days of the EO's issuance (late June 2021) that identifies:

- The nature of cyber incidents that require reporting;
- The types of information regarding cyber incidents that require reporting to facilitate effective cyber incident response and remediation;
- Appropriate and effective protections for privacy and civil liberties;
- 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 not to exceed three days after initial detection;

[4] Emphasis added.

- Reporting requirements for "National Security Systems" (as defined in the order); and
- The type of "contractors and associated service providers" to be covered by the proposed contract language.

To date, the details of DHS's 45-day report have not been made public. The EO calls upon the FAR Council to review the recommendations and publish proposed updates to the FAR for public comment within 90 days (mid-October 2021).

Cybersecurity Requirements

Alongside these reviews and proposals related to incident reporting, the EO directs CISA to review—within 60 days (by mid-July 2021)—agency-specific cybersecurity requirements currently in existence and recommend "standardized contract language" for "appropriate requirements," taking into consideration the "scope of contractors and associated service providers" that will be covered by the proposed language. As of the date of this article's publication, the details of this review and any related recommendations have not been made public.

As these efforts unfold over the next several months, they will raise important practical questions about the operation of existing incident reporting and cybersecurity regimes including the FAR "basic" cybersecurity standards, and more significantly the DFARS provisions addressing the protection of controlled unclassified information ("CUI"), cybersecurity assessments and the CMMC framework.

SOFTWARE SUPPLY CHAIN SECURITY STANDARDS AND ENFORCEMENT

Section 4 of the EO, "Enhancing Software Supply Chain Security," seeks to establish foundational standards for the security and integrity of software products purchased by U.S. federal agencies.

Of particular concern is the security and integrity of so-called "critical software" (now referred to as "EO-critical software"), which the EO broadly defines—preliminarily—to include software that "performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resource)."

The administration's efforts on this front will advance primarily on two interrelated tracks described further below, with one focused on agency policies and compliance, and another focused on developing and implementing guidance for contractors in regulations and procurement rules.

Agency Compliance with "Critical Software" Definition and Guidance

- The EO directed the National Institute of Standards and Technology

("NIST") to publish within 45 days of the EO (by late June 2021) a definition of the term "critical software" that will "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." Companies should carefully track this initiative, as it will likely prove to be a critical element of the ultimate scope of any related rules or policies promulgated under the EO.

- Within 30 days of the publication of this definition (75 days from the EO, late July 2021), CISA is expected to identify and make available to agencies a list of categories of software and software products in use or in the acquisition process meeting the definition of "critical software." The EO does not clarify whether "in use" means in use by agencies, their contractors or both, though guidance[5] subsequently issued by NIST on the "use" of critical software does note that it applies to software "deployed . . . in agencies' operational environments," suggesting it would include systems run or managed by contractors on an agency's behalf.

- The EO also charged NIST to publish guidance within 60 days of the EO outlining security measures for critical software, including "applying practices of least privilege, network segmentation, and proper configuration."
  - Importantly, after publishing its definition of "critical software"[6] in a white paper on June 26,[7] NIST published additional guidance[8] (and launched a related website[9]) on such "security measures" on July 9, including a series of Frequently Asked Questions and a table defining security measures, objectives, and related "Federal Government Informative References" (i.e., ex-

---

[5] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-0.

[6] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory.

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

[8] https://www.nist.gov/system/files/documents/2021/07/09/Critical%20Software%20Use%20Security%20Measures%20Guidance.pdf.

[9] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-0.

isting guidance from federal agencies). In practice, the report and the table are notable for their correlation of existing standards (e.g., from NIST, CISA, NSA, and OMB) and the "security measures" that could eventually inform regulatory and procurement standards for "EO-critical software."

