Articles + Publications | June 11, 2021

Biden Signs Executive Order Intended to Improve the Federal Government's Cybersecurity

WRITTEN BY

Hilary S. Cairnie | Timothy A. Butler | Chelsea Lamb | Travis S. Andrews

On May 12, President Biden signed an executive order intended to improve the federal government's cybersecurity. This comes in the wake of sweeping cyber incidents, such as the SolarWinds incident that affected both public and private sector entities last year. The executive order calls on both the federal government and the private sector to work collaboratively to identify, deter, detect, and respond to cyber incidents, stating that "bold changes and significant investments" are needed to defend the nation's computer systems from attack.

The executive order instructs the Office of Management and Budget (OMB) director to review and revise the federal government's contracts with IT and operational technology (OT) providers. Specifically, the executive order requires the OMB to review federal acquisition regulations to enhance contractors' and federal agencies' ability to share information about cyber incidents and threats. Subject to the final language in the regulations, IT and OT contractors may be required to preserve and share data with federal agencies about cyber threats and may be required to work with federal agencies in investigating and in responding to such incidents — actions that go beyond the current cyber requirements embodied in FAR 52.204-21 and DFARS 252.204-7012.

The executive order also requires the federal government to update and modernize its cybersecurity standards. In particular, the executive order instructs federal agencies to adopt security best practices, including "zero trust architecture" and secure cloud services. The executive order also requires agencies to streamline and centralize access to cybersecurity data and invest in technology and equipment to achieve these modernization goals. Agency heads have 60 days to report on their progress, and they must adopt multifactor authentication and data encryption within 180 days of the executive order.

In addition, the executive order provides a baseline security standard for the federal government's software supply chain security. As the executive order acknowledges, much of the software used by the federal government comes from third parties or other vendors with little or no visibility into the cybersecurity protections that are coded into the software. Software developers (be they prime contractors, subcontractors, or supply chain vendors) now must provide greater transparency into their products, including a requirement to provide federal agencies with a "software bill of materials" for each software product.

The executive order establishes a cybersecurity safety review board, which will be under the purview of the secretary of homeland security. This board will be tasked with reviewing and assessing cyber incidents that affect the federal civilian executive branch information systems or nonfederal systems. The executive order outlines that the cybersecurity safety review board will be comprised of government and private sector members in a similar fashion to the National Transportation Safety Board.

Additionally, the executive order instructs the Department of Homeland Security, OMB, DOD, NSA, and other federal agencies to develop a playbook to respond to cybersecurity vulnerabilities and incidents, while further contemplating that the playbook should outline the agencies' plan to incorporate all appropriate NIST standards and to respond to incidents.

The executive order instructs federal agencies to improve detection of cybersecurity vulnerabilities and incidents on the federal government's networks to maximize the early detection of vulnerabilities and incidents on its networks. In particular, the executive order mandates that agencies will use endpoint detection and response initiatives to support proactive detection of cybersecurity incidents.

Lastly, the executive order intends to strengthen the federal government's investigative and remediation capabilities by developing requirements for logging events and by retaining other relevant data within federal agencies' systems and networks.

RELATED INDUSTRIES + PRACTICES

- Consumer Financial Services
- Government Contracts
- Privacy + Cyber