JENNER & BLOCK

White House Executive Order Seeks to Strengthen Federal Cybersecurity

Client Alerts

January 22, 2025
By: Shoba Pillay, Philip J. Chertoff

On January 16, 2025, former President Biden issued the Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity (the EO).[1] The EO directs various parts of the federal government to adopt a laundry list of cybersecurity standards and contract requirements, ranging from enabling encrypted DNS and communications systems to adopting products using post-quantum cryptography, and prioritizes the acquisition of artificial intelligence cybersecurity tools and digital authentication methods. Most notably for federal contractors, it directs multiple parts of the federal government to cooperate on the creation of a system for validating federal contractor and software supplier use of secure software development practices.

The order caps off a years-long effort by the Biden administration to raise the cybersecurity standards of the federal government. Early in the administration, on May 12, 2021, President Biden signed Executive Order 14028 (EO 14028), which sought to strengthen the federal government's ability to respond to and prevent cybersecurity threats by, among other points, removing obstacles to public-private threat information sharing, modernizing federal security systems, setting new cybersecurity standards for software purchased by the federal government, imposing new cyber incident reporting requirements, and establishing the Cyber Safety Review Board to review and analyze cyber incidents.

While President Trump declined to rescind the EO as part of his "Initial Rescissions of Harmful Executive Order and Actions" Executive Order,[2] it is unclear whether President Trump will ultimately decide to scrap the EO, modify it, or otherwise keep it in place.

Summary of the EO Provisions

Section 2. Operationalizing Transparency and Security in Third-Party Software Supply Chains:

- EO 14028 directed multiple parts of the federal government to develop guidance on secure software development practices and create methods to attest to compliance with those practices. It also mandated agencies use only software from vendors that attest to using those practices. Section 2 advances these objectives by directing OMB, NIST, and CISA to recommend to the

Federal Acquisition Regulatory Council (FAR Council) contract language requiring federal software providers to submit to CISA (1) software development attestations, (2) computer records (or "artifacts") validating those attestations, and (3) a list of the providers' Federal Civilian Executive Branch (FCEB) agency software customers through CISA's Repository for Software Attestation and Artifacts (RSAA).

- Alongside this recommendation, CISA will review "emerging methods of generating, receiving, and verifying machine-readable secure software development attestations and artifacts" and provide guidance to software providers on how attestations and artifacts should be submitted to the RSAA.

- The FAR Council will review these recommendations and the Secretary of Defense, Administrator of the General Services Administration (GSA), and NASA Administrator will amend the Federal Acquisition Regulation (FAR) to implement those recommendations, likely via an interim final rule.

- Subsequently, CISA will develop a program to verify the completeness of attestation forms and continue to validate vendor attestations moving forward. If attestations or artifacts are incomplete, CISA will notify the provider and contracting agency and provide a process for the provider to respond to its initial incompleteness determination. Validated attestations will be publicly posted by the National Cyber Director (NCD) and attestations that fail validation may be referred by the NCD to the Attorney General for appropriate action.

- Section 2 also directs NIST to:

  - In collaboration with an industry consortium, develop guidance on the "implementation of secure software development, security, and operations practices" based on NIST Special Publication 800-218 (Secure Software Development Framework (SSDF)),

  - Update NIST Special Publication 800-53 to provide guidance on "how to securely and reliably deploy patches and updates,"

  - Develop and publish a preliminary update to the SSDF,

  - Incorporate updates to the SSDF into "the requirements of OMB Memorandum M-22-18 (Enhancing the Security of the Software Supply Chain through Secure Software Development Practices) or related requirements," and

  - Incorporate these updated OMB requirements into CISA's Secure Software Development attestations.

- Finally, Section 2 directs OMB, NIST, and the Federal Acquisition Security Council to require agencies to comply with NIST Special Publication 800-161 (Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161 Revision 1)) and provide

annual updates to OMB on its implementation. CISA, OMB, and the GSA will also issue joint recommendations to agencies on "the use of security assessments and patching of open-source software and best practices for contributing to open-source software projects."

Section 3. Improving the Cybersecurity of Federal Systems:

- Section 3 directs FCEB agencies to begin pilot deployments of commercial phishing-resistant authentication measures, such as WebAuthn.
- It directs CISA, in collaboration with the Federal CIO and Federal CISO Council, to develop the technical capability and concept of operations for CISA to gain timely access to required data from FCEB agency endpoint detection and response (EDR) solutions and FCEB agency secure operation centers (SOC).
- It directs the Director of FedRAMP, in collaboration with CISA and NIST to "develop FedRAMP policies and practices to incentivize or require cloud service providers in the FedRAMP Marketplace to produce baselines with specifications and recommendations for agency configuration of agency cloud-based systems in order to secure Federal data based on agency requirements."
- Finally, it directs the Under Secretary of Commerce for Oceans and Atmosphere, the Administrator of the National Oceanic and Atmospheric Administration, and NASA Administrator to review "civil space contract requirements in the FAR" and recommend to the FAR Council, and for the FAR Council to adopt, updates to civil space cybersecurity requirements and relevant contract language.
- The NCD will also submit to OMB a study of space ground systems owned by FCEB agencies, and OMB will take steps to ensure these systems comply with its cybersecurity requirements.

