ca technologies

607 14th St. NW, Suite 660
Washington, DC 20005

January 19, 2018

VIA EMAIL: cyberframework@nist.gov

Edwin Games
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: CA Technologies Comment on Version 1.1 Draft 2 of the Framework for Improving Critical Infrastructure Cybersecurity

CA Technologies appreciates the opportunity to provide comments on Version 1.1 Draft 2 of the Framework for Improving Critical Infrastructure Cybersecurity (Framework). CA Technologies is a global leader in software solutions enabling customers to plan, develop, manage and secure applications and enterprise environments across distributed, cloud, mobile and mainframe platforms. Most of the Global Fortune 500, as well as many government agencies around the world, rely on CA to help manage their increasingly dynamic and complex IT environments.

CA Technologies supports the updates NIST has included in Version 1.1 Draft 2 of the Framework, in particular the new updates on authentication under identity management and access control, and on applying the Framework throughout the life cycle phases of design, build/buy, deploy, operate, and decommission. We have provided more detailed comments on these updates as well as recommended changes for NIST to consider in both the Framework Core and the Framework Roadmap in our response below. Specifically, our response outlines additional detail around state of the art access management and authentication technologies, which NIST can consider in the Access Management subcategories in the Protect Function of the Framework Core, and requests that NIST focus on secure software development processes and practices in the Framework Roadmap.

CA Technologies Use of the Cybersecurity Framework and Changes to the Framework

CA Technologies has been an active user of the Cybersecurity Framework for more than two years. The Framework helps provide a common lexicon to discuss cybersecurity risks and priorities throughout our enterprise, and with customers and suppliers. CA has adopted the Framework as the central, organizing foundation for our internal information security program, and it serves as the means through which we communicate CA's cybersecurity posture to our Board of Directors.

CA Technologies is utilizing the Framework to assess, prioritize, and improve our own cybersecurity program. Our use of the Framework reaffirmed and validated many of the controls and processes that we already had in place, and it also aligned with areas where we were investing to improve technology processes. We are using the Framework to continuously evaluate and measure our cybersecurity program and to prioritize the investments we are making to improve our overall posture in a constantly changing cyber threat landscape.

CA Technologies believes the changes to the Framework in Version 1.1 Draft 2 are an effective reflection of changes in the cybersecurity landscape. We don't believe these changes will make a significant difference in our use of the Framework, but they will help provide greater clarity both internally and externally. We expect that the changes will create some small changes in our cybersecurity program, but we believe these changes are useful with respect to the way cybersecurity risk management is evolving. In particular, the inclusion of new provisions on supply chain risk management in both the Core and Tiers effectively address a significant potential threat vector. In addition, the inclusion of new language on metrics and measurement will help provide stronger consistency in internal assessments of our Framework use.

Identity Management, Authentication and Access Control

CA Technologies welcomes updates to the Identity Management, Authentication and Access Control category in the Framework Core. The addition of new language in Subcategory PR.AC-1, whereby identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes, more accurately reflects current cybersecurity activities in the access management space.

CA Technologies requests the following changes to subcategories within the Identity Management, Authentication and Access Control category to best reflect modern cybersecurity practices and market demand:

- PR.AC-4: CA requests that NIST add language regarding "users with enhanced privileges." The new Subcategory language would read: "Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties, including permissions and authorizations for users with enhanced privileges (e.g. IT administrators, CIOs, CISOs, others)."

  One of the most important areas of IT risk relates to privileged users. Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations and the overall security and privacy of organizational assets and information. Therefore, it is essential that administrators be allowed to perform only those actions that are essential for their role—enabling "least privileged access" for reduced risk. This visibility provides insight on activity and works to prevent or flag anything unusual that indicates security risk.

  It is important to highlight privileged users, specifically, because privileged user credentials were exploited in the preponderance of recent high-profile hacks, enabling attackers to extract much more sensitive data.

The importance of implementing identity management and access control measures for privileged users is recognized in cybersecurity standards, including the NIST 800-53 Rev 4 standard.

- PR.AC-7: CA welcomes the addition of PR.AC-7 on authentication. However, CA requests that "analytics" be added as one of the examples in the e.g. parenthetical. The new language would read: "Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor, analytics) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

  Analytics and/or risk-based authentication were discussed at the 2017 NIST Framework workshop in Gaithersburg in both the identity management and access control breakout session, and in the plenary read-out at the end of the workshop. User experience has become more important in the digital economy because consumers and citizens are demanding intuitive experiences. Security interfaces that are inconvenient and cumbersome often force users into work-arounds, many of which end up violating security policy, even unwittingly.

  Analytics and risk-based authentication have the benefit of not only facilitating the authentication of the identity but, because of the context that is provided under risk-based models, can also facilitate the recognition of the identity. This means that when there is a better understanding of the context around the identity, such as through geo-location data or purchasing behavior, the system may recognize the identity, determine that traditional authentication is unnecessary based on appropriate risk factors, and allow access.

