From: **Brown, Jamie**
Date: Mon, Apr 10, 2017 at 6:17 PM
Subject: CA Technologies Submission: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Dear Mr. Games,

Please find attached a submission from CA Technologies, regarding our Comments on the Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity. As part our submission, we cite a research report, which is also attached, as an appendix to our submission.

Please feel free to contact me if you have any questions about our submission.

Best regards,
Jamie Brown

Jamie Brown
Director, Global Government Relations

CA Technologies | 607 14th Street, NW Suite 660 | Washington, DC 20005

[Attachment Copied Below]

CA TECHNOLOGIES | Business rewritten by software

Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity

Prepared for:

National Institute of Standards and Technology

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

CA Technologies Point of Contact:
Jamie Brown
Director, Global Government Relations, CA, Inc.

Table of Contents

Section 1: Introduction:

CA Technologies appreciates the opportunity to provide comments on draft Version 1.1 of the Cybersecurity Framework (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 environments.

Since the original release of the Framework in February 2014, the cybersecurity landscape has continued to evolve. It is important that the Framework reflect current best practices and processes. Therefore, this is an opportune time to revisit the Framework and determine whether updates and refinements are necessary and/or appropriate.

CA Technologies supports the updates NIST has included in Draft Version 1.1, including new updates on cybersecurity metrics and measurements, cyber supply chain risk management, applications for use of the Framework, and identity management and access control—all key components of cybersecurity programs. We have provided more detailed comments on these updates and on other areas for NIST to consider in our response below. Specifically, our response outlines additional detail around state of the art identity and access management technologies, which NIST can consider in future updates to the Protect Function in the Framework Core or in updates to the Framework Roadmap.

Section 2: CA Technologies Use of the Framework

CA Technologies has been an active user of the Cybersecurity Framework for more than a year. It helps provide a common lexicon to discuss cybersecurity risks and priorities across our entire 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.

Section 3: Metrics and Measurements

CA Technologies supports NIST's efforts to introduce means of applying metrics and measurements to Framework use. CA believes that the discussion around metrics and measurements is both timely and important. Metrics and measurements can help organizations communicate cybersecurity activities and progress to internal and external stakeholders, as appropriate. They can also serve to more closely relate cybersecurity activities and outcomes to business risk management activities and outcomes. However, because the discussion around metrics and measurements is still evolving, CA believes that NIST should make clear that Section 4.0, Measuring and Demonstrating Cybersecurity, and particularly Subsection 4.2, Types of Cybersecurity Measurement, are meant to serve as potential guidance for organizations that wish to develop measurement systems, rather than a specific recommended approach. Organizations may choose to develop different metrics and measurements, based on their

unique threat environments, risk tolerances, assets and resources.

Section 4: Cyber Supply Chain Risk Management

CA Technologies supports the addition of a cyber supply chain risk management category in the Identify Function of the Framework Core as it reflects a key risk factor facing critical infrastructure organizations, and multiple other organizations. However, CA would recommend against any further additions to the Core regarding cyber supply chain risk management until the standards landscape develops further in this space.

Section 5: Applications for Use of the Framework

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.

CA recommends that NIST develop specific use cases for the full spectrum of activities under which the Framework can be applied, as this will help make the Framework more accessible to multiple organizations. This will be increasingly important in IoT device and software development, as the number of internet-connected devices continues to proliferate at an exponential pace. An increasing number of organizations are utilizing third-party, open source components in their development processes, and it is important to determine whether any of these components include potentially harmful vulnerabilities. Development use cases for the Framework can demonstrate the benefits of employing a secure software development process, which utilizes a mix of education, threat modeling, architectural risk assessment, code scanning and analysis, penetration testing, and continuous tracking of known vulnerabilities and attack vectors.

In order to support use cases in software development, NIST could update ID.RA-1 to state: "Asset vulnerabilities, including systems, devices and software, are identified and documented."

Section 6: Identity Management and Access Control

CA Technologies sees updates to the identity management and access control category as very helpful. 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 believes that NIST should include a new subcategory in the Identity Management and Access Control category on the use of authentication, including both multi-factor and risk-factor authentication, when appropriate. CA also believes that NIST should consider adding language around the importance of device and machine to machine authentication, as critical infrastructure organizations are increasingly using network-connected automated systems and processes to deliver services. CA further believes subsection PR.AC-4 could be expanded to include language that specifically recognizes the management of administrative and shared account access.

Identity is now the attack vector of choice for cyber criminals. In virtually every large network breach in recent memory, compromised identities were the common thread. Protecting identities is foundational

to robust security in the application economy.

