SULLIVAN & CROMWELL LLP

S&C memo

May 14, 2021

President Issues Executive Order on Improving the Nation's Cybersecurity

Sweeping Order Aims to Improve and Modernize the United States' Cybersecurity Defenses in Partnership With the Private Sector

SUMMARY

On May 12, 2021, President Biden issued an Executive Order on Improving the Nation's Cybersecurity (the "Order") aimed at improving the nation's ability to identify, deter, protect against, detect and respond to malicious cyber activity in the face of "persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy."[1] The Order requires a series of "bold changes" and "significant investments" in cybersecurity, including by requiring: (i) that certain service providers collect, preserve and share with the government certain cybersecurity information; (ii) the development of a set of cybersecurity best practices to which federal agencies must adhere, including moving toward Zero Trust Architecture[2] and secure cloud services, requiring multi-factor authentication and encryption of data in transit and at rest across all federal agencies, and making significant investments in technology and cybersecurity personnel; (iii) the establishment of baseline security standards for the development of software sold to the federal government, which will include requiring developers to provide greater visibility into their software and to make security data publicly available; (iv) the establishment of a national Cybersecurity Safety Review Board, co-chaired by private sector representatives, with a mandate to investigate significant cyber incidents; (v) the development of a standardized playbook for the federal government's cyber incident responses; and (vi) the deployment of "endpoint detection and response" software and tools throughout the federal government to encourage early detection and response to cyber incidents.

The Order has been a focus of the Biden Administration. It follows a recent string of significant cybersecurity attacks harming U.S. national security and the private sector, including the compromise of software manufactured by SolarWinds Corp that enabled breaches at U.S. federal agencies and major technology

companies, the compromise of Microsoft Exchange, used throughout the public and private sectors, and the ransomware attack last week against Colonial Pipeline Co. that disrupted nearly half of the East Coast's delivery of diesel, gasoline, and jet fuel.

Notably, in announcing the Order, the White House stated that it "encourage[s] 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."[3] The Order specifically calls on the private sector to "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."[4]

The Order may have significant implications for private companies. While the standards the federal government develops as a result of the Order will not be required throughout the private sector, they may become de facto standards to which private companies look when designing their own security systems and, in related industries, regulators look in reviewing cybersecurity programs. In addition, through the creation of a national board to investigate certain cyber incidents and the imposition of heightened evidence-sharing and self-certification requirements for certain private companies that act as vendors to the federal government, the Order suggests there will be heightened visibility and public scrutiny of cybersecurity at those companies, as well as with respect to nationally significant cyber incidents involving all private companies, in the future.

EXECUTIVE ORDER

The Order requires enhancements primarily in six key areas, with implications for the private sector.

A. REMOVING BARRIERS TO SHARING INFORMATION

The Executive Order requires that, within 60 days, the Director of the Office of Management and Budget ("OMB"), in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence ("DNI"), review and recommend updates to contractual requirements for third-party information technology ("IT") and operational technology ("OT") service providers, including cloud service providers. Specifically, these companies will be required to: (i) collect and preserve information "relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control"[5]; (ii) share such information, as it relates to actual or potential cyber incidents relevant to any agency with which they have contracted, directly with the contracting agency and any other appropriate agency, "consistent with applicable privacy laws, regulations, and policies"[6]; (iii) collaborate with federal cybersecurity or investigative agencies in their respective investigations of, and responses to, actual or potential incidents on federal information systems, including by sharing relevant data using industry-recognized formats for incident response and remediation[7]; and (iv) "share cyber threat and incident information with agencies, and doing so, where possible, in industry-recognized formats for incident response and remediation.[8]

The Order further announces that "information and communications technology (ICT) service providers entering into contracts with agencies must promptly report to such agencies when they discover a 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."[9] To effect these requirements, within 45 days, the Secretary of Homeland Security, in consultation with the Attorney General, and the Director of OMB, among others, must provide contractual language regarding: (i) the type of information to be reported; (ii) the time periods within which contractors must report cyber incidents based on severity (notably, the Order requires that the most severe cyber incidents be reported within three days after detection); and (iii) the contractors and associated service providers covered by the recommendations.[10]

The Order further requires cybersecurity requirements for unclassified systems contracts, including cloud-service cybersecurity requirements, to be standardized across all agencies of the federal government.

