Data Privacy and Cybersecurity

Biden Administration Expands Cybersecurity Requirements for Government Contractors that Are Likely to Have a Broad Impact on the Private Sector

By: David Bitkower, David B. Robbins, Shoba Pillay, Aaron R. Cooper, and Tali R. Leinwand

An Executive Order released by the Biden administration last month (the Cybersecurity EO) seeks to bolster the federal government's cybersecurity defenses and resilience by imposing a variety of requirements on federal agencies and government contractors that are likely to have spillover effects in the private sector.[1] While many federal agencies and contractors already abide by existing agency-specific cybersecurity measures, the Cybersecurity EO establishes additional criteria to ensure that all information systems used or operated by federal agencies "meet or exceed" the cybersecurity requirements set forth in the Cybersecurity EO.[2] In particular, the Cybersecurity EO will directly affect companies that provide information technology (IT) and operational technology (OT) services, cloud computing software, and other technology to the federal government. In turn, the private sector, even when not servicing the federal government, is expected to see a renewed emphasis on security requirements and assessment standards.

President Biden signed the highly anticipated Cybersecurity EO just a few months after the discovery of major cybersecurity incidents that targeted the United States, including Solar Winds (the reported Russian cyber espionage operation that affected nine federal agencies and about 100 American companies), a reported Chinese cyber hacking campaign that compromised tens of thousands of small and midsize firms that used Exchange email servers, and, most recently, the largest known cyberattack on the US energy sector, which led to the shutdown of the Colonial Pipeline.[3] Referencing these events, the Cybersecurity EO and corresponding White House fact sheet (1) make clear that the directives are aimed at improving the government's "insufficient cybersecurity defenses," (2) cast remediation of these incidents as a "top priority and essential to national and economic security," and (3) order several dozen actions be taken beginning as soon as this summer.[4]

We highlight here the key initiatives and imminent deadlines that the EO sets out:

- ***Remove barriers to threat information-sharing between the government and private sector.*** [5] Contractual barriers that prevent IT and OT service providers from sharing threat information will be removed, and such providers will be required to share certain breach information with the government.[6] This structure is intended to facilitate a more robust information-sharing regime. Traditionally, only defense contractors have been subject to federal requirements regarding breach reporting,[7] and while the Federal Acquisition Regulation (FAR) imposes basic safeguarding requirements, it stops short of requiring breach notification.[8] The Cybersecurity EO now extends the reporting requirement to all providers of IT and OT services to the federal government. Contractors will also be required to collect and share information related to cyber threats, incidents, and risks with the Cybersecurity and Information Security Agency (CISA), the Federal Bureau of Investigation, and other agencies.[9] While changes to government contracts will take time to implement, deadlines have been imposed on federal agencies to hasten these initiatives, beginning as soon as this month:
    - June 2021: The Secretary of Homeland Security, in consultation with other agency heads,

is directed to recommend to the FAR Council the nature and type of information pertaining to cyber incidents that require reporting.[10]

- July 2021: The Director of the Office of Management and Budget (OMB), in consultation with other agency heads, is directed to review and recommend updates to contractual requirements and language for IT and OT service providers to report cyber incidents.[11]

- September 2021: The Secretary of Homeland Security and the Director of OMB are directed to take "appropriate steps" to ensure service providers are sharing data with certain agencies.[12] This requirement is broad; it implicates information that "*may* be necessary for the Federal government to respond to cyber threats, incidents, and risks," and that information must be shared "to the greatest extent possible."[13] It remains to be seen whether these open-ended directives are ultimately cabined by their implementing regulations.

- ***Modernize and implement stronger cybersecurity standards in federal government.***[14] Over the next several months, the government must develop "security best practices," such as the use of zero-trust architecture, cloud service solutions, and multi-factor authentication and encryption.[15] The government must also modernize the FedRAMP program—the federal government's main security authorization program for cloud security—to include training for agencies and improved communication with cloud service providers.[16]

- ***Improve software supply chain security.***[17] Over the next year, the Department of Commerce's National Institute of Standards and Technology (NIST) is directed to develop guidance to "enhance[e] software supply chain security criteria," with an emphasis on "critical software," that will include standards, procedures, or criteria regarding data encryption, multi-factor authentication, and other measures.[18] Eventually, and critically, only software that abides by these new rules will be eligible for federal procurement; non-compliant software will be removed from federal contracts and purchase agreements, and legacy software will need to be redesigned as necessary to comply with these new requirements.[19] Further, the Secretary of Commerce, acting through the Director of NIST, is also directed to develop criteria for product labels to explain for consumers the cybersecurity capacities of commercial (including Internet-of-Things) devices and software, including the "levels of testing and assessment" that a product may have undergone.[20] From the perspective of companies concerned about potential Federal Trade Commission enforcement, the labelling regime will be especially important to bear in mind so as to ensure that device or software development processes meet or exceed the stated criteria, and accurately reflect existing practice.

