wiley

ALERT

Biden's Cyber EO Aims to Improve Federal Security and Move Private Sector

—

May 13, 2021

On May 12, 2021, President Biden issued the long-expected *Executive Order on Improving the Nation's Cybersecurity* ("EO" or "Order"). The EO comes amidst a series of high-profile cyber-attacks on the Nation and its critical infrastructure, Information and Communications Technology (ICT) supply chain providers, and federal contractors, adding a heightened sense of urgency behind its implementation. In the related Fact Sheet the White House notes that "[r]ecent cybersecurity incidents such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident are a sobering reminder that U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals."

Underscoring the desire for swift and comprehensive changes, the Order states "[t]he Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT))."

Described as "the first of many ambitious steps the Administration is taking to modernize national cyber defenses," the Order pulls together a diverse range of moving pieces from across the government and industry, some of it already underway. The EO's key goals are to:

- Remove Barriers to Threat Information Sharing Between Government and the Private Sector.

Authors

—

- Modernize and Implement Stronger Cybersecurity Standards in the Federal Government.

- Improve Software Supply Chain Security.

- Establish a Cybersecurity Safety Review Board.

- Create a Standard Playbook for Responding to Cyber Incidents.

- Improve Detection of Cybersecurity Incidents on Federal Government Networks.

- Improve Investigative and Remediation Capabilities.

Given the range of issues, the EO will have broad impacts across federal government, its contractors, and the private sector. The EO directs several different agencies to begin implementation and establishes tight timelines for their actions, activities that all stakeholders should monitor. Federal contractors should expect significant rulemaking activity by the Federal Acquisition Regulatory (FAR) Council, which is likely to release interim final rules (and then seek public comment) given the aggressive timelines in the EO.

The Private Sector is in Focus, Especially ICT Service Providers and Federal Contractors

Although the Order aims to secure federal government networks—stating that it "must lead by example"—it looks at the private sector as a necessary partner that must also aggressively strengthen security. Impacts of the Order will be felt across the private sector, in particular by federal contractors, cloud providers, software providers and others in the ICT equipment and services ecosystem. The EO states that "[t]he private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace."

In its Fact Sheet, the Administration states "[w]e encourage private sector companies to follow the Federal government's lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents."

Key takeaways for contractors and ICT service providers include:

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas
—

Cyber and Privacy Investigations, Incidents & Enforcement

Cybersecurity

Government Contracts

National Security

Privacy, Cyber & Data Governance

Strategic Competition & Supply Chain

Telecom, Media & Technology

- The EO introduces new key terms, including "critical software" and several categories of "service providers." But the EO defers to implementing agencies to articulate definitions of these terms, and these to-be-determined definitions will largely drive how quickly, and to what extent, the federal government implements the EO's requirements and the scope of the overall impact on entities operating in this space.

- Aspects of the EO, such as those addressing Zero Trust Architecture, a Software Bill of Materials (SBOM), and vulnerability disclosure rest upon multistakeholder work that has been underway at the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA) and elsewhere, but may not have benefitted from the input of all entities that will be impacted.

- The EO accelerates the shift towards and adoption of secure cloud services within civilian government agencies.

- The EO says that existing contracts may "limit the sharing of threat or incident information" with the government. Enhanced information sharing is important, but details need to be spelled out as to under which legal authorities and how that information will be protected.

In addition:

- Companies who work or have worked with the federal government in almost any capacity related to IT, data, software, or networking should review their contracts and prepare to engage agencies and the FAR Council as obligations develop.

- Developers of connected products and services should heed the EO's emphasis on transparency and its direction to the Federal Trade Commission (FTC) to explore consumer security labels.

New Information Sharing and Incident Reporting Requirements for Contractors

First, Section 2 directs the creation of broad cyber incident reporting obligations for "information and communications technology service providers" who contract with the government. The requirement would require reporting of any "cyber incident involving a software product or service provided to such agencies or involving a support system for a software product or service provided to such agencies."

Second, Section 2 directs the creation of information sharing requirements for government contractors who are "IT and OT service providers." Diverging from the current voluntary information sharing regime, the EO would require covered government service providers to, "collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control." Covered service providers would then be required to share such data with the government and collaborate with any federal investigation into incidents and "potential incidents." The EO contemplates that cooperation might include, "implementing technical capabilities, such as monitoring networks for threats."

