Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

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

May 21, 2021

Key Points

- On Wednesday, May 12, 2021, President Biden issued EO 14,028, "Improving the Nation's Cybersecurity." The EO sets out an ambitious schedule of reviews and rulemakings that portend significant changes in the software and cybersecurity industries, particularly for government contractors and cybersecurity and software solution providers. In the view of the administration, these changes should be regarded as the new normal of what will be considered "reasonable" cyber and supply chain security practices applicable to the government—and potentially the private sector in other industries and sectors.
- Most importantly, the EO sets in motion a series of reviews and rulemakings around two initiatives that will directly affect certain government contractors and those who sell software and related services to U.S. federal agencies: enhancing and expanding cyber and supply chain incident reporting and threat information sharing (Section 2); and creating and enforcing software supply chain security standards (Section 4).
- The EO does not immediately establish any requirements or prohibitions for nongovernmental entities, but it calls for swift action by federal agencies to establish policies and propose changes to federal contracting rules to implement the EO. Importantly, the aggressive timelines in the EO and the sensitive nature of the topic to the administration increase the likelihood that any such proposals will come in the form of interim final rules, increasing the importance of proactive planning and engagement.
- To kick-off what will be a critical period of stakeholder engagement, NIST issued a call for two-page position papers and will host a workshop related to the EO and based on these papers on June 2 and 3, 2021. Position papers must be received by NIST no later than May 26, 2021. Government contractors, software companies, ICT service providers and other stakeholders in the EO should consider submitting position papers and, going forward, prepare to engage with the key agencies involved throughout the lifecycle of the EO and its related rulemakings.

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Michael J. Vernick
Partner
mvernick@akingump.com
Washington, D.C.
+1 202.887.4460

Angela B. Styles
Partner
astyles@akingump.com
Washington, D.C.
+1 202.887.4050

Scott M. Heimberg
Partner
sheimberg@akingump.com
Washington, D.C.
+1 202.887.4085

Chris Chamberlain
Associate
cchamberlain@akingump.com
Washington, D.C.
+1 202.887.4308

Background

On May 12, 2021, President Biden issued Executive Order (EO) 14,028 on "Improving the Nation's Cybersecurity." As noted in the administration's accompanying Fact Sheet, the EO is a direct response to recent high-profile cybersecurity incidents (e.g., SolarWinds). It should, however, also be viewed in context as a response 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 more broadly. Building on initiatives such as Section 889, the Commerce Department's ICTS supply chain regulations, 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 cyber and supply chain security requirements across the government while operationalizing several new programs and frameworks to address existing and emerging threats. As a result, the EO, and its related rulemakings, will have important implications for government contractors, software companies and other ICT service providers, most notably in the form of added or enhanced incident reporting requirements and attestations related to software development and acquisition practices.

EO Overview

The EO consists of 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
- Section 10: Definitions.

While the EO is directed toward 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 will need to 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 (as-yet undefined) information technology (IT) and operational technology (OT) "service providers" and "cloud service providers." As a first step towards establishing this framework, 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 recommendations are specifically to include descriptions of contractors (i.e., the "service providers") to be covered by the proposed updates.

The EO also sets the administration's expectations 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" (emphasis added). 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.
- 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 and criteria that would trigger this new incident reporting regime, instead directing DHS, in consultation with the National Security Agency, the Attorney General and OMB, to recommend contract language to the Federal Acquisition Regulatory Council ("FAR Council")—the body generally charged with overseeing federal acquisition rules—within 45 days 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**.
- Reporting requirements for "National Security Systems" (as defined in the order).
- The type of "contractors and associated service providers" to be covered by the proposed contract language.

Once received, the EO calls upon the FAR Council to review the recommendations and publish proposed updates to the FAR for public comment within 90 days.

Cybersecurity Requirements

Alongside these reviews and proposals related to incident reporting, the EO directs CISA to review—within 60 days—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 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 CUI, cybersecurity assessments and the CMMC framework.

