GT GreenbergTraurig

Alert | Government Contracts

May 2021

Executive Order on Improving the Nation's Cybersecurity: An Ambitious and Timely Call for a Broad Range of Cybersecurity Improvements

On May 12, 2021, President Biden issued an executive order entitled *Improving the Nation's Cybersecurity* (EO). The EO was released only days after the cyberattack impacting Colonial Pipeline, and several months following discovery of the penetration of various federal agencies as a result of the Solar Winds cyber breach by Russian hackers in 2019. The 34-page EO calls for broad and ambitious changes intended to improve Federal Information System cybersecurity, and the prevention, detection, assessment, and remediation of cyber incidents that pose a risk to national and economic security. Many of the changes contemplated by the EO could have significant impacts on contractors doing business the with federal government, and greatly increase their reporting responsibilities and cybersecurity obligations. This GT Alert provides an overview of the key policies, goals, and requirements contained in the EO.

Increased Sharing of Threat Information

The EO includes numerous provisions aimed at "removing barriers" to the sharing of threat information by information technology (IT) and operational technology (OT) service providers. Section 2 of the EO calls on executive agencies to review the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) contract requirements and language applicable to federal government contracts with IT and OT service providers, and recommends updates to such requirements

and language to the FAR Council and other appropriate agencies that will be designed to ensure, *inter alia*, that service providers:

1. Collect and Preserve data relevant to cybersecurity event prevention, detection, investigation, and response, on all information systems over which the service provider has control;

2. Share collected data with any agency with which they have contracted, as well as any additional agencies identified by the Office of Management and Budget (OMB); and

3. Collaborate with federal cybersecurity investigations and responses to incidents or potential incidents related to Federal Information Systems.

Section 2 of the EO also notes that it is the policy of the federal government to require information and communications technology (ICT)[1] service providers to promptly report to relevant federal agencies cyber incidents involving software products or services, or support systems for software products and services supplied to such agencies. To implement this policy, the EO calls for executive agencies to recommend to the FAR Council contract language that identifies:

1. The nature of cyber incidents that require reporting;

2. The types of information that must be reported;

3. Appropriate protections for privacy and civil liberties;

4. The time periods for reporting, with reporting on severe cyber incidents not to exceed three days after initial detection;

5. National Security Systems reporting requirements; and

6. The types of contractors and service providers covered by the proposed contract language.

While the exact reach and application of these proposed new information sharing contractual obligations will become clear in the coming months with regulatory implementation, the plain language in the EO contemplates additional contractor reporting and information-sharing obligations that extend beyond particular federal contracts and related contracting agencies.

Modernizing Cybersecurity

Section 3 of the EO includes goals and directives aimed at modernizing federal government cybersecurity practices. Notably, this section sets out the following broad modernization goals:

1. Adopting security best practices;

2. Advancing toward Zero Trust Architecture;

3. Accelerating the move to cloud services;

[1] "ICT" refers generally to technologies that provide access to information through telecommunications. This includes the internet, wireless networks, cell phones, and other communication mediums. ICT enables real-time communications using technologies such as instant messaging, voice over IP (VoIP), and videoconferencing.

4. Centralizing and streamlining access to cybersecurity data; and

5. Investing in technology and personnel.

The EO directs federal agencies to develop and update existing plans to meet these goals, and to collaborate to develop appropriate guidance and documentation necessary for agencies to prioritize and implement these goals.

As part of this modernization effort, the EO directs the Administrator of General Services to work with other agencies to modernize. The Federal Risk and Authorization Management Program (FedRAMP)[2] by, *inter alia*, increasing the automation of assessments, monitoring, and compliance, as well as mapping relevant compliance frameworks to FedRAMP requirements and allowing those frameworks to be used as a substitute for the FedRAMP authorization process, where appropriate. While it appears that this modernization effort may include some reciprocity between the Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) framework and FedRAMP, details regarding the potential impact on contractors will likely become clear as agencies begin to implement these goals.

Enhancing Software Supply Chain Security

Section 4 of the EO sets out various directives intended to enhance software supply chain security. It first directs agencies to collaborate with other stakeholders to identify and/or develop standards, tools, and best practices aimed at improving the security and integrity of the software supply chain, particularly as it relates that "critical software"[3] that provides system privileges or direct access to network or computing resources. The director of the National Institute of Standards and Technology (NIST) must publish preliminary guidelines resulting from this effort and, thereafter, issue guidance that includes standards, practices, procedures, and criteria regarding:

1. Secure Software Development Environments that include:
    a. Using administratively separate build environments;
    b. Auditing trust relationships;
    c. Using multi-factor, risk-based authentication and conditional access across the enterprise;
    d. Documenting and minimizing dependencies on enterprise products that are part of the build environment;
    e. Employing encryption;
    f. Monitoring and responding to attempted and actual cyber incidents.
2. Generating artifacts that demonstrate conformance with Secure Software Development Environments requirements;

[2] FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

[3] This definition is to be developed through collaboration among the heads of relevant cybersecurity-concerned agencies (NIST, DoD, NSA, HSA, OMB and the Director of National Intelligence) for inclusion in the guidelines NIST is to issue.