Third, Section 2 directs the creation of "standardized contract language for appropriate cybersecurity requirements" for contractors. Currently, cybersecurity requirements for contractors are agency-specific, with some agencies—most notably the U.S. Department of Defense (DOD), which requires implementing NIST 800-171 or the Cloud Computing Security Requirements Guide—requiring significantly more burdensome requirements than others. The push to standardize cyber requirements across federal contractors may have significant impacts on contractors who have largely avoided burdensome cyber requirements or who have been subject to piecemeal requirements across various federal agencies.

Section 2 largely directs the FAR Council, working with others across government, to develop contractual terms to implement these requirements. Major questions remain unanswered. For example, "service provider" is not defined, and the EO directs the FAR Council to determine the "scope of contractors and associated service providers to be covered by the proposed contract language."

Modernizing Federal Government Cybersecurity—Cloud, Zero Trust Authentication, MFA and Encryption

Section 3 directs the Federal government to, "take decisive steps to modernize its approach to cybersecurity." Specifically, Section 3 requires the government to:

- Advance toward Zero Trust Architecture as developed by NIST, which released NIST 800-207, *Zero Trust Architecture*, last summer. NIST also has an effort underway to develop an example solution for implementing Zero Trust Architecture.

- Increase usage of secure cloud services, including requiring a reevaluation of FedRAMP that will include "develop[ing] security principles governing Cloud Service Providers [(CSPs)]."

- Adopt multi-factor authentication and encryption for data at rest and in transit across the federal government.

Implementing these cybersecurity practices may significantly alter the security of the federal government—but they are also intended to push the private sector to change its cyber standards.

The White House Fact Sheet points to both the public and private sectors as lagging behind modern security needs stating that, "[o]utdated security models and unencrypted data have led to compromises of systems in the public and private sectors. . . The Federal government must lead the way and increase its adoption of security best practices, including by employing a zero-trust security model, accelerating movement to secure cloud services, and consistently deploying foundational security tools such as multifactor authentication and encryption."

Improving Software Supply Chain Security—SBOM and Labelling

Section 4, "Enhancing Software Supply Chain Security," broadly addresses supply chain issues that have been in the news and incorporates several ideas that thus far have been under development. The EO does not limit its interest to federal contractors and delves into some complicated areas like labeling of consumer devices and software supply chain provenance. In sum, the EO asserts that the government "must take action to

rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software." Section 4 contains mandates for federal agencies, new obligations for the private sector, and notably, it leaves several key concepts to be defined by federal agencies, including NIST.

The EO prioritizes the security of "critical software" but establishes baseline security standards that could eventually apply to the development of all software sold to the government, including requiring developers to maintain greater visibility into their software and make security data publicly available. The guidance to be developed by NIST must address distinct build environments, audits, multifactor authentication, encryption, system monitoring, automated tools for evaluating source code, vulnerability management, among other standards. NIST's guidance also must address verification by purchasers, participation in vulnerability disclosure programs, and provision of a SBOM. Agencies will also face new guidelines and "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."

- Vulnerability disclosure programs have been a subject of increasing interest across government, and have been mandated for certain federal acquisitions, though no uniform approach has been developed.
- SBOM has been an open effort by NTIA at the Commerce Department to develop a consensus approach based on voluntary stakeholder input.

Several key issues are left to be determined by federal agencies. For example, the EO does not define "critical software" and instead directs Commerce, acting through NIST, to do so. That definitional effort is not itself clearly limited to software purchased or used by the government but the EO subsequently requires NIST, after defining "critical software" 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 also contemplates mandatory requirements as refined by, for example, the FAR Council and implementing agencies, that could potentially apply beyond those software products identifies as "critical software." Federal contractors should expect a slew of new obligations from the FAR Council and some transition issues in this area. The EO mandates that agencies "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 removals would have to be accomplished through contract modifications, which will require a significant and complicated undertaking across numerous agencies considering the large number of contracts involved. The EO also contemplates additional guidance from the Office of Management and Budget (OMB) on how to remediate "legacy software" acquired before these requirements take effect. This will likely drive significant contracting activity, as agencies seek to modify current contracts and potentially seek out assistance to remediate older legacy software for which its original contracts have expired.

