January 17, 2025

White House Releases Executive Order to Strengthen and Promote Cybersecurity Innovation

On January 16, 2025, the White House released an Executive Order on "Strengthening and Promoting Innovation in the Nation's Cybersecurity," finalizing an effort to strengthen cybersecurity defenses throughout the federal government. The Order emphasizes cybersecurity requirements in federal contracting and use of third-party software, as well as steps to shore up security protections for federal communications. Further, the Order calls on the National Institute of Standards and Technology ("NIST") to identify minimum cybersecurity practices to be included in federal contracts, creates mechanisms for the Cybersecurity and Infrastructure Security Agency ("CISA") to access data from federal civilian agencies for threat-hunting purposes, and expands sanctions authority for persons connected to cybercrimes.

While significant uncertainty remains regarding whether the incoming Trump administration will retain the Order in part or in its entirety, it illustrates the federal government's continued emphasis on strengthening cybersecurity, particularly in light of the recent discovery that Chinese state-sponsored hackers breached the Treasury Department and several telecommunications networks.[1] Although the impact of the proposed updates to federal procurement rules, if implemented, will most directly impact government contractors, all companies should monitor updated guidance from NIST and other agencies, as this guidance also has influenced cybersecurity standards in the private sector.

Background

The Executive Order is the latest in a line of efforts by the Biden administration to continue strengthening cybersecurity at the federal level. Early in the administration, on May 12, 2021, President Biden signed Executive Order 14028, which stated the policy that cybersecurity is a "top priority and essential to national and economic security," and instructed federal agencies to take steps to strengthen their cybersecurity measures, improve information-sharing about threats with contractors, and prepare guidance regarding security in software development, among other steps.[2] The administration also updated the White House's National Cybersecurity Strategy, which included efforts to improve cybersecurity, incentivize private investments in cybersecurity and collaboration with the public sector, and marshal the federal government to counteract threat actors.[3] Consistent with these strategies, federal entities have pursued dedicated cybersecurity efforts, including the Disruptive

1 *See* Sean Lyngaas, *Chinese Hackers Breached US Government Office that Assesses Foreign Investments for National Security Risks*, CNN (Jan. 10, 2025), available here; Ellen Nakashima, *Biden Administration Looks to Penalize Salt Typhoon Telecom Hackers*, THE WASHINGTON POST (Jan. 13, 2025), available here.

2 The White House, *Executive Order 14028 on Improving the Nation's Cybersecurity* (May 12, 2021), available here (the "Order").

3 Paul, Weiss Client Alert: *Biden Administration Announces Updated National Cybersecurity Strategy* (Mar. 13, 2023), available here; *see also* Paul, Weiss Client Alert: *White House Signals Additional Private Sector Cyber Obligations as Part of National Cybersecurity Strategy Implementation Plan* (July 19, 2023), available here.

Technology Strike Force led by the Departments of Justice and Commerce,[4] and the U.S. Cyber Trust Mark, a voluntary cybersecurity labeling program created by the FCC for wireless consumer Internet of Things ("IoT") devices.[5]

The Executive Order

The Order contains detailed instructions for federal agencies and seeks to leverage the government's procurement power to foster adoption in the private sector. In a press call preceding the release of the Order, Anne Neuberger, the outgoing Deputy National Security Advisor for Cyber and Emerging Technology, framed the Order in the context of recent cyberattacks, explaining that the "goal was to better understand how to better protect and secure these systems and stay ahead of new threats," after "carefully reviewing each hacking incident to determine exactly how the Chinese, other governments and criminals got through the gates."[6] The Order also anticipates completion of a number of these steps on specified timelines extending into the incoming Trump administration.Cybersecurity in Software Acquisition

The Order identifies several areas of focus in cybersecurity guidance and contemplates incorporating them into the federal government's procurement processes. These steps include the following:

- The Office of Management and Budget ("OMB"), in consultation with CISA and NIST, must recommend language for government contracts requiring providers to give machine-reasonable attestations of secure software development, offer high-level artifacts to validate those attestations and include a list of each provider's Federal Civilian Executive Branch ("FCEB") agency software customers.[7]

