Professional Perspective

Implementation Issues of Biden's Cybersecurity EO for Software Vendors

Alexander O. Canizares and Paul Korol, Perkins Coie

Bloomberg Law

Implementation Issues of Biden's Cybersecurity EO for Software Vendors

Contributed by Alexander O. Canizares and Paul Korol, Perkins Coie

President Joe Biden's May 12, 2021 Executive Order on Improving the Nation's Cybersecurity (EO 14028) calls for urgent actions to strengthen the government's protections against increasingly sophisticated and damaging cyber threats. Among the objectives of EO 14028 is to safeguard the security and integrity of software supply chains.

Citing a "pressing need" to make the development of commercial software more transparent and resistant to attack and malicious tampering, EO 14028 calls for new guidance related to software security, with a focus on a new category of "critical software." The implementation process is already well underway, and software developers and vendors that support the federal government should expect the government to issue new software security standards and requirements in late 2021 and 2022.

This article provides an overview of EO 14028 and its significance for companies that sell software to the government, focusing on key issues for contractors to consider in anticipation of changes.

Enhancing Software Supply Chain Security

In response to the SolarWinds incident and other high-profile cyberattacks against U.S. companies and federal agencies, EO 14028 calls for sweeping changes and investments to protect U.S. government systems and networks, which rely heavily on contractor-furnished information technology and operational technology. The EO sets ambitious deadlines for implementation by agencies—as well as the promulgation of regulations to amend the Federal Acquisition Regulation (FAR) and the Defense FAR Supplement (DFARS)—resulting in new contract requirements for government contractors.

Section 4 of the EO focuses on enhancing software supply chain security. It directs agencies to implement "more rigorous and predictable" mechanisms to secure software and software components against cyber threats. As explained below, among the areas of focus for the National Institute of Standards and Technology (NIST) and other agencies are new standards for "critical software," secure software development and testing, a "Software Bill of Materials" requirement, and a software consumer labeling program.

Critical Software

The EO makes the protection of "critical software"—i.e., software critical to trust—a priority for the federal government. Section 4(g) of the EO directs NIST to develop a definition of "critical software" that ultimately will be incorporated into the standards required under the EO.

After hosting a public workshop and consulting with other agencies, NIST issued on June 25, 2021, the following definition:

EO-critical software is defined as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

- Is designed to run with elevated privilege or manage privileges
- Has direct or privileged access to networking or computing resources
- Is designed to control access to data or operational technology
- Performs a function critical to trust
- Operates outside of normal trust boundaries with privileged access

NIST's definition of "critical software" focuses on the function of software's components, as opposed to how an agency uses the software. Examples cited by NIST include an operating system for a server, desktop, or mobile device, as well as software that performs remote scanning looking for vulnerabilities. According to NIST, "critical software" includes both standalone software and software integral to specific devices or hardware. It applies to products located on-premises as well as in cloud-based environments. Open-source software can be critical too.

On July 9, 2021, NIST published proposed security measures for agencies' use of "critical software," focusing on five objectives, including protecting critical software and software platforms from unauthorized access and usage, and quickly detecting, responding to, and recovering from threats and incidents. NIST says that its security measures are components of a "zero trust architecture" approach, which the EO separately requires agencies to adopt.

NIST's guidance regarding "critical software" is not binding on contractors, but it is likely to become a procurement issue. On Aug. 10, 2021, the Office of Management and Budget (OMB) issued a memo directing agencies to identify all critical software they currently use or are in the process of acquiring within 60 days. The memo further directed agencies to implement NIST's security measures by Aug. 10, 2022. Vendors should thus expect that software falling into this broad category of "critical software" will be subject to heightened requirements in future procurements.

Software Development, Testing & Verification

The EO also sets in motion efforts to develop practices and processes for the development and testing of software to make it more secure and resilient against cyber threats.

The EO directs NIST to issue guidance identifying practices that enhance the security of software supply chains by February 2022, with preliminary guidance due in November 2021.

The guidance will focus on practices related to the development and testing of software sold to agencies, including security testing of software and tools, screening of software for vulnerabilities, and determining how developers can prove compliance. A rulemaking process to adopt guidance into binding regulations is expected to start in May 2022.

Significantly, the EO requires that, following the issuance of any final rule amending the FAR on these issues, agencies shall, "as appropriate and consistent with applicable law," remove software products that do not meet the new requirements from all Indefinite Delivery/Indefinite Quantity (ID/IQ) contracts, Federal Supply Schedules, and other multiple-award contracts.

On July 9, 2021, after conducting a public workshop and soliciting position papers, NIST issued additional guidelines recommending minimum standards for vendors to use when testing (verifying) source code, addressing threat modeling, automated testing, fixing bugs, and other steps. The guidelines are voluntary, but NIST says that it expects them to serve as a basis for "mandated standards in the future."