Section 4 of the EO also delves into the controversial topic of Internet of Things (IoT) device labeling and software labeling. Specifically, NIST must initiate pilot programs, informed by existing consumer product labeling programs, "to educate the public on the security capabilities of [IoT] devices and software development practices." With respect to the software labeling program, the White House explains that the pilot program will "create an 'energy star' type of label so the government – and the public at large – can quickly determine whether software was developed securely," noting that "the purchasing power of the Federal Government [is needed] to drive the market to build security into all software from the ground up." For both pilot programs, the EO instructs NIST to "consider ways to incentivize manufacturers and developers to participate." These pilot programs will be reviewed after a year, and NIST must consult with the private sector in assessing their effectiveness.

In particular, the EO tasks NIST and the FTC with identifying IoT cybersecurity criteria for a consumer labeling program. As part of this effort, NIST is required to "examine all relevant information, labeling, and incentive programs and employ best practices." Of note, NIST earlier this year announced its plans to "work with consumer groups, industry, standards bodies, and other stakeholders to survey options for confidence mechanisms that enable identification of cybersecurity device capabilities in consumer home IoT devices." NIST has also done extensive work—some of which is still underway—on identifying baseline cybersecurity capabilities and non-technical supporting capabilities for IoT devices. It stands to be determined how NIST will leverage this work to meet this new EO requirement.

Establishing a Cybersecurity Safety Review Board

Modeled after the National Transportation Safety Board, which investigates major accidents and transportation incidents, Section 5 establishes a "Cyber Safety Review Board." This Board will be co-chaired by government and private sector leads, that may convene following a significant cyber incident to analyze what happened and make concrete recommendations for improving cybersecurity. The Secretary of the U.S. Department Homeland Security (DHS) will convene the Board following a significant cyber event triggering the establishment of a Cyber Unified Coordination Group (UCG)—which was recently organized in response to the SolarWinds attack. The SolarWinds incident will be the topic of the Board's initial review, for which the Board will provide recommendations for improving cybersecurity and incident response practices.

After this initial review, the Secretary of DHS will provide to the White House the recommendations of the Board related to its composition, authorities, mission, and scope.

Members of the board will include representatives from DOD, the U.S. Department of Justice (DOJ), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) "as well as representatives from appropriate private-sector cybersecurity or software suppliers as determined by the Secretary of DHS." The OMB will also participate in certain circumstances.

Responding to Cyber Incidents—Developing a Playbook

Section 6 directs the creation of a standardized playbook and set of definitions for cyber incident response by federal departments and agencies. "Standardized response processes ensure a more coordinated and centralized cataloging of incidents and tracking of agencies' progress toward successful responses."

Among other things, the playbook "shall incorporate all appropriate NIST standards[,]" and OMB, informed by CISA and the NSA, may issue guidance on agency use of the playbook. Additionally, according to the White House Fact Sheet, the Order intends for the playbook to also "provide the private sector with a template for its response efforts."

Improving Detection of Incidents on Federal Networks

Section 7 directs the government to "employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks." It enables a government-wide endpoint detection and response (EDR) initiative to "support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response."

The section also enhances CISA's ability to collect additional federal agency data and directs enhanced and more responsive information sharing within the government.

Improving Investigative and Remediation Capabilities

Section 8 creates cybersecurity event log requirements for federal departments and agencies. "Information from network and system logs on Federal Information Systems (for both on-premises systems and connections hosted by third parties, such as CSPs) is invaluable for both investigation and remediation purposes. It is essential that agencies and their IT service providers collect and maintain such data and, when necessary to address a cyber incident [on federal systems] provide them [to CISA and the FBI]."

Further, recommendations from DHS and DOJ on the types of logs to be maintained, the time periods to retain the logs and other relevant data, the time periods for agencies to enable recommended logging and security requirements, and how to protect logs will be provided to OMB. "Such recommendations shall also be considered by the FAR Council when promulgating rules pursuant to section 2 of this order."

Conclusion

As highlighted throughout, this Order will have a broad impact on the private sector. It seeks to mandate raising the bar through a series of steps that will aggressively alter the cyber landscape for both the public and private sector.

Wiley's multidisciplinary Privacy, Cyber & Data Governance team has been involved in almost every topic addressed in the EO, from cloud security certifications to incident reporting to the development and use of NIST standards and IoT regulation. The implementation of this EO, like prior cybersecurity EOs in which we

were heavily involved, will generate a great deal of uncertainty and regulatory action across the government.

Our Government Contracts, Telecom, Media & Technology (TMT), and National Security practices work seamlessly to help clients adapt to and shape evolving cyber obligations. Please contact us for more information about any aspect of the EO and its impacts.