Updates
May 17, 2021

President Biden's Cybersecurity Executive Order Focuses on IT and Software Supply Chain Vulnerabilities

On May 12, 2021, President Biden signed a sweeping Executive Order (EO) to protect federal government networks and software supply chains against increasing threats of attacks from malicious cyber actors, setting the stage for future rulemaking and amendments to the Federal Acquisition Regulation (FAR) focusing on IT and software sold to the government.

Citing the need for the federal government to "partner with the private sector" to protect the nation against cyber threats from nation-state actors and cyber criminals, the EO urges "bold changes and significant investments" in cybersecurity. Among other things, the EO calls for:

- Requiring IT and communication contractors supporting the government to share information with agencies about cyber threats and to report cyber incidents.
- Accelerated adoption of cloud networks and deployment of multifactor authentication and other practices to "modernize" the government's cybersecurity protections.
- New security standards for software sold to the government to address vulnerabilities in software supply chains, including requiring developers to provide greater visibility into their software and make security data publicly available. The order also establishes a consumer labeling program to identify whether software products are securely developed.
- Establishing a Cybersecurity Safety Review Board, co-chaired by government and private sector leads, to analyze significant cyber incidents and make recommendations.
- Cybersecurity event log requirements for federal departments and agencies.

The EO follows a series of high-profile cyberattacks highlighting vulnerabilities in federal and private sector networks, including the ransomware attack on the Colonial Pipeline, resulting in gas shortages earlier this month. Calling this and other recent incidents a "sobering reminder," a White House statement accompanying the EO states that the order is "the first of many ambitious steps" the administration is taking to "modernize" national cyber defenses and respond to cyberattacks.

This update provides an overview of the EO and its implications for federal contractors, including software vendors and IT contractors.

Cyber Incident Reporting and Information Sharing Requirements

Section 2 of the EO calls for removing barriers for IT and Operational Technology (OT) service providers to share cyber threat and incident information with the government to help deter, prevent, and respond to cyber incidents.

According to the EO, IT and OT service providers have "unique access to and insight into cyber threat and incident information on Federal Information Systems" but contract terms or restrictions may limit their ability to share such information with federal departments and agencies responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of

Investigation (FBI).

To remove such barriers, the EO adopts a timeline for changing existing contract clauses through regulatory rulemaking. Within 60 days of the EO, the Office of Management and Budget (OMB) will recommend contract language in the FAR and Defense FAR Supplement (DFARS). Within 90 days of receipt of those recommendations, the FAR Council is directed, as appropriate, to publish amendments to the FAR implementing the reporting requirements.

According to the EO, any recommended contract language must ensure that IT and OT service providers "collect and preserve" certain data "on all information systems over which they have control" and must share such data related to "cyber incidents or potential incidents" with agencies with which they have contracted as well as potentially other agencies. The EO also indicates that service providers will be required to collaborate with investigative agencies.

The EO also directs the establishment of new cyber reporting requirements for "Information and Communication Technology" service providers that contract with the government. It directs the Department of Homeland Security (DHS), in consultation with other agencies, to recommend contract language to the FAR Council to require such contractors to "promptly" report cyber incidents to agencies, CISA, and the FBI within certain time periods (e.g., not to exceed three days for "severe" incidents).

Once the FAR Council publishes a rule, agencies will be required to update their agency-specific cybersecurity requirements to remove any "duplicative" requirements. The EO calls for "standardizing" common cybersecurity contractual requirements across federal agencies.

Prioritized Use of Cloud Services and Other Security Requirements for Federal Agencies

The EO also outlines the need for the federal government to increase its use of cloud services, among other practices to "modernize" the government's approach to cybersecurity.

Section 3 of the EO calls upon agencies to adopt security best practices that include "accelerat[ing] movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS)[.]" Within 60 days of the date of the EO, the head of each agency must update existing plans to "prioritize resources for the adoption and use of cloud technology" and develop a plan to implement Zero Trust Architecture, a security model that eliminates implicit trust in any one element, node, or service.

The EO also requires the development of security principles governing Cloud Service Providers (CSPs) for incorporation into agency modernization efforts. Within 90 days of the order, OMB, CISA, and the General Services Administration (GSA) acting through FedRAMP, must develop a federal cloud-security strategy and provide guidance to agencies. CISA is also directed to develop and issue a cloud-service governance framework within 90 days.