- CISA is to evaluate machine-readable secure software attestations and artifacts and to develop a process for responding to incomplete or insufficient validations. The Order contemplates that attestations that fail validation will be reported to the Attorney General for action as appropriate.[8]

- NIST is to establish a consortium with industry at the National Cybersecurity Center of Excellence and develop guidance to "demonstrate[] the implementation of secure software development, security, and operations practices" based on the NIST Secure Software Development Framework ("SSDF"). The Order also establishes a process for NIST to provide updated "guidance on how to securely and reliably deploy patches and updates."[9]

- OMB is to work with NIST and other agencies to implement NIST's guidance on cybersecurity supply chain risk management practices, and to address the "integration of cybersecurity into the acquisition lifecycle."[10]

---

4 Paul, Weiss Client Alert: *Deputy Attorney General Announces Creation of Disruptive Technology Strike Force* (Mar. 3, 2023), available here.

5 The White House, *White House Launches "U.S. Cyber Trust Mark", Providing American Consumers an Easy Label to See If Connected Devices Are Cybersecure* (Jan. 7, 2025), available here.

6 Sam Sabin, *Biden to Sign Executive Order on AI and Software Security*, Axios (Jan. 16, 2025), available here.

7 Order at § 2(b)(i), (ii).

8 *Id.* at § 2(b)(iii), (v), (vi).

9 *Id.* at § 2(c).

10 *Id.* at § 2(d).

2. Improving the Cybersecurity of Federal Systems

The Order also prioritizes strengthening a number of cybersecurity practices to "improve visibility of security threats across networks and strengthen cloud security" and "maintain the ability to rapidly and effectively identify threats across the Federal enterprise,"[11] including the following measures:

- FCEB agencies are required to begin using commercial phishing-resistant authentication standards.[12]
- CISA is directed to develop the technical capability to gain timely access to required data from FCEB agency endpoint detection and response ("EDR") solutions and from FCEB agency security operation centers for threat detection and response.[13] The Order contemplates a multistage process in which CISA first develops a concept of operations and technical controls, and then FCEB agencies enroll endpoints using those controls.[14]
- The Director of the Federal Risk and Authorization Management Program ("FedRAMP") must incentivize or require cloud service providers in the FedRAMP Marketplace to produce baseline specifications and recommendations for agency configuration of cloud-based systems.[15]
- Agencies must take steps to "continually verify" that federal space systems have the "requisite cybersecurity capabilities," including through updates to cybersecurity requirements in contracts.[16]
- NIST must issue guidance identifying minimum cybersecurity practices, to be incorporated into the Federal Acquisition Regulation ("FAR").[17]
- The Order suggests future preparation of a proposed National Security Memorandum addressing cybersecurity.[18]

3. Securing Federal Communications

The Order sets forth detailed requirements for FCEB agencies to implement increased authentication and encryption for communications. For example, the Order provides that:

- The National Cyber Director must recommend contract language to the Federal Acquisition Regulatory Council ("FAR Council") that would require agencies' contracted Internet service providers to adopt and deploy certain Internet routing security technologies.[19]

11 *Id.* at § 3(a), (c).

12 *Id.* at § 3(b).

13 *Id.* at § 3(c)(i).

14 *Id.* at § 3(c)(ii)-(vi).

15 *Id.* at § 3(d).

16 *Id.* at § 3(e).

17 *Id.* at § 7(b), (c).

18 *Id.* at § 8(b).

19 *Id.* at § 4(b)(iii).

- NIST must publish updated guidance on Border Gateway Protocol ("BGP") security methods for federal government networks and service providers, as well as other emerging technologies for Internet routing security.[20]

- Each FCEB agency must take steps to support encrypted Domain Name System ("DNS") traffic and encrypted and authenticated transport for connections between email clients and servers, and OMB must establish requirements to expand the use of transport-layer encryption between email servers.[21] OMB similarly must take steps to enable transport layer encryption by default for voice, video and instant-messaging services. The Order also indicates that, where practical and consistent with recordkeeping obligations, these communications should be end-to-end encrypted.[22]

- Agencies are instructed to take additional steps to prepare for post-quantum cryptography – i.e., cryptographic systems that are secure against quantum computers – into product solicitations, and to protect and monitor access to cryptographic keys.[23]

4. Cybercrime

The Order also offers solutions to combat cybercrime and fraud, specifically in the realms of digital identity verification and so-called "malicious cyber-enabled activities."