Software Supply Chain Security Standards and Enforcement

Broadly, 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 security and integrity of so-called "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:

Agency Compliance with "Critical Software" Definition and Guidance

- Within 45 days of the EO, NIST is directed to publish 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 and engage in this initiative, as it will likely prove to be a critical element of the ultimate scope of any related rules or policies.
  - Within 30 days of the publication of this definition (75 days from the EO), 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.
- Within 60 days of the EO, NIST will publish guidance outlining security measures for "critical software," including "applying practices of least privilege, network segmentation, and proper configuration."
- Within 30 days of the issuance of this guidance (90 days from the EO), and at which point CISA's "list" of "critical software" categories should have been made available to federal agencies, OMB will be expected to take appropriate steps to **require** that agencies comply with the new guidance. At this time, it is unclear whether CISA's "list" will be shared outside the federal ecosystem, leaving open questions about

whether and how companies will know whether their software may or may not qualify as “critical software” subject to the NIST guidance noted above.

NIST Guidance and FAR Rules for Contractors

- Within 30 days of the EO, NIST will 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 did just this by announcing a call for position papers and a workshop to be held virtually on June 2–3, described further below.
- Within 180 days of the EO, NIST will publish preliminarily 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; various software supply chain guidance documents published by CISA; and materials developed through the National Telecommunications and Information Administration’s (NTIA) Software Bill of Materials initiative.
  - Within 360 days of the EO, NIST will publish additional guidance on procedures for review and updating of these guidelines.
- 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, the EO explains that the anticipated guidance will include standards, procedures or criteria regarding:
  - Secure software development environments, including such actions as:
    - (A) using administratively separate build environments.
    - (B) auditing trust relationships.
    - (C) establishing multi-factor, risk-based authentication and conditional access across the enterprise.
    - (D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build and edit software.
    - (E) employing encryption for data.
    - (F) 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.
  - 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 of a product.
- Within 30 days of the issuance of this guidance (360 days from the EO), 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, which we described in our November 20, 2020, webinar here, as well as the regulations implementing Section 889 of the National Defense Authorization Act for Fiscal Year 2019, which we describe here and in related prior publications. 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 directs NIST to issue, within 60 days, guidelines recommending minimum standards for vendors' testing of their software source code, including identifying recommended types of manual or

automated testing (such as code review tools, static and dynamic analysis, software composition tools and penetration testing). 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 (IoT) 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, described above, 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.
- 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 United States 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 policy-makers as well as gain insights to anticipate the eventual scope of the forthcoming policies and regulations.

To kick-off the engagement period, NIST announced that it will host a virtual workshop on June 2–3 pursuant to the EO's directive in Section 4 that it consult with federal agencies, the private sector, academia and other stakeholders to identify the standards, tools, best practices and other guidelines that will feed into the policies and rules flowing from the EO. In advance of the workshop, participants are encouraged to submit two-page position papers addressing one or more of five areas:

- Criteria for designating "critical software." Functional criteria should include, but not be limited to, level of privilege or access required to function, integration, dependencies, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised. See EO Section 4(g).
- Initial list of secure software development lifecycle standards, best practices and other guidelines acceptable for the development of software for purchase by the federal government. This list of standards shall include criteria and required information for attestation of conformity by developers and suppliers. See EO Section 4(e)(i, ii, ix and x).
- Guidelines outlining security measures that shall be applied to the federal government's use of critical software, including but not limited to least privilege, network segmentation and proper configuration. See EO Section 4(l).
- Initial minimum requirements for testing software source code including defining types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools and penetration testing), their recommended uses, best practices and setting realistic expectations for security benefits. See EO Sections 4(e)(iv and v) and 4(r).
- Guidelines for software integrity chains and provenance. See EO Sections 4(e)(ii, vi and viii).

Position papers should be submitted no later than **May 26, 2021**.

akingump.com