Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A Gov't Contractor's Road Map To Biden Cybersecurity Order

By **Justin Chiarodo and Sharon Klein** (June 11, 2021, 5:17 PM EDT)

Justin Chiarodo

President Joseph Biden's May 12 executive order to improve the nation's cybersecurity infrastructure heavily relies on contractual flow-downs in the purchasing power of the government to align private and public interests.[1]

The executive order mandates a rapid push to modernize federal networks, improve incident tracking and information sharing, and standardize federal incident response and oversight. Though the executive order will impact a wide swath of the private sector — including companies providing information technology, cloud computing services and the Internet of Things — government contractors will face special challenges.

Sharon Klein

We lay out in this article a road map for what government contractors can expect under the new executive order (i.e., new regulations), who will most likely be impacted (i.e., civilian agency contractors and software providers) and when we can expect concrete changes to show up in federal contracts (i.e., if the order's ambitious timeline holds, new Federal Acquisition Regulation clauses will arrive later this year).

A Brief Summary of the Executive Order

Recent high-profile attacks involving SolarWinds Inc., Colonial Pipeline Co., and Microsoft Corp's Exchange Server email system underscore the continuing challenges in preventing and minimizing cyber intrusions, promoting incident detection and response, and incorporating lessons learned from cyber events.

The executive order is an ambitious attempt to further build on the National Institute of Standards and Technologies', or NIST's, five core cybersecurity functions: identify, protect, detect, respond and recover.[2]

What does the end state of executive order implementation look like? If the goals are achieved, expect a better coordinated and managed federal incident-response strategy, the accelerated adoption of security best practices and technologies including Zero Trust Architecture[3] and secure cloud services, and improved software supply chain security.

The executive order covers a lot of ground and runs about 8,000 words, addressing a number of government-facing directives — including the governmentwide adoption of multifactor authentication, modernizing of the Federal Risk and Authorization Management Program and establishing a cybersafety review board.

Two sections stand out for their likely impact on federal contractors. Section 2, Removing Barriers to Sharing Threat Information, and Section 4, Enhancing Software Supply Chain Security.

We summarize below four key areas that we think government contractors should pay special attention to as the executive order moves into implementation.

1. New IT Security and Information-Sharing Requirements

What

Section 2 of the executive order mandates revisions to the FAR, covering contractors that provide systems that process data — information technology, or IT — and those that "run the vital machinery that ensures our safety" — operational technology, or OT. Covered contractors will need to comply with new data collection and information-sharing requirements, and collaborate with law enforcement and investigative agencies in investigations and responses impacting federal information systems.

We expect that these requirements will look similar to those now well known to defense contractors, like the incident response and reporting requirements under Defense Federal Acquisition Regulation Supplement 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

DFARS 252.204-7012, in full effect since 2017, implements security control standards set forth in NIST Special Publication 800-171, and requires contractors to report covered cyber events within 72 hours to the U.S. Department of Defense.

More recently, the DOD rolled out its Cybersecurity Maturity Model Certification, requiring varying levels of cyber hygiene consistent with the sensitivity of the procurement. We expect to see similar frameworks extending to civilian agency contracts.

Who

This affects covered providers of information and operational technology, including cloud service providers.

When

Within 60 days of the executive order — mid-July — the government will review the FAR and DFARS and recommend updates for IT and OT contractors. Within 90 days of these recommendations — mid-October — the FAR Council should publish new FAR clauses implementing these changes. Also expect guidance by this September on how covered service providers should share cyber incident data with the government.

2. New Cyber Incident Reporting Involving Software Products and Services

What

Section 2 of the executive order also mandates new FAR rulemaking requiring cyber incident reporting involving software products and services provided to the government, as well as the support systems for those products and services. This will include direct notifications to the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Agency for incidents involving civilian agencies.

This will be a big change for contractors accustomed only to the FAR's basic safeguarding clause, FAR 52.204-21, which requires basic cybersecurity hygiene but no incident reporting.

Who

This affects information and communications technology service providers, with more details to come in rulemaking.

When

Within 45 days of the executive order — late June — designated agencies will recommend to the FAR Council contract language providing details on what type of information must be reported, and when it must be reported. The most serious cyber incidents will need to be reported within 72 hours, mirroring the incident reporting period currently in the DFARS.

Within 90 days of these recommendations — late September — the FAR Council will publish a new cyber incident reporting rule.

3. Standardized Cybersecurity Requirements

What

Recognizing that cybersecurity requirements for unclassified system contracts are largely addressed through agency-specific regulations and guidance, Section 2 of the executive order also seeks to standardize common cybersecurity requirements across agencies.

Who

This affects contractors subject to existing cybersecurity regulations — almost all federal contractors.

When

Within 60 days of the executive order — mid-July — designated agencies will recommend to the FAR Council standardized contract language for appropriate cybersecurity requirements. Within 60 days of receiving these recommendations, the FAR Council will propose updates to the FAR implementing these changes.

After the public comment period, individual agencies must update their own agency-specific requirements to eliminate duplication with these new standards.

4. Enhanced Software Supply Chain Security

What

As a response to the SolarWinds breach, Section 4 of the executive order targets improving software supply chain security. Expect a particular focus on critical software — that is, software that performs functions critical to trust, like providing access to system privileges or access to networks. Notable among the mandates is revisiting a requirement for a software bill of materials, as a means of identifying impacted software and related risks.[4]

The executive order contemplates a heavy role by NIST in this process, similar to its role in current DOD cybersecurity standards. Notably, the executive order contemplates that noncompliant software shall be removed from all indefinite-delivery, indefinite-quantity contracts; federal supply schedules; federal governmentwide acquisition contracts; blanket purchase agreements and multiple-award contracts.

Who

This will affect developers, resellers and users of software — extending well into the commercial marketplace.

When

Following input from industry in the coming months, expect new NIST guidelines on software supply chain security by November — within 180 days of the executive order. Throughout this summer, expect significant attention to key definitions and standards, including the definition of critical software.

Within one year of the executive order — mid-May 2022 — designated agencies shall recommend to the FAR Council new rules regarding software security, including certification requirements. And following these FAR amendments, agencies shall begin the removal of noncompliant software for purchase by federal agencies.

Conclusion

There can be little doubt that this executive order is an ambitious use of executive power to address a serious and continuing threat to our national security. While the devil is in the details, and the rollout will take some time, government contractors and their suppliers should plan ahead and take advantage of the opportunity to evaluate their exposure, comment on the rulemaking, and prepare to bring to bear the resources they will need to operate in a new compliance environment.

Justin A. Chiarodo and Sharon R. Klein are partners at Blank Rome LLP.

[1] https://www.blankrome.com/publications/president-bidens-recent-cybersecurity-executive-order-will-increase-compliance; Executive Order on Improving the Nation's

Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[2] https://www.nist.gov/cyberframework/online-learning/five-functions.

[3] https://csrc.nist.gov/publications/detail/sp/800-207/final; https://www.nist.gov/publications/zero-trust-architecture.

[4] https://www.ntia.gov/SBOM.