Executive Order on Improving the Nation's Cybersecurity

July 13, 2023

Summary:

The Executive Order on Improving the Nation's Cybersecurity (EO 14028) was released on May 12, 2021. This executive order issued guidance on the National Institute of Standards and Technology (NIST) developing new software supply chain security standards. EO 14028 was created in response to the Solarwinds attack where hackers utilized a backdoor trojan to access Solarwinds' client networks. This attack infected 18,000 customers, which included nine federal agencies. To achieve the goals of this executive order, the government must partner with private industry to adapt, build, and operate in an ever-changing cyber ecosystem.

EO 14028 instructed NIST to publish standards for testing of vendor software source code. NIST and the Federal Trade Commission (FTC) were also instructed to launch a pilot program for security risks related to the Internet of Things (IoT).

Overview

The Executive Order outlines improvements needed within the federal government to ensure proper cybersecurity of essential operations. EO 14028, with an emphasis on supply chain security and zero trust, does the following:

- Requires service providers to share cyber incident and threat information that could impact Government networks
- Establishes baseline security standards for development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available
- Establishes a Cybersecurity Safety Review Board, co-chaired by government and private sector leads, that may convene following a significant cyber incident to analyze what happened and make recommendations for improving cybersecurity
- Creates a standardized playbook and set of definitions for cyber incident response by Federal departments and agencies
- Improves the ability to detect malicious cyber activity on Federal networks by enabling a government-wide endpoint detection and response system and improved information sharing within the Federal government
- Creates cybersecurity event log requirements for Federal departments and agencies

Status

All deadlines within the executive order have passed.

Actions Required

Agencies must:

- Prioritize adoption of cloud technology, develop a plan to implement Zero Trust Architecture, and provide a report to Office of Management and Budget (OMB) with plans detailing cloud and Zero Trust adoption
- Report to the Cybersecurity & Infrastructure Security Agency (CISA) and OMB on types and sensitivity of agency unclassified data
- Report to CISA, OMB, and the Assistant to the President for National Security (APNSA) on progress in adopting multifactor authentication (MFA) and encryption of data at rest and in transit or provide a written rationale as to why they were unable to adopt

OMB must:

- Develop a federal cloud-security strategy and provide guidance to agencies to ensure risks of using cloud-based services are understood and addressed

CISA must:

- Issue a cloud-service governance framework
- Issue cloud-security technical reference architecture
- Establish a framework to collaborate on cybersecurity and incident response activities related to cloud technology
- Take appropriate steps to maximize adoption of MFA and encryption based on reported gaps from agencies

General Services Administration (GSA) must:

- Begin modernizing FedRAMP to train agencies to manage FedRAMP requests, improve communication with cloud service providers (CSPs), incorporate automation, digitize documentation, and map out reciprocal compliance frameworks.

What Contractors Can Expect

EO 14028 will impact federal agencies and those doing business with the federal government. Contactors will see modification of contract language to reflect new guidance from NIST and CISA. If your company cannot accept the modification, you will not be able to sell to the Federal government. Additionally, there will be future updates to the Federal Acquisition Regulation (FAR).