- ***Establish a cyber safety review board.***[21] An incident review board will convene when there are "significant" cybersecurity incidents.[22] The board reflects a public-private partnership centered on digital defense and identifying lessons learned. It will be co-led by the Secretary of Homeland Security and others, including representatives from private sector entities, who will be selected based on the particular incident being investigated.[23]

- ***Create a standard playbook for responding to cyber incidents.***[24] By September 2021, the Department of Homeland Security (DHS), OMB, and other federal agencies will be required to develop a "playbook"—*i.e.*, a standard set of operating procedures—to be used in planning and conducting cybersecurity vulnerability and incident response activity with respect to Federal Civilian Executive Branch (FCEB) Information Systems.[25] The playbook must (1) incorporate all appropriate NIST standards, (2) be used by FCEB agencies, and (3) articulate progress and completion through all phases of incident response.[26]

- ***Improve detection of cybersecurity incidents on federal government networks.***[27] In order to detect incidents early, agencies must deploy Endpoint Detection and Response initiatives to support proactive detection of cybersecurity incidents within federal government infrastructure, active cyber hunting, containment and remediation, and incident response.[28] These requirements will be based on requirements issued by OMB in consultation with DHS.[29]

- ***Improve investigative and remediation capabilities.***[30] Over the next three months, the Secretary of Homeland Security, in consultation with other federal agencies, is directed to develop standardized requirements for maintaining information event logs for federal agencies.[31] The requirements will include the types of logs to be maintained, the time periods to retain the logs, and guidance for protecting those logs.[32]

As written, the Cybersecurity EO is designed to have a meaningful impact not only on the federal government but also on its contractors and, ultimately, the private sector. Yet for all of the Cybersecurity EO's ambitious directives and timelines, execution of these directives will take time, and the Cybersecurity EO's ultimate effect will be heavily informed by implementing regulations that have not yet been announced. It remains to be seen how soon the new initiatives envisioned by the Cybersecurity EO will actually take effect, but IT and OT providers most likely to be directly impacted are on notice that change is on the horizon, and that the security community as a whole is contemplating new benchmarks for what cybersecurity looks like.

Of course, the Cybersecurity EO only offers one vector of the federal government's cybersecurity response, and therefore is equally notable for what it does not, and cannot, address. For example, in the wake of the hack of Solar Winds and the ransomware attack on Colonial Pipeline, it is natural to ask what the Biden Administration's response will be to continued Russian and Chinese state-sponsored cyber intrusions and, relatedly, foreign safe-harbors provided to criminal groups.[33] The Cybersecurity EO does not say. Separately, will Congress go beyond the Cybersecurity EO to impose broad-sweeping and mandatory breach disclosure requirements, as some have alluded to?[34] From that perspective, the Cybersecurity EO may signal just the beginning of a broader effort within the federal government that is likely to continue in the coming months.

Contact Us

David Bitkower

dbitkower@jenner.com | Download V-Card

David B. Robbins

drobbins@jenner.com | Download V-Card

Shoba Pillay
spillay@jenner.com | Download V-Card

Aaron R. Cooper
acooper@jenner.com | Download V-Card

Tali R. Leinwand
tleinwand@jenner.com | Download V-Card

Meet Our Team

Practice Leader

David Bitkower
Chair
dbitkower@jenner.com
Download V-Card

---

[1] White House, *Executive Order on Improving the Nation's Cybersecurity* (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[2] Cybersecurity EO § 1.

[3] Ellen Nakashima, *Biden Signs Executive Order Designed to Strengthen Federal Digital Defenses*, Washington Post (May 12, 2021), https://www.washingtonpost.com/national-security/biden-executive-order-cybersecurity/2021/05/12/9269e932-acd5-11eb-acd3-24b44a57093a_story.html.

[4] Cybersecurity EO § 1; White House, *Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks* (May 12, 2021), 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/

[5] Cybersecurity EO § 2.

[6] Cybersecurity EO § 2.

[7] DFARS 252.204.7012.

[8] FAR 52.204-21.

[9] Cybersecurity EO §§ 2(a), 2(e).

[10] Cybersecurity EO § 2(g)(i).

[11] Cybersecurity EO § 2(b).

[12] Cybersecurity EO § 2(e).

[13] Cybersecurity EO § 2(e) (emphasis added).

[14] Cybersecurity EO § 3.

[15] Cybersecurity EO § 3(d).

[16] Cybersecurity EO § 3(f).

[17] Cybersecurity EO § 4.

[18] Cybersecurity EO §§ 4(c)-(e). Under the EO, "critical software" is "software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources)," and which will be subject to additional security guidance. *Id.* §§ 4(a), (g)-(j).

[19] Cybersecurity EO §§ 4(p)-(q).

[20] Cybersecurity EO §§ 4(s)-(t).

[21] Cybersecurity EO § 5.

[22] Cybersecurity EO § 5(c).

[23] Cybersecurity EO § 5(e).

[24] Cybersecurity EO § 6.

[25] Cybersecurity EO § 6(b).

[26] Cybersecurity EO § 6(b).

[27] Cybersecurity EO § 7.

[28] Cybersecurity EO § 7(b).

[29] Cybersecurity EO §§ 7(c)-(d).

[30] Cybersecurity EO § 8.

[31] Cybersecurity EO §§ 8(b)-(c).

[32] Cybersecurity EO § 8(b).

[33] *See* Mae Anderson & Frank Bajak, *Cyberattack on U.S. Pipeline is Linked to Criminal Gang*, Associated Press (May 9, 2021), https://apnews.com/article/europe-hacking-government-and-politics-technology-business-333e47df702f755f8922274389b7e920.

[34] *See* Eric Geller & Martin Matishak, *A Federal Government Left 'Completely Blind' on Cyberattacks Looks to Force Reporting*, Politico (May 15, 2021), https://www.politico.com/news/2021/05/15/congress-

colonial-pipeline-disclosure-488406.