May 26, 2021
National Institute of Standards and Technology (NIST)
Via email to swsupplychain-eo@nist.gov

Position Paper on Standards and Guidelines to Enhance Software Supply Chain Security

Palo Alto Networks appreciates the opportunity to provide input to NIST's call for papers on standards and guidelines to enhance software supply chain security, per the requirements of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*. As the world's largest cybersecurity company, we serve more than 80,000 enterprise and government organizations--protecting billions of people--in more than 150 countries, and we collaborate with key government stakeholders on policy and operational matters.

At Palo Alto Networks, our highest priorities are the integrity of our products and security of our customers. Palo Alto Networks has instituted a number of best practices and processes to ensure the integrity of its products. Our approach standardizes the software development, deployment, delivery, and operation pipeline to ensure there are sufficient and necessary security controls in all phases.

Below, please find specific responses to question areas 2, 4, and 5.

2. *Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government.*

First, the Administration should finalize and implement existing authorities designed to improve supply chain security, in particular Section 1655 of the FY2019 National Defense Authorization Act, which requires vendors to the U.S. Department of Defense to disclose whether they have shared the source code of products with certain countries of concern.

Second, pursuant to EO Section 4(e)(1), a foundational requirement for software development environments should incorporate secure infrastructure-as-code. Infrastructure-as-code is increasingly used to streamline development processes by enabling software developers to configure cloud resources at scale. A recent Palo Alto Networks report found more than 199,000 potential vulnerabilities in infrastructure-as-code templates.[1] Secure infrastructure-as-code processes should provide security assessment and enforcement capabilities throughout the DevSecOps lifecycle.

Third, the U.S. government should ensure that specific security measures are applied to critical software. Among these: restrictions on who scopes and defines source code changes, reviewing new source code with a hierarchy of oversight, and ensuring a chain of custody throughout development, testing and quality assurance processes. Development managers should be required to review and sign off on all code changes. These checks mitigate the risk of any modification to the code that was not approved in design specifications.

[1] https://unit42.paloaltonetworks.com/cloudy-with-a-chance-of-entropy/

3. *Initial minimum requirements for testing software source code.*

Organizations should employ a secure continuous integration/continuous delivery (CI/CD) "shift left" approach that focuses on integrating security tools early into the engineering lifecycle. Controls like static and dynamic analysis help detect any inadvertent vulnerabilities in code. In particular, minimum requirements for testing software code, pursuant to EO Sec. 4(e)(iv), should include:

- Static Application Security Testing (SAST), also known as "white box testing," a process of reviewing source code to identify security vulnerabilities.
- Open Source Software Vulnerability Analysis (OSSVA), which identifies vulnerabilities in third-party components and provides visibility into third-party code for control across the software supply chain.
- Container Vulnerability Analysis (CVA), a process of evaluating containers against common container misconfiguration and software package vulnerabilities.
- Secure Infrastructure-as-code, a process to identify, prevent and remediate security misconfigurations in infrastructure code before deployments in cloud such as: unauthorized privileges, network exposure, public storage buckets.

5. *Guidelines for software integrity chains and provenance.*

The most impactful step the U.S. government can take to maintain "accurate and up-to-date data... of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes," and perform "audits and enforcement of these controls on a recurring basis," as required in EO Sec. 4(e)(vi), is to deploy a capability for the continuous discovery, monitoring, and management of Internet-facing systems and assets and their activities on the Internet. Such a capability could be used to identify government or critical infrastructure-run software utilizing prohibited equipment or services such as those banned under Section 889 of the FY2019 National Defense Authorization Act. The capability could also create a complete system of records of all U.S. government or critical infrastructure Internet assets, detect potential vulnerabilities for immediate remediation, assess Internet-facing asset compliance with CISA directives, and provide real-time, ongoing tracking and awareness with centralized reporting. By focusing on software intentionally or unintentionally connected to the Internet, such a capability would assist network security personnel in prioritizing systems for remediation or mitigation in the event of a discovered zero-day vulnerability exploitation.

**

Finally, Palo Alto Networks welcomes the opportunity to be considered as a speaker at the workshop. Senior-level Palo Alto Networks experts are available to present on each of the question areas addressed above. Coleman Mehta, Senior Director, U.S. Policy, cmehta@paloaltonetworks.com, can facilitate briefing requests for the workshop.