BARNES & THORNBURG LLP

ALERTS

Biden Executive Order Aims To Fight Off Government, Private Sector Cybersecurity Threats

July 16, 2021

Highlights

President Biden's executive order on cybersecurity may result in swift changes and significant investments in cybersecurity at the federal level

Dramatic reforms to federal contracting terms expected as new agency guidelines due in September

Consider assessing and making necessary updates to networks now to remain in compliance with standardized procedures across all federal civilian executive branch agencies

In May, President Biden issued an executive order establishing new guidelines for the United States to "identify, deter, protect against, detect, and respond to" cybersecurity threats. The order lays out eight directives for strengthening the nation's response to cyber threats, mostly focused on preventive and planning measures but including responsive measures as well.

The president seeks to "lead by example" by guiding the private sector on how to best "adapt to the continuously changing threat environment" and ensure the products they develop are "built and operate securely." The

RELATED PEOPLE

Brian J. McGinnis
Partner
Indianapolis

P 317-231-6437
F 317-231-7433
brian.mcginnis@btlaw.com

RELATED PRACTICE AREAS

Data Security and Privacy
Internet and Technology

order calls for “bold changes and significant investments,” and invites the private sector to “partner with the Federal Government to foster a more secure cyberspace.”

Impact on Businesses

The order outlines directives for various federal agencies designed to improve security. These directives immediately flow down to government contractors through request for proposal (RFP) guidelines and contract provisions. Under the order, government contractors will need to make a renewed showing that they are taking cybersecurity seriously and have taken identifiable steps to secure government data.

Agencies and contractors should expect to see swift changes and significant investments in cybersecurity at the federal government level. Agencies have been tasked to develop guidelines by Sept. 9, 2021, and businesses should be prepared for dramatic changes to federal contracting terms. They should also assess and make necessary updates to their networks to comply with standardized procedures and sharing across all federal agencies. It is foreseeable that these changes could provide more opportunities for private sector and federal government partnerships.

To address these changes and capitalize on new opportunities, government contractors should consider developing and implementing an information security program (ISP) and then utilize that ISP as part of a comprehensive qualifications and marketing platform for their business.

The Eight Provisions

The order identifies eight directives, which are intended to address a hindrance to or provide a means for improved cybersecurity. Specific steps are identified that should be taken, and by which federal agency, for each provision. Deadlines for meaningful action to implement the directives range from 14 to 270 days (to February 2022). Standardized procedures and data sharing across federal agencies are themes across the various provisions. Additionally, several provisions directly impact federal government contracting.

1. Removing Barriers to Sharing Threat Information

The theme running throughout the order and all its provisions is greater sharing of data related to cybersecurity threats. The White House is instituting, to the extent it can, and advocating beyond its authority for, standardized procedures that allow sharing of cyber threat vulnerabilities, incidents, and responses across all federal civilian branch FCEBagencies. Because our system of government relies on contractors, the call for sharing is extended to private-sector companies contracting with the government.

In this provision, Biden seeks to change the contract terms of government services providers, in particular informational and operational technology service providers, to allow these vendors to share cyber threat and incident information with the FCEB agencies to which they are contracted. The order goes further by stating that the White House’s intent is to require service providers to collect and preserve data related to cybersecurity event prevention, detection, response, and investigation.

The order anticipates new contract changes to be implemented by Sept.

9, 2021.

Coming into compliance with new contract terms that as of yet have not been implemented could prove challenging for many vendors. Sharing data can have other implications within an organization and can affect client trust. Staying abreast of the changes that come out of this order are critical to being able to respond.

2. Modernizing Federal Government Cybersecurity

The order urges a move toward zero trust architecture (ZTA), acceleration of the use of secure cloud services, and more focus on data analytics in addressing cyber threats. ZTA, as the name suggests, assumes none of the parameters involved in network transmission can be trusted, i.e., the network, the users, or the resources. In traditional network security paradigms, the security is focused on the network itself. Under the ZTA scheme, the security focus shifts to the users and the resources, e.g., the accounts and services. Other cybersecurity standards are elevated under this provision of the order, including multi-factor authentication and encryption of data in transit as well as at rest.

The White House acknowledges that investments in technology and personnel are needed to meet these goals, but calls for FCEB agencies to prioritize resources for the implementation of cloud technology and draft a plan to implement ZTA by July 12, 2021.