B. MODERNIZING FEDERAL GOVERNMENT CYBERSECURITY

Intended to increase the federal government's visibility into cyber threats, while recognizing privacy and civil liberties protections, the Order requires the federal government to adopt security best practices, including by moving towards "Zero Trust Architecture," prioritizing resources for the adoption and use of cloud technology, developing a cloud-security strategy, centralizing and streamlining cybersecurity data access to drive analytics to identify and manage cybersecurity risks, and investing in technology and personnel consistent with these goals.[11] The Order further requires that all federal agencies adopt within 180 days multi-factor authentication and encryption for data at rest and in transit.[12]

To help ensure a secure migration to cloud technology, the Order requires the Secretary of Homeland Security, in consultation with others, to develop security principles governing private Cloud Service Providers ("CSPs").[13] The Order sets out a timeline for developing a cloud-security strategy, providing relevant guidance to agencies, issuing cloud-security technical reference architecture documentation that illustrates recommended approaches to cloud migration and data protection, issuing a cloud-service governance structure, and evaluating and reporting on the types and sensitivity of each agency's unclassified data.[14] In addition, the Order mandates the development of a framework for the collaboration among certain agencies on cybersecurity and incident response activities related to cloud technology to allow for effective information sharing among the agencies and between the agencies and CSPs.[15]

C. ENHANCING SOFTWARE SUPPLY CHAIN SECURITY

The Order notes that "[t]he development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended."[16] To meet this need, the Order requires the Secretary of Commerce, within 30 days, to solicit input from the federal government, private sector, academia and other appropriate actors to identify existing or develop new standards, tools and best practices for complying with

new guidance that will be issued to identify practices that enhance the security of the federal government's software supply chain.

The new guidance required by the Order will include standards and requirements regarding: (i) secure software development environments; (ii) generating and, when requested by a purchaser, providing artifacts that demonstrate conformance to the guidance; (iii) employing automated tools or processes to maintain trusted source code supply chains and to check for and remediate known and potential vulnerabilities; (iv) providing, when requested by a purchaser, artifacts of the execution of those tools and processes, and making publicly available a summary description of the risks assessed and mitigated; (v) maintaining accurate and up-to-date data, provenance of software code or components, and controls on internal and third-party software components, tools and services, and performing audits and enforcement of these controls; (vi) providing a purchaser a Software Bill of Materials for each product; (vii) participating in a vulnerability disclosure program that includes a reporting and disclosure process, and attesting to conformity with secure software development practices; and (viii) ensuring and attesting, to the extent practicable, to the integrity and provenance of open-source software used within any portion of a product.[17]

Notably, the Biden Administration stated, in issuing the Order, that an intention in requiring these supply chain enhancements is to incentivize the private market, through federal procurement contracts, "to develop new and innovative approaches to secure software development."[18] Thus, for example, in requiring software vendors to self-certify as to conformity with these baseline security standards—the Biden Administration stated that it envisions a form of consumer labeling so that both the government and the public will know that the software was developed securely.[19]

D. ESTABLISHING A CYBER SAFETY REVIEW BOARD

The Order calls for the establishment of a Cyber Safety Review Board ("CSRB"). Modeled, after the National Transportation Safety Board, which investigates and makes recommendations following transportation incidents, including airplane crashes, the CSRB will convene following certain significant cyber incidents affecting either federal or private sector systems. The CSRB will be co-chaired by representatives from the Department of Defense, CISA, the Intelligence community and the Department of Justice (and, where appropriate, OMB), as well as private sector leaders, including in the areas of cybersecurity and software. The CSRB will analyze the relevant incident—as well threat activity, vulnerabilities, mitigation activities, and agency responses—and make recommendations for systems and infrastructure changes to prevent, to the extent possible, future cybersecurity events.[20]

The Order also provides the CSRB's first mandate—a review of the SolarWinds compromise—and orders the CSRB to provide its recommendations for improving cybersecurity and incident response practices to the Secretary of Homeland Security within 90 days.[21]

E. STANDARDIZING THE FEDERAL GOVERNMENT'S PLAYBOOK FOR RESPONDING TO CYBERSECURITY VULNERABILITIES AND INCIDENTS

Given the varied cybersecurity vulnerability and incident response procedures employed by federal agencies—a factor that hinders a comprehensive cybersecurity defense—the Order seeks to establish a standardized playbook and set of definitions for the federal government's cyber incident responses to allow "more coordinated and centralized cataloging of incidents and tracking of agencies' progress toward successful responses."[22] The playbook empowers the Director of CISA to review and validate an agency's incident response and remediation results and recommend the use of another agency or a third-party incident response team where appropriate.[23]

F. IMPROVING DETECTION OF CYBERSECURITY VULNERABILITIES ON FEDERAL GOVERNMENT NETWORKS AND THE FEDERAL GOVERNMENT'S INVESTIGATIVE AND REMEDIATION CAPABILITIES

The Order establishes a government-wide Endpoint Detection and Response ("EDR") initiative.[24] Endpoint detection and response software and tools, which have been adopted with particular frequency following the risk of ransomware attacks, generate warnings when a system detects a possible compromise, improving the user's ability to proactively contain and remediate malicious cyber activity. Relatedly, the Order directs the federal government to "employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks" and identify a timeline for doing so.[25]

Recognizing that importance of network and system logs in addressing cybersecurity incidents, the Order mandates certain cybersecurity event logs be maintained by federal agencies and their IT service providers.[26] The Order provides for the encryption and protection of this data, along with requirements that the data be maintained in a manner consistent with privacy laws and regulations.[27]

Finally, the Order requires the Secretary of Defense to adopt requirements for national security systems that meet or exceed all requirements in the Order.

