Bloomberg Law

Privacy & Data Security Law

Biden's Cyber Executive Order: How It Could Impact Your Business

Bloomberg Law

By Jennifer C. Archie, Serrin Turner, and Alexander L. Stout

June 8, 2021

President Biden's executive order requiring the networks of federal departments and agencies to have strengthened safeguards against cyberattacks will impact federal government contractors directly and are likely to have an indirect effect on private businesses as well, say Latham & Watkins cybersecurity and data privacy attorneys.

President Biden signed an executive order to bolster the federal government's cybersecurity posture on May 12. The order focuses on implementing vital improvements to networks of federal departments and agencies, many of which still lack basic safeguards despite past presidential and congressional actions.

Several upcoming changes will affect businesses that rely on the government as a customer, but a White House memorandum urges all businesses to implement the best practices from the executive order.

As Biden noted in a May 13 press briefing, the executive branch lacks authority to "dictate" that private companies "do certain things relative to cybersecurity." While its legal reach is therefore limited, the order may foreshadow how standards of care will be applied in other contexts where private companies are subject to cybersecurity regulatory requirements or scrutiny.

In particular, the government's new standards for incident response and secure software development—along with mandates that departments and agencies use two-factor authentication, encryption, and secure cloud services—may gain traction beyond the federal government and its contractors.

More broadly, the order will likely continue shifting regulatory and public expectations in favor of more transparency. Federal technology contractors will be required to cooperate before, during, and after a cyberattack, and all companies will be encouraged to develop secure software and display labels affirming that their products have satisfied to-be-developed security standards.

Failure to Disclose Is Not an Option

The order directs policy changes that will require information technology (IT) and operational technology (OT) providers that service federal departments and agencies, including cloud providers, to collect and preserve cybersecurity information related to all information systems.

They also must provide the government information about cyber incidents or potential incidents that could impact government networks, and collaborate with government cybersecurity agencies to detect and remediate cyber incidents. The Office of Management and Budget will review the Federal Acquisition Regulation (FAR) to update contract requirements.

Similarly, the order sets out explicit notification and information-sharing requirements for information and communications technology (ICT) service providers which, although undefined here, generally include providers that fulfill or enable information or data processing, storage, retrieval, or communication.

All ICT providers serving federal departments and agencies will be required to "promptly" report to their agency customer and the Cybersecurity and Infrastructure Security Agency (CISA) regarding any cyber incident involving a software product or service provided to the government.

Established in 2018, CISA is responsible for protecting federal networks and collaborating with the private sector to secure critical infrastructure. The Department of Homeland Security will recommend changes to the FAR to update contract requirements.

Standardizing Incident Detection and Response

The order requires CISA to create a standardized playbook and set of definitions for cyber incident response for use by federal departments and agencies. The playbook, to be updated at least annually, will replace existing agency practices.

The playbook is also intended to provide the private sector with a template for cyber response, so it will likely inform regulatory or other legal expectations for incident response preparedness.

The order directs agencies to create cybersecurity event logs to improve detection of intrusions, mitigate those in progress, and determine the extent of prior incidents—a practice already mandated for some private sector entities under HIPAA and other sector-specific laws with defined security rules. CISA's requirements may likewise affect expectations for event logging and after-action steps beyond the parties covered directly by the order.

It also establishes a Cybersecurity Safety Review Board, co-chaired by government and private sector leads. Modeled on the National Transportation Safety Board, the new group will convene following a significant cyber incident to analyze what happened, make concrete recommendations for improvement, and advise the president accordingly.

While the order requires the board to protect confidential information that it obtains—including business information—future large-scale cybersecurity incidents will likely be followed by similarly large-scale government investigations.

Secure Development Standards

The order requires the National Institute of Standards and Technology (NIST) to work with government, the private sector, and academia to develop and publish within 180 days mandatory standards for securely developing software and evaluating software security, applicable to all federal civilian software procurements.

Developers will be required to monitor and resolve software vulnerabilities and to make security data available publicly. The government's buying power, which encompasses many or even most commercially available software products, will likely make the new NIST standards the default framework for assessing whether software has been developed with the requisite security focus.

The order also directs NIST to pilot a program educating consumers on the security capabilities of Internet-of-Things devices and software. The program—based on the popular "Energy Star" appliance labels—would allow companies that submit to comprehensive testing and evaluation to label their products and services as having been developed securely.

Such policy initiatives articulated in the order should be understood as aligning the U.S. globally and competitively. European cyber authorities (ENISA) have been working for several years on standardizations and certifications for key infrastructure such as 5G networks and consumer IoT.

Accelerated Cloud Migration

The order embraces and advances a longstanding recommendation and intention for federal departments and agencies to "accelerate movement to secure cloud services."

Federal departments and agencies have 60 days to update plans to prioritize resources for cloud migration, as well as to develop plans to implement a zero-trust architecture , which is a security model that "eliminates implicit trust" in the network and requires continuous verification of data access rights.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

Jennifer C. Archie is a partner at Latham & Watkins in Washington, D.C. She is a cybersecurity and data privacy lawyer who advises clients ranging from emerging companies to Fortune 50 global enterprises in litigation, investigations, compliance, and the protection of trade secrets and confidential information.

Serrin Turner is a partner at Latham & Watkins in New York. He is a former federal cybercrime prosecutor with experience handling every aspect of cybersecurity incident response—including internal investigations, crisis management, regulatory inquiries, business-to-business disputes, and class action litigation.

Alexander L. Stout is an associate at Latham & Watkins in Washington, D.C. He represents communications and information technology companies in transactional and regulatory matters, as well as data privacy and cybersecurity.