  Gartner's "Market Guide for User and Entity Behavior Analytics[1]" and Forrester's "The Future of Identity and Access Management[2]" both highlight the use of analytics and risk based authentication methods increasingly in use in the marketplace.

Secure Software Development Processes and Practices in the Framework Roadmap

CA Technologies supports the inclusion of new language in Section 3.0 'How to Use the Framework' on how the Framework can be applied in design, build/buy, deploy, operate, and decommission system lifecycle phases. Cybersecurity must be considered throughout the information technology activities of an organization, especially as organizations across the full range of industry and government sectors increasingly leverage digital technologies in the delivery of products and services to their customers and citizens.

Software applications are increasingly integrated into our commercial and infrastructure processes to improve efficiencies. The global economy, critical infrastructure and government operations have increased their dependence on software. However, this makes software applications a prime target for hackers.

[1] https://www.gartner.com/doc/3134524/market-guide-user-entity-behavior
[2] https://www.forrester.com/report/The+Future+Of+Identity+And+Access+Management/-/E-RES136522

Data from CA Veracode's 2017 State of Software Security (SOSS) Report[3] demonstrate the pervasive risk of software security. For example, the frequent use of software components speeds up development, but also increases risk. In the past, vulnerabilities were isolated to the single application in which they resided, requiring hackers to create an exploit that targeted only one application. Today, the widespread use of components means a vulnerability in a single component can reach thousands of applications – so a hacker must only create one virus or program to breach thousands of applications and potentially millions of companies. Examination by CA Veracode demonstrated that 77 percent of applications had at least one vulnerability on initial scan.

While the importance of software has increased, the way software is developed and deployed has continued to evolve. In addition to the importance applications play in our economy, contemporary application development methodologies like DevOps (combining development and operations practices) are increasing the speed and precision with which software is produced and deployed. The ability to create software that can resist modern forms of attack and exploits will be crucial to our ability to protect not just applications, but the social, economic and political processes that depend on that software.

Development use cases for the Framework can demonstrate the benefits of employing a secure software development process, which utilizes a mix of developer education, threat modeling, architectural risk assessment, code scanning and analysis, penetration testing, and continuous tracking of known vulnerabilities and attack vectors.

CA Technologies is a charter member of SAFECode (the Software Assurance Forum for Excellence in Code)[4], a non-profit organization, made up of leading software development companies, dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode develops software assurance guidance publications available for free to the public, outlining software development best practices for developers and organizations. For instance, the SAFECode publication, "Fundamental Practices for Secure Software Development, 2nd Edition,"[5] is designed to help others in the industry initiate or improve their own software security programs and to encourage the industry-wide adoption of fundamental secure development methods.

CA Technologies requests NIST takes the following action items to promote secure software development practices through the Framework:

- CA requests that NIST include a new subsection in Section 4 of the Framework Roadmap on "Secure Software Development Processes and Practices."
- NIST, through the National Cybersecurity Center of Excellence, can partner with leading software assurance organizations, such as SAFECode, and other stakeholders, to develop risk-based, scalable guidance on effective secure software development processes and practices.

[3] https://www.veracode.com/resources/state-of-software-security

[4] https://safecode.org/

[5] https://www.safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf

- NIST can work with industry and other stakeholders to develop a Framework profile focused on secure software development.
- NIST can work with international governments to promote policies that align with international standards and enable continued innovation and flexibility in secure software development, while strengthening security. An emerging ISO Standard, ISO 27034 can provide a basis for independent certification of conformance with software security assurance best practices in the future.

Conclusion

The Cybersecurity Framework is increasingly being adopted by a full range of critical infrastructure and other organizations, both in the US and internationally. The flexibility built into the Framework recognizes that different organizations have diverse business and cybersecurity priorities, and face a range of distinct threats. The Framework provides a common lexicon for communicating cybersecurity threats both within and across organizations, and it promotes continuous assessment and improvement.

Version 1.1 Draft 2 of the Framework incorporates key changes to reflect the changing dynamic of the cybersecurity landscape, including the introduction of metrics, the inclusion of supply chain risk management, and the updating of identity management and access control outcomes. While it is helpful to update the Framework as cybersecurity threats and practices evolve, it is also important to ensure that the Framework is accessible to new users. CA Technologies believes version 1.1 Draft 2 largely achieves this balance.

We recommend that NIST incorporate a reference to privileged users in PR.AC-4, and include analytics in its examples of authentication in PR.AC-7. Further, we recommend that NIST add Secure Software Development Processes and Practices as an addition to Section 4 of the Framework Roadmap.

We appreciate the opportunity to comment on this second draft of Version 1.1 of the Framework, and we look forward to continue working with NIST, industry, and other stakeholders to improve US and global cybersecurity.