On September 8, 2021, OMB released a draft memo for public comment outlining the federal "Zero Trust Architecture" strategy, which includes several considerations for software applications used by agencies. For example, the memo directs agencies to treat every application they use as if it were internet-accessible. The memo further states that the Cybersecurity & Infrastructure Security Agency (CISA) and the General Services Administration (GSA) will collaborate on creating a procurement structure to allow agencies to rapidly procure external security testing services for agency applications.

Software Bill of Materials

The EO specifically instructs NIST's guidance to address a "Software Bill of Materials" (SBOM) that would be provided to the government for each product or published on a public website. An SBOM is a human or machine-readable accounting of each component of given software. Like a list of ingredients on a packaged food item, an SBOM can include component-specific details such as where a component came from, who authored it, and its version number.

According to the EO, obtaining an SBOM for software is crucial because it helps reduce the risk of an agency installing software with known, exploitable vulnerabilities. An SBOM requirement has significant implications for software vendors, particularly those supporting IT and OT systems, and potentially systems integrators and resellers.

Section 4 tasks the National Telecommunications and Information Administration (NTIA) with responsibility for the development of the minimum requirements for an SBOM. In accordance with the EO, on July 12, 2021, the NTIA issued guidance outlining the minimum criteria for an SBOM as well as recommendations for related practices and processes. If an SBOM requirement ultimately becomes mandatory, it would create a new consideration for companies bidding on government contracts and for agencies conducting competitive source selections.

Consumer Labeling Pilot Programs

The EO also directs NIST to develop new consumer labeling pilot programs to educate the public on the security capabilities of Internet of Things (IoT) and software development practices. The consumer labeling system would be similar to the government's Energy Star program for energy-efficient products and devices. NIST is required to identify the cybersecurity criteria to be used in the labeling programs in February 2022.

At least in theory, consumer labeling has the potential to change behavior by driving consumers toward more secure devices and software. The idea is that companies that do not participate in the program risk being at a competitive disadvantage in the marketplace. The EO directs NIST to consider ways to "incentivize" manufacturers and developers to participate in the programs.

Key Considerations for Software Companies

While the implementation of Section 4 of the EO is still in its early stages, its impact for companies that sell software to the government is likely to be significant—and potentially will extend beyond government contractors to commercial software developers and vendors.

The following are key issues for companies to consider as they prepare for the impending changes.

- Government contractors should review guidance and proposed standards issued to date, including NIST's definition of critical software, and consider the implications for their products. They should also anticipate that federal agencies will take actions on their own, including inserting software security requirements into their procurements. The concept of "critical software" will thus likely become important in competitive procurements.

- Section 4 of the EO presents a range of procurement and legal issues that will affect software suppliers to federal agencies, as well as resellers, higher-tier subcontractors, and prime contractors that furnish software made by others to federal agencies. Companies at all tiers of the supply chain should expect to grapple with "flow down" issues, especially to the extent that prime contractors demand more transparency from their vendors.

- The EO is plainly intended to change industry behavior, declaring that the "private sector must adapt" to the changing threat environment. The EO seeks to leverage the government's purchasing power to strengthen security practices among contractors. The impact of the EO on the commercial software industry remains uncertain.

- The SBOM may present challenges for industry. Systems integrators and resellers of software without access to details about acquired software components should consider the implications of an SBOM requirement for their supply chains of software. The SBOM also raises intellectual property issues for companies, many of which may be wary about disclosing details to the government or to the public about their software.

- Given the longer lead time on the development of the consumer labeling pilot programs, there may be opportunities for public comment on the criteria or structure of the programs. For example, NIST held a "virtual public workshop on challenges and practical approaches to initiating cybersecurity labeling efforts" for IoT devices and consumer software in September 2021. Companies with an interest in these issues should be on the lookout for further opportunities for public comment.

To help companies track further developments and anticipate future requirements, the following is a timeline of agency actions to be taken under Section 4 of the EO.

Section 4 of EO 14028 – Key Deadlines		
Expected Date	**Agency**	**Description**
November 2021	NIST	Publish preliminary guidelines on secure software development standards.

February 2022	NIST	Publish final guidelines on secure software development standards.
February 2022	NIST	Identify IoT cybersecurity criteria and secure software development criteria for consumer labeling pilot programs.
March 2022	OMB	Take steps to ensure federal agencies comply with NIST's secure software development standards.
May 2022	NIST	Publish additional guidelines on secure software development standards, including a procedure for periodically reviewing and updating the guidelines.
By May 12, 2022	NIST	Conduct a review of consumer labeling pilot programs and determine what improvements can be made going forward.
By May 12, 2022	Department of Homeland Security (DHS)	Recommend contract language to require government contractors to comply with standards issued under Section 4 of the EO.
Sometime after May 12, 2022	Federal Acquisition Regulatory Council	Propose amendments to the Federal Acquisition Regulation based on DHS recommendations.