The order anticipates using the existing Federal Risk and Authorization Management Program (FedRAMP) to implement this plan. FedRAMP standardizes authorization of cloud products and services across FCEB agencies and acts as a certification program to which vendors must comply prior to managing or storing federal data in the cloud.

3. Enhancing Software Supply Chain Security

The order criticizes current commercial cybersecurity software and calls for government, private-sector, and academic input to identify and develop new best practices. It further indicates a desire by the White House to establish criteria for evaluating software and routine updating of any standards that are set. Ten criteria are identified for evaluating and improving what is termed the software supply chain, such as employing automated tools to check vulnerabilities or to maintain trusted source codes. As is customary in development best practices, the National Institute of Standards and Technology (NIST) is tasked with leading this effort.

As part of the effort to enhance the software supply chain, the order suggests that consumer product labeling programs be established as pilot programs in order to educate the public on cybersecurity measures integrated in the devices and software they purchase. Essentially, the program would operate as a certification of sort to show the level of testing and assessment that he product may have undergone.

Clearly, this provision has a huge impact on the software and cybersecurity industries. Other private-sector companies and government contractors should stay abreast of the changing best practices in cybersecurity software and utilize any certification or consumer labeling programs to garner trust with their customers.

4. Standardizing the Federal Government's Playbook for Responding to

Cybersecurity Vulnerabilities and Incidents

Cybersecurity protocols for identifying and responding to cyber threats vary widely across agencies. These differences frustrate efforts to synthesize threats and manage the response across agencies. This provision of the order mandates a single set of operational procedures, consistent with NIST best practices y, to be used by FCEB agencies in addressing cyber vulnerabilities. When prior cybersecurity related directives, such as the Federal Information Security Modernization Act of 2002, as amended in 2014, and FedRAMP, were mandated FCEB agencies, private-sector contractors doing business with covered federal agencies were also swept up in the new requirements. It is likely we will see many of the standards implemented under this order filtering down to government contractors.

5. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks

Early detection of cybersecurity vulnerabilities is key to Biden's plan to improve the nation's response to cyber incidents. This provision institutes proactive detection of cyber incidents by implementing endpoint detection and response (EDR) measures. EDR is a cybersecurity tool that continuously and automatically monitors and collects data at the end or delivery point of a transmission, allowing swift identification and response to cyber threats. Federal agencies are expected to adopt EDR techniques by Aug. 10, 2021. Inclusion of EDR in the order signifies its place as a best practice that the government is likely to expect its contractors to implement in the near future.

6. Improving the Federal Government's Investigative and Remediation Capabilities

This provision focuses on data collection and retention from network and system logs, and requires recommendations be drafted for logging events and retaining other relevant data within a government agency's systems and networks. Upon implementation, expect centralized access to security operations of each agency and consistency of requirements for system logging, log retention, log management, log protection, and log sharing with the federal agencies tasked with various aspects of cybersecurity. It is likely that implementation of this provision will impact the government contractors whether they are IT service providers for the government or providers of other services that handle government data.

7. Establishing a Cyber Safety Review Board

The order calls for the creation of a Cyber Safety Review Board under the Department of Homeland Security that would convene following a "significant cyber incident" and at other times when deemed necessary. Federal officials and private-sector representatives will jointly lead and serve on the board. The details regarding the board's proposed mission, scope and duties is still to be determined. However, the intent is for the review board to advise the Secretary of Homeland Security, and ultimately the president, on how the government should improve its cyber position based on reviews of each cyber incident.

8. National Security Systems

This provision delays applicability of the order to the U.S.'s national security systems to give time to identify "unique mission needs" with

which the directives may interfere. All other national security systems requirements must be updated to exceed the cybersecurity standards laid out in the order by July 12, 2021.

Best Practices:

In the wake of this order, businesses and government contractors should consider developing and implementing an information security program that involves:

- Performing routine assessment of cyber vulnerabilities
- Taking an assessment of risk level based on data value, system criticality, and consequence analysis
- Creating or updating internal policies based on risk and vulnerability assessments (access assessment, employee training, retention planning, cyber insurance strategy)
- Instituting redundancy, whenever possible
- Improving system security to meet best practices (two-factor authentication, endpoint detection and response, NIST)
- Drafting an incident response plan to be prepared in case of a security incident

For more information, please contact the Barnes & Thornburg attorney with whom you work, or Sahara Williams at 317-231-6407 or sahara.williams@btlaw.com, or Brian McGinnis at 317-231-6437 or brian.mcginnis@btlaw.com.