WESTLAW TODAY
powered by Reuters

New cybersecurity executive order emphasizes enhancing software supply chain security

By Mario Mancuso, Esq., Sanjay Mullick, Esq., and Jeremy Iloulian, Esq., *Kirkland & Ellis LLP*

MAY 24, 2021

On May 12, 2021, President Biden signed the Executive Order on Improving the Nation's Cybersecurity[1] ("Executive Order"), a sweeping set of proposals.

Though the Executive Order contains many important elements, a key point is software supply chain security, where the Department of Commerce ("Commerce") principally through the National Institute of Standards and Technology ("NIST") is charged with establishing and implementing new standards and practices, which generally become binding within approximately one year.

> The Executive Order establishes that the "prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security."

Though strictly these criteria will apply to software sold to the U.S. federal government, as a practical matter they are likely to inform the security requirements that software developers will have to adhere to for software sold in the commercial market as well.

THE VIEW FROM WASHINGTON

The Executive Order establishes that the "prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security." A Fact Sheet[2] released by the White House with the Executive Order states that "U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals."

The last year alone has seen a series of significant and impactful incidents and attacks from cybercriminal groups believed to be in China and Russia.

The U.S. government has already been taking steps to restrict foreign-origin items (particularly from China and Russia) from the U.S. supply chain out of concern they pose vulnerability risks to U.S. critical infrastructure and government networks.

For example, the National Defense Authorization Act[3] ("NDAA") restrictions prohibit federal government contractors using certain telecommunications and video surveillance equipment and services from certain Chinese companies, and Commerce's emerging regulatory regime on Information and Communications Technology and Services[4] restricts transactions with "foreign adversaries" (*e.g.,* China, Russia).

Though neither the Fact Sheet nor the Executive Order identifies any countries, this new initiative to "modernize national cyber defenses" in part can be seen as related to those.

ELEVATED SOFTWARE STANDARDS AND PRACTICES

The Executive Order outlines a series of cybersecurity measures, including enabling a government-wide endpoint detection system to actively monitor for malicious cyber activity on federal networks and implementing "Zero Trust Architecture"; requiring reporting to the government of certain cybersecurity breaches impacting government networks; and creating a standardized playbook for responding to cyber incidents.

It emphasizes that "the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software." Accordingly, the Executive Order calls for establishing criteria to evaluate software security practices (including those of software developers and suppliers), defining and identifying critical software, and testing source code.

ISSUING GUIDANCE ON SECURITY PRACTICES

Within 180 days (*i.e.*, November 8, 2021), NIST is required to publish preliminary guidelines for enhancing software supply chain security. 90 days thereafter, NIST is required to "issue guidance identifying such practices" with a goal of achieving baseline security standards and increased transparency.

Core elements include:

Trust: Creating secure software development environments by (i) using administratively separate build environments; (ii) auditing trust relationships; and (iii) establishing multi-factor, risk-based authentication and conditional access across an enterprise.

Automation: Using automated tools to maintain trusted source code supply chains and check for known and potential vulnerabilities and remediate them.

Encryption: Employing encryption for data both at rest and in transit.

30 days after the aforementioned guidance is issued (*i.e.*, up to 300 days after the Executive Order or March 8, 2022) the Office of Management and Budget ("OMB") is required to take steps to mandate agencies comply with the security guidelines, absent extensions or waivers, accompanied by a plan for meeting the underlying requirements and mitigating any potential risks.

For legacy software, i.e., that developed and procured prior to the Executive Order, OMB generally shall require agencies employing it to either comply with the same requirements or provide a plan for meeting or remediating them.

IDENTIFYING "CRITICAL SOFTWARE"

Within 45 days (*i.e.*, June 26, 2021) Commerce will define what constitutes "critical software," and 30 days thereafter, the Department of Homeland Security ("DHS") through the Cybersecurity and Infrastructure Security Agency ("CISA") is required to identify a list of categories of software and software products in use or in the acquisition process considered "critical software."

Simultaneously, within 60 days (*i.e.*, July 11, 2021) Commerce through NIST is required to publish guidance outlining critical software security measures.

TESTING SOURCE CODE

Within 60 days (*i.e.*, July 11, 2021), Commerce is required to publish guidelines recommending minimum standards for vendors' testing of their software source code. This includes identifying recommended types of manual or automated testing, such as code review tools, static and dynamic analysis, software composition tools, and penetration testing.