3. Employing Automated Tools to maintain trusted source code supply;
4. Employing Automated Tools to check for and remediate vulnerabilities;
5. Providing to a purchaser artifacts of the Automated Tools and making certain information regarding these tools available to the public;
6. Maintaining accurate and up-to-date origin information for software code, and utilizing and auditing controls on third-party software components;
7. Providing purchasers with a Software Bill of Materials[4] for each product or publishing it on a public website;
8. Participating in a vulnerability disclosure program that includes a reporting and disclosure process;
9. Attesting to conformity with secure software development practices; and
10. Ensuring and attesting to the integrity and provenance of open source software used within any portion of a product.

Section 4 outlines various dates for the publication of key definitions and guidance required to implement the noted enhancements to the software supply chain. Notably, the EO also states that OMB will require agencies employing software developed and procured prior to the date of the EO to comply with certain requirements issued pursuant to the EO, or provide a plan outlining actions to remediate or meet those requirements.

Section 4 of the EO also includes a number of directives aimed at educating the public on the security capabilities of Internet-of-Things (IoT) devices and software development practices. Unlike most other portions of the EO, Section 4 contemplates the development and application of new standards to commercial software products, not just products that are the subject of federal procurements.

Cyber Safety Review Board

Section 5 of the EO directs the secretary of Homeland Security to establish a Cyber Safety Review Board (CSRB) responsible for reviewing and assessing threats, mitigation activities, vulnerabilities, and significant cyber incidents affecting both federal civilian agency information systems and non-federal systems. The CSRB will be comprised of federal officials and representatives from private-sector entities, and will provide recommendations for improving cybersecurity and incident response practices. The EO specifically provides that the secretary of Homeland Security will determine appropriate CSRB private-sector representatives, and that the CSRB will include representatives from DoD, the Department of Justice, the Cybersecurity & Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the FBI. The CSRB's advice and recommendations will be provided to the secretary of Homeland Security and the president.

[4] The term "Software Bill of Materials," or "SBOM," means a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components included in a product. Buyers can use an SBOM to perform vulnerability or license analysis, both of which can be used to evaluate risk in a product.

Standardizing Federal Responses

Section 2 of the EO notes that the standardization of cybersecurity requirements for unclassified systems would streamline and improve compliance for vendors and the federal government. As a result, the EO directs various federal agencies to consult and recommend to the FAR Council standardized cybersecurity contract language for unclassified systems to be used across all federal agencies. Within 60 days of receiving the recommendation, the FAR Council must publish for public comment an appropriate update to the FAR.

Section 6 of the EO also outlines various requirements intended to standardize the federal government's response to cybersecurity vulnerabilities and incidents. This section of the EO notes that current cybersecurity vulnerability and incident response procedures vary across agencies, hindering coordinated responses. As a result, the EO directs various federal agencies to develop a standard set of operational procedures (playbook) to be used in planning and conducting cybersecurity vulnerability- and incident-response activities for federal civilian agency information systems. The EO directs that the "playbook" is required to:

1. Incorporate all appropriate NIST standards;
2. Be used by all federal civilian agencies; and
3. Articulate progress and completion through all phases of an incident response, while allowing flexibility.

The EO further requires the director of CISA to review and update the "playbook" annually, and to review and validate federal civilian agency incident responses and remediations upon completion by the agency. The EO provides that the director of CISA is permitted to recommend another agency or third-party response team to perform the review and validation of incident response and remediations.

Improving the Detection of Vulnerabilities and Incidents and Improving Investigative and Remediation Capabilities

Section 7 of the EO directs federal civilian agencies to deploy an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents within the federal government, active cyber hunting, containment and remediation, and incident response. More specifically, Section 7 directs various federal agencies to provide recommendations for the implementation of the EDR initiative and requires the director of OMB to issue requirements for federal civilian agencies to adopt government-wide EDR approaches. Similar directions are included in Section 7 of the EO for National Security Systems. In addition, Section 7 directs agencies to coordinate and ensure alignment between Department of Defense Information Network (DODIN) directives and those applicable to civilian agencies.

Section 8 of the EO similarly seeks to improve investigative and remediation capabilities by directing agencies to collect and maintain network and system logs for Federal Information Systems, including those hosted by contractors. The EO directs the secretary of Homeland Security to make recommendations regarding requirements for logging events, including the types of logs to be maintained, the time periods of retention, and cryptographic methods that must be used to ensure the integrity of the logs. These recommendations are to be considered by the FAR Council when promulgating rules and contract language under Section 2 of the EO.

Key Takeaways

The EO identifies a large number of goals and changes intended to improve cybersecurity and the prevention, detection, assessment, and remediation of cyber incidents that pose a risk to national and economic security. While many of the EO's directives and goals seek increased uniformity in federal cybersecurity standards and regulations – welcome news for federal contractors – the EO also includes a number of goals and requirements that could significantly increase the reporting responsibilities and cybersecurity burdens on contractors.

The EO heralds a "ground up" review of vulnerabilities and increased incident awareness across federal agencies concerned with security; a change from past strategies that relied too heavily on methods of protecting networks against penetration (while assuming that elements within the network were worthy of trust). Whether data is at rest, in transit, or inside a network, increased emphasis on encryption and security and the imposition of zero trust for all applications within a network requesting access to data or resources suggest that there are also opportunities ahead for cybersecurity contractors as the rules and guidelines that will implement the EO take shape.

Authors

This GT Alert was prepared by:

- Scott A. Schipma | +1 202.331.3141 | schipmas@gtlaw.com
- Paul F. McQuade | +1 202.331.3187 | mcquadep@gtlaw.com