Section 4. Securing Federal Communications:

- Section Four directs FCEB agencies to take several steps to secure their communications and Internet traffic, including:
    - Registering their assigned Internet number resources (Internet Protocol (IP) address blocks and Autonomous System Numbers) with the American Registry for Internet Numbers or another appropriate regional Internet registry.
    - Creating and publishing Route Origin Authorizations in the public Resource Public Key Infrastructure repository hosted or delegated by the American Registry for Internet Numbers or the appropriate regional Internet registry for the IP address blocks they hold.
- It directs the NCD to recommend to the FAR Council, and for the FAR Council to adopt, contract language requiring federally contracted providers of Internet services to adopt and deploy

Internet routing security technologies, including publishing Route Origin Authorizations and performing Route Origin Validation filtering. NIST will also publish updated guidance to agencies on the deployment of BGP security methods on their systems and on "other emerging technologies to improve Internet routing security and resilience, such as route leak mitigation and source address validation."

- It directs CISA to propose, and for the FAR Council to adopt, template contract language requiring products acting as DNS resolvers to support encrypted DNS, directs OMB to require expanded use of transport layer encryption between FCEB agency email servers and across voice and video conferencing and instant messaging (including end-to-end encryption where supported), and requires FCEB agencies to enable encrypted DNS protocols and encrypted and authenticated email transport between agency email servers and clients.

- It directs CISA to develop and release a list of product categories with widely available products that incorporate post-quantum cryptography (PQC), agencies to require PQC in any solicitations for products appearing in these categories, agencies to implement PQC key establishment or hybrid key establishment, NIST and the Department of Commerce Under Secretary for International Trade to encourage key countries to transition to PQC algorithms standardized by NIST, and the Secretary of Defense and OMB Director to issue requirements for National Security Systems (NSS) and non-National Security Systems to support Transport Layer Security protocol version 1.3 or a successor version.

- Finally, it directs NIST and CISA to develop guidelines for the secure management of access tokens and cryptographic keys used by cloud service providers; the FedRAMP Director, in consultation with NIST and CISA, to develop updated FedRAMP requirements incorporating these access token and cryptographic key guidelines; and the OMB Director, in consultation with NIST, CISA, and the GSA, to require FECB agencies to "follow best practices concerning the protection and management of hardware security modules, trusted execution environments, or other isolation technologies for access tokens and cryptographic keys used by cloud service providers in the provision of services to agencies."

Section 5. Solutions to Combat Cybercrime and Fraud:

- Section 5 directs agencies with grantmaking authority to make available federal grant funding to assist states with the development and issuance of mobile driver's licenses, which may be used to access public benefits programs requiring identity verification.

- It directs NIST to issue practical implementation guidance to support remote digital identity verification. It further directs agencies to consider accepting digital identity documents as evidence to access public benefits programs, in a manner that is interoperable with relevant standards and trust frameworks, does not enable surveillance and tracking by authorities and private parties, and supports user privacy and data minimization.

- It directs the Commissioner of Social Security and the head of any other designated agency to, where possible, adopt the usage of "Yes/No" validation services, also known as attribute validation services, to confirm an individual's identity for the purposes of government-operated identity verification systems and public benefits programs.

- Finally, it directs the Treasury and GSA to develop and conduct a pilot program for technology that notifies individuals when their identity information is used to request a payment from a public benefits program.

Section 6. Promoting Security with and in Artificial Intelligence:

- Section 6 orders the launch of a public-private partnership-driven pilot program to use AI to enhance cyber defense of critical infrastructure in the energy sector, focusing on vulnerability detection, automatic patch management, and identification of anomalous and malicious technology across information technology or operational technology systems.

- It directs the Secretary of Defense to establish a program for use of advanced AI models for cyber defense; NIST, Energy, DHS, and the National Science Foundation (NSF) to prioritize funding for the development of large-scale labeled datasets needed for cyber defense research and the availability of existing datasets to the broader academic research community; NIST, Energy, DHS, and NSF to prioritize research on human-AI interaction methods for defensive cyber analysis, security of AI coding assistance, methods for designing secure AI systems, and methods for responding to cyber incidents involving AI systems.

- Finally, it directs Defense, DHS, and ODNI to incorporate management of AI software vulnerabilities and compromises into their agencies' existing processes and interagency mechanisms for vulnerability management.

Section 7. Aligning Policy to Practice:

- Section 7 mandates revisions to OMB Circular A-130 (Managing Information as a Strategic Resource) to outline expectations for agency cybersecurity information-sharing, be less technically prescriptive in key areas to promote evolving best practices, and address how agencies should mitigate risks to mission essential functions presented by concentration of IT vendors and services.

- It directs NIST, CISA, and OMB to establish a pilot program of a "rules-as-code" approach for machine-readable versions of OMB, NIST, and CISA cybersecurity policies and guidance.