- On August 10, and as called for in the EO, OMB issued an interagency memorandum providing instructions for implementing the measures outlined in NIST's July guidance, kicking off further actions by federal agencies to identify critical software and incorporate security measures outlined in the NIST guidance.[10]

NIST Guidance and FAR Rules for Contractors

- Within 30 days of the EO, NIST was tasked to solicit input from federal, private sector, academic, and other "appropriate" actors to identify existing, or develop new, "standards, tools, and best practices" for complying with a set of baseline standards, procedures, and criteria set forth in Section 2(e) of the EO (listed below). Shortly after the administration issued the EO, NIST announced a call for position papers and held a virtual workshop, which it followed by issuing a definition of "critical software" and related guidance, as noted above.
- Within 180 days of the EO (around November 2021), NIST will publish preliminary guidelines based on these consultations and "drawing on existing documents as practicable" for enhancing software supply chain security. Likely candidates for "existing documents" would include NIST's Special Publication ("SP") 800-161, Cyber Supply Chain Risk Management Practices for Systems and Organizations;[11] various software supply chain guidance documents[12] published by CISA; and materials developed through the National Telecommunications and Information Administration's ("NTIA") Software Bill of Materials initiative.[13]
    - Within 360 days of the EO, NIST will publish additional guidance on procedures for review and updating of these guidelines.

---

[10] OMB, M-21-30: Protecting Critical Software Through Enhanced Security Measures (Aug. 10, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf.

[11] https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft.

[12] https://us-cert.cisa.gov/ncas/current-activity/2021/04/26/cisa-and-nist-release-new-interagency-resource-defending-against.

[13] https://www.ntia.gov/SBOM.

- Within 90 days of the publication of these preliminary guidelines (270 days from the EO), NIST and the heads of other agencies as NIST "deems appropriate" are expected to issue guidance identifying "practices" that enhance the security of the software supply chain. As a preview of what may be to come, Section 2(e) of the EO explains that the anticipated guidance will include standards, procedures or criteria regarding:
    - Secure software development environments, including such actions as:
        - Using administratively separate build environments.
        - Auditing trust relationships.
        - Establishing multi-factor, risk-based authentication, and conditional access across the enterprise.
        - Documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software.
        - Employing encryption for data.
        - Monitoring operations and alerts and responding to attempted and actual cyber incidents.
    - Generating and, when requested by a purchaser, providing "artifacts" that demonstrate conformance to these standards.
    - Employing automated tools, or comparable processes, to maintain trusted source code supply chains.
    - Employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version or update release.
    - Providing, when requested by a purchaser, artifacts of the execution of such tools and processes and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated.
    - Maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis.

- Providing a purchaser a Software Bill of Materials ("SBOM") for each product directly or by publishing it on a public website.
  - Importantly, on July 12, and as required by the EO, and following a public comment period,[14] the Commerce Department's National Telecommunications and Information Administration ("NTIA") published a report[15] outlining the minimum elements of an SBOM, breaking down the elements into three categories (*see* Figure 1) of "data fields," "automation support," and "practices and processes." While not yet operational, the report and other SBOM-related initiatives[16] will play a key role in shaping subsequent guidance and requirements flowing from the EO.

Minimum Elements	
Data Fields	Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.
Automation Support	Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.
Practices and Processes	Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodations of Mistakes.

Figure 1

- Participating in a vulnerability disclosure program that includes a reporting and disclosure process.
- Attesting to conformity with secure software development practices.
- Ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion

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

[15] https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf.

[16] https://www.ntia.gov/sbom.

of a product.

- Within 30 days of the issuance of this guidance (360 days from the EO) (around May 2022), OMB will implement appropriate steps to require that agencies comply with the guidelines with respect to software procured after the date of the EO.
- Finally, and also within one year of the EO, DHS, in consultation with the DOD, the Attorney General and OMB, are to recommend to the FAR Council contract language requiring "suppliers of software available for purchase by agencies" to comply with, and attest to their having complied with, any requirements issued pursuant to the guidance discussed above. The EO's language suggests that the attestation requirement will be incorporated into existing systems used by contractors to make representations to federal customers (e.g., through the System for Award Management (SAM.gov)). While the exact language and mechanisms will presumably be developed through the required rulemakings, contractors could look to recent rulemakings implementing the DOD's cyber assessments and CMMC frameworks, as well as the regulations implementing Section 889 of the National Defense Authorization Act for Fiscal Year 2019. Based on the EO, however, it is unclear whether, or how, the administration will require attestations on a product-by-product, contract-by-contact or entity-by-entity basis, leaving this issue open for resolution through the course of forthcoming engagement and rulemakings.
- Once these recommendations are promulgated in a final rule, agencies will begin to remove software products that do not meet the requirements of the amended FAR from all indefinite delivery indefinite quantity contracts, federal supply schedules, federal government-wide acquisition contracts, blanket purchase agreements and multiple award contracts. Such an action would be a substantial blow, both economically and reputationally, to any software providers whose products are deemed noncompliant.

