Legal Update Article

Biden Administration Issues Cybersecurity Executive Order

By Joseph J. Lazzarotti & Laura A. Mitchell

May 18, 2021

Meet the Authors

Joseph J. Lazzarotti

Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Laura A. Mitchell

(She/Her)
Principal
303-225-2382
Laura.Mitchell@jacksonlewis.com

Related Services

Affirmative Action, OFCCP and Government Contract Compliance
Government Contractors
Privacy, Data and Cybersecurity

The Biden Administration has issued the much-anticipated "Improving the Nation's Cybersecurity" Executive Order (EO), setting certain standards and requirements to prevent cyberattacks for government agencies, federal contractors, and others.

Recent Attacks

The EO was in the works prior to a cyberattack on the Colonial Pipeline at the beginning of May that slowed and snarled the flow of gas on the East Coast for days. Reportedly, it was a ransomware incident. Ransomware attacks are not new, but they are becoming more severe. Most do not see the large sums paid to hackers by victim organizations needing access to their encrypted data or wanting to stop a disclosure of sensitive information if they can. But most do see the crippling of vital infrastructure caused by compromised computer systems without which basic services cease to flow.

Some attacks that have affected entities considered to be critical infrastructure have been well-publicized. In February 2021, ABC News reported that weak cybersecurity controls "allowed hackers to access a Florida wastewater treatment plant's computer system and momentarily tamper with the water supply," based on a memo by federal investigators it obtained. A month later, sensitive data held by New England's largest energy provider were exposed for some time in cloud storage, according to reports. The SolarWinds breach in 2020, named Sunburst, was a massive compromise of government agencies, including the Department of Energy.

Key Provisions

The EO clearly states the policy:

> It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.

Generally, the EO will affect the federal government and its agencies. However, some requirements will reach certain federal contractors and influence entities in the private sector.

Among other requirements, the EO directs the following:

- *Remove contractual barriers in contracts between the federal government and its information technology (IT) and operational technology service providers.* The goal is to increase information sharing about threats, incidents, and risks to accelerate incident deterrence, prevention, and response efforts and to enable more effective defense of government systems and information. As part of this effort, the EO requires a review of the Federal Acquisition Regulation (FAR) concerning contracts

with such providers and recommendations for language designed to achieve these goals. Recommendations will include, for example, time periods contractors must report cyber incidents based on severity, with reporting on the most severe cyber incidents not to exceed three days after initial detection. The changes also will seek to standardize common cybersecurity contractual requirements across agencies.

- *Modernize the approach to cybersecurity.* Steps called for in the EO include adopting security best practices, advancing to Zero Trust Architecture, moving to secure cloud services, including Software as a Service (SaaS), and centralizing and streamlining access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks. The EO requires that, by November 8, 2021 (within 180 days of the date of the EO), agencies must adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with federal records laws and other applicable laws.
- *Improve software supply chain security.* Driven by the effect of the SolarWinds incident (hackers used a routine software update to slip in malicious code that allowed the cyberattack), the EO points to the lack of transparency in software development and asks whether adequate controls exist to prevent tampering by malicious actors, among other things. The EO calls for guidance to be developed that will strengthen this supply chain. This will include potential new standards, procedures, and criteria, such as securing development environments and attesting to conformity with secure software development practices. The EO also requires recommendations for contract language that would require suppliers of software available for purchase by agencies to comply with, and attest to, complying with the guidance developed. Efforts also will be made to reach the private sector. For instance, pilot programs will be initiated by the Secretary of Commerce acting through the Director of National Institute of Standards and Technology to educate the public on the security capabilities of internet-of-things (IoT) devices and software development practices and consider ways to encourage manufacturers and developers to participate in these programs.
- *Establish a Cyber Safety Review Board.* Among the new Board's duties are reviewing and assessing certain significant cyber incidents affecting Federal Civilian Executive Branch Information Systems or non-federal systems, threat activity, vulnerabilities, mitigation activities, and agency responses.
- *Standardize incident response.* Standardize the federal government's response to cybersecurity vulnerabilities and incidents to ensure a more coordinated and centralized cataloging of incidents and tracking of agencies' progress toward successful responses.
- *Improve detection.* The EO seeks to improve detection of cybersecurity vulnerabilities and incidents on federal government networks.
- *Improve investigative and remediation capabilities.* Recognizing it is essential that agencies and their IT service providers collect and maintain network and system logs on federal information systems in order to address a cyber incident, the EO seeks recommendations on the types of logs to be maintained, the time periods to retain the logs and other relevant data, the time periods for agencies to enable recommended logging and security requirements, and how to protect logs. These recommendations also will be considered by the FAR Council when promulgating rules for removing barriers to sharing threat information.

***

The U.S. government is expected to ramp up efforts to strengthen its cybersecurity, and states likely will continue to legislate and regulate in this area. All businesses, including federal contractors, can expect pressure to evaluate their data privacy and security threats and vulnerabilities and adopt measures to address their risk and improve compliance.

Please contact a Jackson Lewis attorney with any questions about the EO. For timely insights and analysis on privacy and data security, subscribe to our blog, Workplace Privacy, Data Management & Security Report.