- Finally, it directs NIST to "identify minimum cybersecurity practices" based on common practices and control outcomes across industry, international standards bodies, and other risk management programs. After publication of this guidance, it directs the FAR Council to amend the FAR to require federal government contractors to follow these "minimum cybersecurity standards" when

contracting with the federal government and to require vendors to the government of Internet-of-Things products to carry United States Cyber Trust Mark labeling for their products.

Section 8. National Security Systems and Debilitating Impact Systems:

- Section 8 directs, with certain exceptions, the development of requirements for NSS and debilitating impact systems based on the requirements stated in the entire order.
- It directs the Committee on National Security Systems to review and update relevant policies and guidance regarding space system security and identify requirements to implement cyber defense on federal government procured space NSS.
- Finally, it directs OMB to issue guidance directing agencies to inventory all major information systems and provide the inventory to CISA, DOD, or the National Manager for NSS, which shall also share these inventories with each other.

Section 9. Additional Steps to Combat Significant Malicious Cyber-Enabled Activities:

- Section 9 grants additional sanctions authorities for designating foreign actors for malicious cyber-enabled activities, including unauthorized access or disruption to critical infrastructure or critical infrastructure-supporting computer networks, interference in election institutions and processes, ransomware, misappropriated intellectual property and confidential information, cyber-enabled intrusions, and sanctions evasion.

Key Takeaways

- **Federal Vendors and Contractors Will Need to Prove Compliance with Existing and Heightening Secure Software Development Standards**

  Throughout the Biden administration, the government suffered multiple high-level cyber incidents which ultimately traced back to federal supply chain vulnerabilities, such as SolarWinds and BeyondTrust (which provided the software used by Chinese intelligence to penetrate the Treasury Department in recent weeks). The EO creates a new system of accountability for federal contractors, requiring proof that federal software complies with the government's secure software development standards. Federal contractors should immediately undertake reviews and gap analyses of their internal software development to ensure that they are prepared to attest that supplied software meets government requirements. For those vendors whose software does not meet standards, they may need to prepare to issue software updates to ensure compliance.

- **Increasing Exposure to Enforcement Action Based on False and Misleading Claims About Cybersecurity Practices**

In addition to the new compliance required by the EO, this new attestation system poses additional risk of related enforcement actions. The EO directs that the National Cyber Director should "refer" failed secure software development attestations to the Attorney General for further action. While it is still unclear whether the Trump administration will continue the Civil Cyber Fraud Initiative, this new secure software development attestation system could create a pipeline for DOJ to find and bring False Claims Act cases based on failures to comply with secure software development practices.

If a federal contractor has contractually agreed to follow federal secure software development practices and then either fails to attest or fails to comply with those practices, DOJ will almost certainly open an investigation into potential False Claims Act violations by the company. Federal contractors should immediately review contractual language to determine whether they are bound to meet government secure software development standards and perform gap analyses to determine whether they can attest to their compliance.

Separately, federal contractors will need to undertake reviews of their public statements about their software development practices to ensure that past statements did not mislead investors about the company's compliance with secure software development practices. Failed attestations or failure to comply with these standards may give rise to liability for false or misleading statements about the company's cybersecurity practices and lead to potential SEC or private enforcement.

Finally, alongside the new requirements to prove compliance with secure software development practices, the EO directs the creation of a range of new contractual language on various cybersecurity standards and practices to be inserted into federal contracts. Like with the federal secure software development standards, government contractors should prepare to comply with this new contractual language, lest they run afoul of a new round of False Claims Act enforcement based on these requirements.

- **Opportunities for Federal Vendors of Next Generation Technologies**

  Biden's final executive order is more than just a set of new requirements and standards for federal agencies and contractors, it lays out a roadmap of government priorities for the adoption of new technologies like artificial intelligence, post-quantum cryptography, digital identities, and next-generation authentication. Federal vendors and contractors should prepare for competitive bidding in these high-value areas in the coming months.

- **Potential Sanctions Exposure for Ransomware Payments**

  While Executive Orders 13694, 13757, and 13984 provided authorities for the designation of individuals involved in certain malicious cyber-enabled activities and election interference, the EO expands government authorities to designate individuals and entities involved in ransomware attacks. While companies who agree to pay ransomware payments already risk

exposure to US sanctions, the new authority greatly expands the probability that ransomware payments will be made to designated individuals or entities and, as a result, poses additional risk for companies deciding whether to pay a ransom to end an attack.

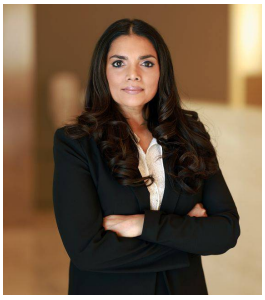
We will continue to monitor developments and provide updates as US federal agencies begin to implement these directives or if the Trump Administration scuttles or otherwise modifies the EO.

Footnotes

[1] Executive Order, *Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity*, (Jan. 16, 2025), https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/.

[2] Executive Order, *Initial Rescissions of Harmful Executive Order and Actions*, (Jan. 20, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions/

Related Attorneys



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605

Philip J. Chertoff
Associate
pchertoff@jenner.com
+1 202 637 6346

Related Capabilities

Data Privacy and Cybersecurity

National Security and Crisis

Stay Informed →