SheppardMullin

Government Contracts & Investigations Blog

Latest updates on Developments Affecting Government Contracts & Investigations

Right on Time – NIST Releases Definition of “Critical Software” Per Biden’s Cybersecurity Executive Order

By Townsend Bourne & Nikole Snyder on June 29, 2021

POSTED IN CYBERSECURITY, FAR, INFORMATION TECHNOLOGY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

As called for in the May 12, 2021 Cybersecurity Executive Order (“EO”) released by the Biden Administration (discussed **here**), NIST met its deadline to release a definition of “critical software” within 45 days of the date of the Order. The determination of what constitutes “critical software” is a key step in the process set forth in the Order for securing the software supply chain, which will culminate sometime next year in new Federal Acquisition Regulations for contractors that supply software.

NIST’s definition of “critical software” as set forth in a **white paper** released on June 25, 2021 is as follows:

EO-critical software is defined as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

- is designed to run with elevated privilege or manage privileges;
- has direct or privileged access to networking or computing resources;
- is designed to control access to data or operational technology;
- performs a function critical to trust; or,
- operates outside of normal trust boundaries with privileged access.

The white paper further specifies that "[t]he definition applies to software of all forms (e.g., standalone software, software integral to specific devices or hardware components, cloud-based software) purchased for, or deployed in, production systems and used for operational purposes." Further, "[o]ther use cases, such as software solely used for research or testing that is not deployed in production systems, are outside of the scope of this definition."

NIST provides further information on key terms within the definition. For example:

- "Direct software dependencies" means, for a given component or product, "other software components (e.g., libraries, packages, modules) that are directly integrated into, and necessary for operation of, the software instance in question. This is not a systems definition of dependencies and does not include the interfaces and services of what are otherwise independent products."
- "Critical to trust" means "categories of software used for security functions such as network control, endpoint security, and network protection."

The white paper also includes a chart explaining each category of software it considers "EO-critical" as well as a list of Frequently Asked Questions (FAQs) and responses. The categories of software listed in NIST's chart include:

- Identity, credential, and access management (ICAM)
- Operating systems, hypervisors, container environments
- Web browsers
- Endpoint security

- Network control
- Network protection
- Network monitoring and configuration
- Operational monitoring and analysis
- Remote scanning
- Remote access and configuration management
- Backup/recovery and remote storage

Contractors that provide software throughout the government supply chain, particularly those that provide what may be considered “EO-critical” software, should be closely following agency activity under the EO relating to software, which will include publishing minimum elements for a Software Bill of Materials (SBOM) and guidance for security measures for critical software (both in mid-July). Further, contractors should anticipate new requirements next year that must be implemented (and likely flowed down to suppliers and subcontractors) in order to continue to supply certain software to the federal government.

Government Contracts & Investigations Blog