In addition to the security enhancement efforts, the EO directed NIST to issue guidelines recommending minimum standards for vendors' testing of their software source code, including identifying recommended types of manual or automated testing.

Accordingly, and concurrently with its July 9 publication of guidance on "critical software," NIST published a guidance document[17] and a corresponding website[18] on "Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software." While not yet operational, the guidance provides technical descriptions and summarizes supplemental information on various tools, techniques, and procedures (e.g., code review tools, static and dynamic analysis, software composition tools, and penetration testing) that could ultimately form the basis for software security evaluation standards. In the meantime, with the emergence of this guidance, contractors should be prepared for the possibility that agencies—and potentially other commercial customers—begin factoring these standards into their buying decisions, even before promulgation of formal rules and contract language.

The EO also calls for the creation of a pilot program modeled after other consumer product labeling programs to "educate the public" on the security capabilities of Internet-of-Things devices and software development practices, which could form the basis for a "tiered security rating system" for such products.

In sum, Section 4 of the EO promises potentially sweeping changes in the software acquisition process and, in the longer term, software development and security practices both in and outside the federal ecosystem.

OTHER SIGNIFICANT DEVELOPMENTS AND INITIATIVES

In addition to the reviews and rulemakings called for under Sections 2 and 4, the EO calls for significant enhancements and initiatives in various other aspects of federal cybersecurity policy, virtually all of which will in some way affect—if indirectly—companies that operate in or with the ICTS and cybersecurity industries. For example:

- Section 3 of the EO calls for agencies to prioritize adoption and migration to secure cloud environments, implement Zero Trust Architecture, adopt multifactor authentication and encryption for data at rest and in transit, and modernize FedRAMP.
- Section 5 calls for DHS to establish a Cyber Safety Review Board tasked with examining significant cyber incidents and affected federal and nonfederal information systems.

---

[17] https://www.nist.gov/system/files/documents/2021/07/13/Developer%20Verification%20of%20Software.pdf.

[18] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or.

- Section 6 directs DHS and OMB to standardize federal incident response procedures and develop a government-wide "Playbook"—procedures that will undoubtedly have a role for private companies involved in responding to such incidents, and which could become a de facto standard for incident response procedures employed by private companies even outside the federal ecosystem.
- Section 7 calls for agencies to enhance their deployment of Endpoint Detection and Response ("EDR") update agreements with CISA related to DHS's Continuous Diagnostics and Mitigation Program.
- Section 8 calls on DHS to issue logging guidance to federal agencies within 14 days of the EO, and eventually have OMB factor such guidance and recommendations into FAR updates pursuant to Section 2. In practice, this will likely have an immediate impact on cybersecurity vendors currently engaged in managing or supporting federal networks, and as with other enhancements called for in the EO, could become a de facto standard for logging practices both in and outside the federal ecosystem.

Although these other developments and initiatives are less direct in their potential effect on the federal contracting community and private sector, they represent important developments in U.S. cybersecurity and supply chain security policy, and as a result they have the potential to alter the ICTS and cybersecurity industries broadly. In particular, and notably in the view of the Biden-Harris administration, they should be understood as long term, permanent enhancements to minimum standards that the government—and potentially the private sector—will come to see as the new floor for what is "reasonable" cyber and supply chain security in other related data and technology protection domains (e.g., data privacy, export controls).

RECOMMENDATIONS AND NEXT STEPS

With so much of the EO's scope and implications left to unfold and on such rapid timelines, it will be critical for potentially affected contractors and other stakeholders to closely monitor the various timelines and releases laid out in the order. Each juncture will provide critical opportunities to engage and educate policymakers as well as gain insights to anticipate the eventual scope of the forthcoming policies and regulations.