- *Digital Identify Verification.* The Order announces that it is the "policy of the executive branch to strongly encourage the use of digital identity documents to access public benefits programs that require identity verification."[24] It thus directs agencies to consider accepting digital identity documents and validation services for public benefits programs. The Order also directs development of a mechanism for notifying recipients of public benefits when their identity information is used to request a payment from a public benefits program so as to avoid potentially fraudulent transactions.[25]

- *Malicious Cyber-Enabled Activities.* The Order amends Executive Order 13694 (covering blocking the property of persons engaging in "significant malicious cyber-enabled activities") to expand the types of cyber-related activities that will trigger sanctions and/or the blocking of transactions. For example, the Order expands the reach of E.O. 13694 to cover persons who engage in a ransomware attack against the United States or a United States person, ally or partner, or citizen or resident of an ally, or who attempt "to gain unauthorized access to a computer or network of computers" so as to threaten the national security, foreign policy, or economic health of the United States. The Order also expands the application of E.O. 13694 to leaders, officials, senior executive officers, or directors of blocked entities.[26]

5. Artificial Intelligence

The Executive Order contains directives for the Departments of Energy, Defense, and Homeland Security related to the development and use of AI. For instance, the Order mandates that:

---

20 *Id.* at § 4(b)(iv).

21 *Id.* at § 4(c), (d).

22 *Id.* at § 4(e).

23 *Id.* at § 4(f), (g).

24 *Id.* at § 5(a).

25 *Id.* at § 5(a)-(c).

26 *Id.* at § 9 (adding, *inter alia*, § 1(a)(ii)(F), (iii)(B) and (iii)(F)).

- The Energy Department, in coordination with the Defense Advanced Research Projects Agency, is to launch a pilot program on the use of AI for cyber defense of critical infrastructure in the energy sector.[27]

- The Department of Defense must establish a "program to use advanced AI models for cyber defense,"[28] and several agencies must prioritize funding for the development of datasets for cyber defense research and AI cyber research generally.[29]

- The Departments of Defense and Homeland Security, and the Director of National Intelligence, must "incorporate management of AI software vulnerabilities and compromises" into existing vulnerability management processes.[30]

Conclusion

The Order caps efforts by the Biden administration to strengthen the federal government's cybersecurity defenses and encourage the private sector to adopt protections through public-private partnerships, guidance documents, and contracts. While the prospect of a change in administration calls into question the future of some of the Order's specific provisions – and the timelines on which they are expected to occur – the effort to raise the bar on cybersecurity across federal agencies, and to increase the government's tools to respond to nation-state cyber-threats, is consistent with longer-term, bipartisan trends.

In particular, the Order's efforts to leverage federal procurement processes to enhance cybersecurity indicate that going forward, agencies will expect private sector partners to continue improving cybersecurity measures. As Deputy National Security Advisor Neuberger noted in announcing the Order, the federal government spends approximately $102 billion per year on IT contracts; the White House can accordingly use this purchasing power to seek to drive change.[31] Organizations that provide technology, communications, or Internet-connected services to federal agencies should continue to monitor changes in cybersecurity requirements.

* * *

27 *Id.* at § 6(a).

28 *Id.* at § 6(b).

29 *Id.* at § 6(c), (d).

30 *Id.* at § 6(e).

31 *See* James Rundle, *Biden Issues 11th-Hour Cyber Executive Order*, THE WALL STREET JOURNAL (Jan. 16, 2025), available here.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

L. Rush Atkinson
+1-202-223-7473
ratkinson@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Katherine B. Forrest
+1-212-373-3195
kforrest@paulweiss.com

Anna R. Gressel
+1-212-373-3388
agressel@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Associates Matthew J. Disler, Rachel Gallagher, Corey Goldstein, Thomas E. Nielsen and Emma White contributed to this Client Alert.