IMPACTS ON INDUSTRY

The focus of the Executive Order is the federal government's own network, and it acknowledges (absent legislation) the federal government can only "encourage" the private sector to follow its lead, even where the private sector owns and operates critical infrastructure.

Notwithstanding that limitation, given the importance of federal procurement, the Executive Order contains many measures that in practice will use the government market as a lever "to drive the market to build security into all software."

ATTESTING TO COMPLIANCE BENCHMARKS

Within one year (*i.e.*, May 11, 2022), DHS shall recommend to the Federal Acquisition Regulatory ("FAR") Council (which assists with coordinating federal government procurement policy) contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, the software security requirements. Once amended, agencies shall begin to "remove software products that do not meet the requirements."

The Executive Order calls for the establishment of a Cyber Safety Review Board comprising public and private sector officials and tasked with reviewing significant cyber incidents, similar to how a transportation review board does after major accidents.

In the event of such a cyber incident, a software developer that made an attestation and whose product then was found not to meet the applicable security requirements could suffer significantly adverse reputational impacts.

COMPLYING WITH CONTENT DISCLOSURE REQUIREMENTS

The Executive Order will require vendors to provide a U.S. government purchaser with a "Software Bill of Materials" ("SBOM") (a "formal record containing the details and supply chain relationships of various components used in building software") for each product, either directly or by publishing it on a public website.

Given the importance of federal procurement, the Executive Order contains many measures that in practice will use the government market as a lever "to drive the market to build security into all software."

It notes that obtaining one and using it to analyze vulnerabilities is "crucial in managing risk" for software developers, buyers, and operators. Commerce is required to list the minimum elements of a SBOM within 60 days (*i.e.*, July 11, 2021).

The Executive Order and Fact Sheet provides that such a regime is necessary because developers often use open source and third-party software components to create a product, and "[t]oo much of our software, including critical software, is shipped with significant vulnerabilities that our adversaries exploit."

As discussed above, there is increasing suspicion and regulation of goods, software, and services from "foreign adversaries" in the U.S. supply chain. Whether such developers would comply with the transparency an SBOM would require remains to be seen, but not doing so may result in being shut out of the U.S. market.

GETTING A CONSUMER RATING LABEL

The Executive Order envisions creation of a consumer labeling program (like an "Energy Star" rating) to inform and educate the public about the security of "Internet-of-Things (IoT) devices and software development practices," to rate manufacturers and developers accordingly.

Within 270 days (*i.e.*, February 6, 2022), NIST is required to identify IoT cybersecurity criteria and secure software development practices for such a consumer labeling program, perhaps contributing to a "tiered software security rating system." Participating software developers would seem apt no longer to maintain obsolete programs after making security improvements.

KEY TAKEAWAYS

The Executive Order outlines a robust set of standards and practices to be established and implemented across a whole host of areas to safeguard U.S. cybersecurity;

The key focus area of software supply chain security seems to dovetail with other U.S. government initiatives to regulate use of foreign items in U.S. systems and networks;

Though this effort is directed at the federal government, the importance of this market is likely to have a ripple effect on the commercial market and catalyze upgrades there as well;

For those involved in the software industry, the need to meet a higher bar of security is forthcoming in order to remain competitive in the marketplace and try to avoid legal and reputational risk in the event of a cybersecurity incident.

Notes

[1] https://bit.ly/3ysQaMu

[2] https://bit.ly/3ff7b5t

[3] https://bit.ly/3bPfF0U

[4] https://bit.ly/34d9P5m

This article was published on Westlaw Today on May 24, 2021.

ABOUT THE AUTHORS



Mario Mancuso (L) is a partner at **Kirkland & Ellis LLP** and leads the firm's International Trade and National Security Practice. He focuses on guiding private equity sponsors and companies through the Committee on Foreign Investment in the United States process and resolving crises involving economic sanctions and export control-related investigations by the U.S. government. He can be reached at mario.mancuso@kirkland.com. **Sanjay Mullick** (C) is a partner with the firm, focused on representing clients in investigative, regulatory and transactional matters related to economic sanctions, export and import controls, anti-money laundering and anti-corruption. He can be reached at sanjay.mullick@kirkland.com. **Jeremy Iloulian** (R) is an associate who advises clients globally on complex cross-border transactional, regulatory and investigative matters that touch U.S. national security, foreign investment and international trade. He can be reached at jeremy.iloulian@kirkland.com. All the attorneys are based in the firm's Washington, D.C., office.