The accelerated shift to cloud-based systems will likely expand opportunities for CSPs to support federal agencies and further encourage contractors to move their networks to the cloud.

The EO also requires agencies, within 180 days, to adopt multifactor authentication and encryption for data at rest and in transit, to the maximum extent possible.

Software Supply Chain Security and Consumer Labeling

The EO lays the groundwork for regulation targeting the security of software in the government's supply chain. Citing a lack of transparency and adequate controls in certain commercial software, Section 4 of the EO states that there is a "pressing need" to implement "more rigorous and predictable" mechanisms to ensure that software products are secure, with a priority on addressing the security and integrity of "critical software," which the EO describes as software that performs functions critical to trust.

The EO directs the National Institute of Standards and Technology (NIST) to issue guidance identifying practices to enhance security of software in the government's supply chain. Such guidance must include standards, procedures, or criteria in ten areas, including secure software development environments, using automated tools to check for vulnerabilities, and creating a "Software Bill of Materials" that records components used in building software. The EO also instructs NIST to develop minimum standards for vendors to use when testing their software source code, including identifying recommended types of manual or automated testing.

Within 30 days of the issuance of NIST's guidance, agencies will be directed to comply with such guidelines when procuring software. Within one year of the date of the EO, DHS, in consultation with other agencies, must recommend contract language to the FAR Council implementing the changes in software supply contracts. After a final rule is issued, agencies will have to "remove" any noncompliant software products from their procurements.

The EO also creates a pilot program to establish an "energy star" type of consumer label so that the government and public can quickly determine whether software and Internet of Things (IoT) devices were developed securely. Within 270 days of the order, NIST, in coordination with the Federal Trade Commission (FTC) and other agencies, must identify criteria for the labeling program. The White House's statement accompanying the EO states: "We need to use the purchasing power of the federal government to drive the market to build security into all software from the ground up."

Cyber Safety Review Board

Section 5 of the EO establishes a new Cyber Safety Review Board charged with reviewing and assessing "significant cyber incidents" affecting federal and nonfederal systems, threat activity, vulnerabilities, mitigation activities, and agency responses. The board will comprise federal officials, including representatives of the DoD, the U.S. Department of Justice (DOJ) , CISA, the National Security Agency (NSA), and the FBI, as well as representatives from "appropriate private-sector cybersecurity or software suppliers" as determined by DHS. According to the White House, the Cyber Safety Review Board is modeled after the National Transportation Safety Board (NTSB), which investigates airplane crashes and other incidents.

Standardizing the Government's "Playbook"

Section 6 of the EO calls for a "standardized" response to cybersecurity vulnerabilities and incidents, citing the fact that varying approaches across agencies hinder the ability of lead agencies to analyze vulnerabilities and incidents more comprehensively. Within 120 days of the EO, DHS is required to adopt a standard set of operational procedures (a "playbook") for agencies to use in planning and conducting cybersecurity vulnerability and incident response.

Final Thoughts

The EO marks a significant step to strengthen—and standardize—cybersecurity protections across the government, signaling the Biden administration's intent to move away from agency-specific policies in favor of a uniform approach with expanded participation from industry.

Many details will need to be worked out through a rulemaking process. IT and software vendors, as well as companies that make internet-connected products, should prepare for an extensive implementation period that ultimately will result in new contract requirements in the FAR.

Agencies will have to move quickly to meet near-term deadlines under the EO, including updating plans to prioritize cloud technology within 60 days and adopting multifactor authentication and encryption for data within 180 days. The development of a cloud-security strategy within 90 days will require coordinating with the FedRAMP cloud-security program.

Other key questions for rulemaking will include to whom the data-sharing requirements will apply, what types of information must be tracked and reported, and how such data will be used and maintained within the government.

Defense contractors monitoring the EO's implementation should also watch for any impact it may have on DoD's interim rule implementing its Cybersecurity Maturity Model Certification (CMMC) program and other initiatives to safeguard data on contractor-managed networks.

Authors

Alexander O. Canizares

Partner
ACanizares@perkinscoie.com 202.654.1769

Explore more in

Government Contracts Technology Transactions & Privacy Law Communications

Related insights

Update

FERC Meeting Agenda Summaries for November 2024

Update

Ninth Circuit Rejects Mass-Arbitration Rules, Backs California Class Actions