PUBLICATION

Biden Administration Signals Dramatic Shift in Focus to Confront Cyber Concerns In Government Contracting

Authors: Alisa L. Chestler

May 13, 2021

In a paradigm shift for cybersecurity, President Biden signed an ambitious Executive Order (the Order) on May 12 to address the increasingly sophisticated threats by malicious cyber actors to the nation's software supply chains and federal information systems. The Executive Order on Improving the Nation's Cybersecurity seeks to modernize federal government cybersecurity, improve information sharing between federal agencies and the private sector, and enhance the nation's resiliency to cyber-attacks. While the Order primarily focuses on concrete steps the federal government must take to adopt cybersecurity best practices, there are several provisions that will also significantly impact government contractors, subcontractors and other private sector entities. These changes come at a critical time for such organizations, especially those that are diligently working to meet Cybersecurity Maturity Model Certification (CMMC) requirements.

Key Takeaways

Upcoming Changes to the FAR and DFARS

Agencies across the federal government are required to provide recommendations for changes to the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) contract requirements for information communications technology (ICT) service providers. The changes will obligate ICT service providers under contract with the federal government to collect and retain data and information relevant to cybersecurity incidents, to promptly share such data directly with designated federal agencies, and to cooperate with investigations of and responses to incidents on federal information systems.

Modernization of Federal Government Cybersecurity

The federal government will be moving toward zero trust architecture and secure cloud services in compliance with National Institute of Standards and Technology (NIST) standards and guidance. To facilitate this shift to cloud-based infrastructure, the Federal Risk and Authorization Management Program (FedRAMP) will develop and promulgate security principles governing Cloud Service Providers (CSPs). Additionally, all federal agencies are required to adopt multi-factor authentication (MFA) and encryption for data at rest and in transit by November 3, 2021. While this requirement currently is limited to the federal government, the Order is unclear as to whether MFA and encryption will also apply to government data and controlled unclassified information (CUI) resident on defense industrial base (DIB) and other contractor networks.

Software Supply Chain Security

Considering the impact the SolarWinds breach continues to have across multiple sectors, this Order seeks to implement more stringent measures to ensure the proper functioning and reliability of critical software. Over the next 30 days, NIST will engage with representatives from the federal government, the private sector, and academia to develop criteria to evaluate security practices of software developers, after which NIST will publish guidelines to enhance software supply chain security. Among these guidelines will be a requirement for software developers to provide the federal government with a software bill of materials for all critical software. Once NIST publishes its guidelines, federal agencies will have 30 days to comply. Within one year, the

Department of Homeland Security (DHS) will provide recommendations for amendments to the FAR to contractually obligate vendors to comply with the NIST guidelines. All software that does not meet the NIST standard will be removed from federal government contracts and networks. NIST will publish further guidelines articulating minimum standards for developers testing their software source code.

Internet of Things

NIST will develop criteria for a baseline level of secure practices and an associated rating schema for IoT devices which will likely include parallels with Underwriters Laboratories (a third-party certification company).

Cybersecurity Safety Review Board

The Order establishes the Cybersecurity Safety Review Board (CSRB). Similar to the National Transportation and Safety Board (NTSB), the CSRB will be comprised of government officials and industry professionals who are called upon to review and assess significant cyber incidents. The Board's first order of business is to review the SolarWinds breach and to provide DHS with recommendations for improving cybersecurity and incident response.

Network Logs

Over the next two weeks, the government will develop requirements for logging events, retaining relevant data, and encrypting logs for activity on federal information systems – including those hosted and managed by third parties. This requirement will obligate third-party vendors that maintain information systems used by the federal government to collect, retain, and supply network logs to the government.

Summary

This Order represents more than an incremental step in cybersecurity – it is a significant shift towards modernization and increased public-private partnership. It seeks to consolidate nonuniform policies across multiple agencies and to standardize common cybersecurity contractual language to improve compliance for vendors and security for the federal government. For federal contractors and their subcontractors, a keen understanding the requirements of the forthcoming standards will be crucial. Companies must work to consider whether these changes will impact their overall business strategy, responses to RFPs and current plans to comply with the CMMC requirements.

As the guidelines affecting government contractors are announced over the coming months, Baker Donelson stands ready to support you. If you have any questions about this Order or any other aspect of your data protection and security practices, please contact Alisa Chestler or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.