CA Technologies believes that Identity and Access Management (IAM) and API management technologies are central to protecting systems, networks, devices and data, and enabling secure interactions with customers and citizens.
Identities constitute the new security perimeter and are the single unifying control point across all apps, devices, data and users. Identity and access management software authenticates individuals and services and governs the actions they are permitted to take. API management software authenticates devices and data and is fundamental to securing the IoT. API management software also secures and protects the APIs themselves from threats, and ensures authorized access to the APIs by the approved apps and individuals. As such, identities and APIs serve as the foundations of the application economy because they enable secure development, deployment and management of applications. They are how one protects access to apps and data, whether that be by human to machine or machine to machine.

IAM has always been about establishing, managing, and understanding the relationships between resources and those that need to access and interact with those resources. This serves as the basis for logical security, independent of the physical location of where the resource resides or where the subject that is interacting with these resources resides. IAM determines the policies by which appropriate access is defined, which requires an understanding of both the subject and the resource as well as the context through which they can and should interact. IAM also provides the opportunity for greater understanding of the subject, which enables organizations and governments to provide better quality and more tailored services.

The overall user experience has become more important in the application economy because customers won't tolerate a poor experience for long – business requires a quality and efficient experience that will drive customer retention and loyalty. "Frictionless Security" becomes the business imperative for most organizations. However, the value of a quality user experience is not based solely on increased user satisfaction. Security interfaces that are inconvenient and cumbersome often force users into work-arounds, many of which end up violating security policy, even unwittingly. In short, users need a convenient, intuitive experience that will enable them to easily conform to established security policy, rather than an experience that encourages them to violate security policy to get their jobs done. Below are some components of what CA believes comprise a frictionless authentication experience.

Continuous authentication methods leverage behavioral and biometrics monitoring throughout a user session to determine if the session has been compromised. This provides a consistent level of assurance throughout the session rather than only checking at the beginning of the session.

Risk-based authentication has 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, and allow access. Conversely, if the system detects anomalies, such as logging in from a foreign country in the middle of the night after having a few failed passwords, then this is a very high-risk operation and access will be denied absent additional authentication steps.

Privileged Access Management solutions provide the visibility, monitoring and control needed for those users and accounts that have the "keys to the kingdom." 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.

As part of our submission, CA Technologies has attached recent research that we conducted in partnership with Coleman Parkes on the value business leaders place on strong identity-centric security. The research demonstrates that advanced users of identity-centric security see significant improvements in business outcomes, such as improvement in digital reach, customer experience and customer retention.[1]

[1] https://www.ca.com/us/rewrite/articles/security/the-security-imperative--driving-business-growth-in-the-app-econ.register.html

Section 7: Promoting the Framework with Federal Agencies and State and Local Governments

CA Technologies believes that one of the best steps the U.S. Government can take to increase the sharing of best practices is to promote alignment of federal information security practices with the Framework Core. A majority of information security vendors service both the public and private sectors. Aligning Federal Information Security Management Act requirements with the Framework subcategories, and mapping these requirements to other global standards referenced in the Framework, will enable more vendors to compete in the public and private sector information security marketplace, driving further innovation and improving security capabilities.

In addition, NIST should continue to support public and private sector efforts to align state cybersecurity requirements with the Framework, to avoid a patchwork of cybersecurity compliance requirements across multiple states. We are encouraged by the work of the National Governors Association to help states utilize the Framework.[2]

Section 8: Promoting the Framework with International Governments

NIST and its federal agency partners should increase resources dedicated to the promotion of the Framework, and its flexible, technology-neutral approach with global government counterparts. International acceptance of industry-led, global cybersecurity standards allows for even greater competition and innovation in the marketplace. International adoption of the Framework approach to critical infrastructure cybersecurity establishes a common lexicon across a range of stakeholders, yet allows for technology flexibility to address unique threats and priorities. While CA recognizes there may be a need for distinct national policies at the margins, these should build on an aligned approach exemplified by the Framework, and should not create alternative and potentially contradictory approaches.

Section 9: Providing Use Cases for the Framework

CA continues to support federal government efforts to promote critical infrastructure cybersecurity guidance alignment with the Framework. NIST has cited Gartner research, which estimated that the Framework had been adopted by 30 percent of organizations in 2016, and which projected that use

would climb to 50 percent by 2020[3]. NIST can accelerate this process by continuing to develop strong use cases for critical infrastructure industry sectors, and by working with sector specific agencies to align any existing or proposed cybersecurity guidance and/or regulations with the Framework.

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. It provides a common lexicon for communicating cybersecurity threats both within and across organizations, and it promotes continuous assessment and improvement.

Version 1.1 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 make some changes as
cybersecurity evolves, it is also important to ensure that the Framework is accessible to new users. CA Technologies believes version 1.1 largely achieves this balance. We recommend that NIST incorporate additional authentication language into the Protect Function of the Framework. And we encourage NIST to continue its strong focus on building awareness and adoption of the Framework both within the US and internationally.

[2] http://ci.nga.org/cms/home/ci1617/index.html
[3] https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success