IMPLICATIONS

The Order recognizes the seriousness and pervasiveness of the threat posed by malicious cyber activity. In issuing the Order, the White House characterized the sweeping changes it requires as essential "to defend the vital institutions that underpin the American way of life," and yet just "the first of many ambitious steps the Administration is taking to modernize national cyber defenses." The Order makes clear that it is intended to "bring to bear the full scope of [the federal government's] authorities and resources to protect and secure its computer systems."

Through the Order, the Biden Administration is also seeking to encourage private sector companies to enhance their own cybersecurity defenses. As the White House stated in issuing the Order, "[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." The Order has implications that are intended, and can be expected, to reach well beyond the specific requirements that the Order imposes on federal agencies and their vendors and suppliers in the private sector.

As an example, the Order's establishment of baseline cybersecurity standards and norms for all agencies of the federal government can be expected to have effects outside the government. Companies may look to these standards for guidance as they consider the cybersecurity standards they may wish to meet and require their service providers to meet. Indeed, in issuing the Order, the White House specifically invited companies to look to these standards, noting, for example, that the incident response playbook with which federal agencies will be required to comply "will also provide the private sector with a template for its response efforts." Similarly, in requiring providers of software to the federal government to publicly self-certify their compliance with new software supply chain standards, the White House stated that it envisions the self-certification as "an 'energy star' type of label so the government—and the public at large—can quickly determine whether software was developed securely."

A similar phenomenon occurred after the Obama Administration issued Executive Order 13636 in 2013, pursuant to which the National Institute of Standards and Technology ("NIST") was required to develop a Cybersecurity Framework to assess cyber risk and maturity for critical infrastructure. The resulting Cybersecurity Framework, which is only voluntary for the private sector, has become widely adopted in the intervening years throughout the private sector in the U.S. and abroad, a fact the Biden Administration presumably had in mind in issuing the Order.

The Order reiterates the long-expressed views of the federal government, through multiple administrations, that cybersecurity for the public and private sectors can only be achieved through a partnership between those sectors. In encouraging the private sector to elevate its cybersecurity standards, and requiring the federal government to lead by example, however, the Order may ultimately create certain challenges for companies in the private sector. Among other things, establishing baseline cybersecurity standards for all federal agencies and certain service providers may potentially affect the future views of courts, investigative agencies, and civil litigants as to the cybersecurity norms and standards that should apply to the private sector more broadly. In situations where companies' standards were less than those required by the Order, for example, private plaintiffs and regulators may attempt to point to the standards required by the Order in an effort to establish a baseline of what was reasonable. Similarly, the creation of the CSRB will, by definition, lead to enhanced public scrutiny of companies involved in certain significant cybersecurity

incidents, and the requirement that certain service providers report certain actual and potential cyber incidents to the government increases the likelihood of public scrutiny and litigation arising out of those incidents.

* * *

ENDNOTES

1 *See* Exec. Order No. 14,208 at § 1 (May 12, 2021), https://public-inspection.federalregister.gov/2021-10460.pdf.

2 As defined in the Executive Order, "Zero Trust Architecture" refers to:

> "[A] security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity." *Id*. at § 10(k).

3 *See* THE WHITE HOUSE, *FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks*, *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/.

4 Exec. Order No. 14,028 at § 1.

5 *Id.*

6 *Id*. § 2(c)(ii).

7 *Id*. § 2(c)(iii).

8 *Id*. § 2(c)(iv).

9 *Id*. § 2(f)(i). The service providers must also report any cyber incidents to CISA when the agency at issue is a Federal Civilian Executive Branch ("FCEB") agency (which includes all agencies except for the Department of Defense and agencies in the Intelligence Community). *Id*. § 2(f)(ii).

10 *Id*. § 2(g).

11 *Id*. § 3.

12 *Id*. § 3(d).

13 *Id*. § 3(c).

14 *Id*.

15 *Id*. § 3(e).

16 *Id*. § 4(a).

17 *See Id*. § 4(e).

18 *See* THE WHITE HOUSE, *supra* note 3.

19 *See* Exec. Order No. 14,028 at § 4(r)–(x).

20 *Id*. § 5(a)–(c).

21 *Id*. § 5(d).

22 *Id.* § 6(a).

23 *Id.* § 6(f).

ENDNOTES (CONTINUED)

[24] *Id.* § 7(b).

[25] *Id.* § 7(a).

[26] *Id.* § 8.

[27] *Id.* § 8(b).

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.