Enterprise Cloud Coalition

May 26, 2021

RE: Comments from the Enterprise Cloud Coalition Responding to NIST's Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security

Submitted via email to swsupplychain-eo@nist.gov

On behalf of the Enterprise Cloud Coalition (ECC), it is my pleasure to submit these position statements for the National Institute of Standards and Technology (NIST) efforts on the President's Executive Order on Improving the Cybersecurity of the Federal Government (14028), issued on May 12, 2021. By way of background, the ECC is a group of companies that are united by a common business model and shared policy concerns. Our main objective is to educate policymakers about cloud computing, including the underlying technology, and how cloud computing both promotes innovation and benefits enterprises and their customers.

Overview

As NIST is aware, given its long track record on working with all stakeholders to improve the state of cybersecurity, there are no silver bullets, there are no universally applicable checklists, there is no set of best practices that inevitably improve the state of cybersecurity immediately. The EO has appropriately highlighted the dauntingly large set of rules, standards, and guidelines that will be needed to improve federal cybersecurity. It will be essential that the public and private sector stakeholders that shape a more secure future for federal and private sector networks take a balanced, technology neutral, risk-based approach to the problem. It is essential that all stakeholders understand that forcing a solution on one link of the supply chain that is designed for another link (say cloud services versus government hosted "on-premises" solutions) could create a false sense of security and ultimately do more harm than good.

Therefore, the initial step in each of the strategic questions NIST is tasked with helping answer must identify and prioritize the risks associated with each of the elements (i.e., the "links") in the entire supply chain of systems serving the government. Once risks are identified and prioritized, specific rules, guidance, standards, and controls can then be established.

While this may seem like a long-term approach to the many short-term deadlines established by this EO, this risk categorization is absolutely critical, as it will provide a shared understanding of the appropriate framework for addressing the highest risks immediately before turning to important, but lower risk, items.

Answers to Questions 1 through 4

On question 1 regarding critical software, the ECC believes that the definition of "critical software" should not encompass every software element that might pose a vulnerability risk, as this would capture virtually any system on a network. Instead, the definition of "critical software" should take a risk-management based approach to cybersecurity and should be specific enough for organizations to understand how they are classified. By taking this focused approach to critical software, NIST can more effectively target federal resources at ensuring that the most critical pieces of software utilized by the federal government are in fact secured and managed according to the risk they pose to the federal system user. Furthermore, organizations and the global community should be given assurances that

working with the federal government as a "critical software" provider does not require additional data sharing outside of a standard customer-software provider relationship. This is important to ensure that software providers are not deterred from working with the federal government due to the potential perception of additional data sharing from software providers' other customers, both in the U.S. and abroad.

On question 2 regarding secure software development lifecycle standards, the ECC believes that all proposed guidelines, best practices, or standards adopted as a result of the EO must be technology and tool agnostic. These proposed guidelines, best practices, or standards adopted because of the EO should focus specifically on practices, procedures and architecture guidelines that set forth a risk-based approach to secure development and consider the nature and risk level associated with a given software component. By taking this approach, companies would be able to comply with a targeted list of guidelines, best practices or standards that are the most effective in improving cybersecurity for the federal community.

Additionally, in terms of a software development lifecycle, NIST should consider establishing a minimum bar, with requirements that are measurable. For example, as part of this process NIST might issue guidance saying, "Build systems should not pull untrusted code from the Internet during the build process," with a corollary test that could say "Build systems do not have access to the Internet" and "All build dependencies are either part of the build environment base image or contained in the source code repository." The ECC also believes all code bases, whether developed internally or incorporated from third-party sources, must have an identified internal owner(s) with appropriate succession planning and absence coverage. These internal owners should be responsible for documentation of their product architecture, as well as monitoring for and incorporating into the code base publicly available security patches. Software developers should also understand and build mitigations to potential threats into their products, and code should always be reviewed by another person or by some other process to identify potential security risks.

A similar approach has been implemented successfully with PCI standards, and has created some important predictability about the changes that will come. This approach might be further expanded or coordinated through the Cyber Safety Review Board.

On question 3, guidelines for critical software, the ECC believes that critical software deployed by the government must not utilize traditional network-level access systems for use, management, or support. Instead, critical software must be deployed in a manner that ensures an appropriate Zero Trust Architecture to support the function of the relevant software or system.

Additionally, all critical application services should be protected with a Zero Trust access model so that all access, both outbound and inbound, goes through an identity aware proxy. On the inbound side, only strongly authenticated and authorized users (or other software systems) should have access or be able to "see" such applications. On the outbound side, such applications should be able to access only those systems that are required for it to perform its functions. In addition, as a best practice, critical software applications should be independently audited per widely accepted standards, such as the International Organization for Standardization (ISO) standards, to ensure that important security measures, such as least-privilege and data segregation, are functioning properly.

Finally, throughout this guidelines-generating process, we believe there should be a strong emphasis on updating existing standards rather than creating new ones.

On question 4, minimum code testing requirements, testing software source code should rely on a risk-based approach that focuses on the specific risk areas for a given piece of software and should include penetration testing and code reviews for some products.

Thank you very much for this opportunity to contribute to NIST's important work in improving the state of federal cybersecurity. We look forward to being part of this dialogue going forward and stand at the ready to answer any questions you might have.

Andrew Howell
Enterprise Cloud Coalition
andrew@enterprisecloudcoalition.org
https://www.enterprisecloudcoalition.org/