CA TECHNOLOGIES | Business rewritten by software

Views on the Framework for Improving Critical Infrastructure Cybersecurity

Prepared for:

National Institute of Standards and Technology

Attn: Diane Honeycutt
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.
Jamie.Brown@ca.com

2291 Wood Oak Drive
Herndon, VA 20171-2823

February 23, 2016

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899
Via email: cyberframework@nist.gov

Reference: Views on the Framework for Improving Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

CA Technologies (CA) appreciates this opportunity to provide comments to the National Institute of Standards and Technology (NIST) on the variety of ways in which the Framework for Improving Critical Infrastructure Cybersecurity (the Framework) is being used to improve cybersecurity risk management, how best practices for using the Framework are being shared, the relative value of different parts of the Framework, the possible need for an update of the Framework, and options for long-term governance of the Framework.

CA Technologies helps customers succeed in a future where every business is being rewritten by software. From planning to development to management to security, at CA we create software that fuels transformation for companies in the application economy.

CA Technologies is responding to this RFI as a user of the Framework, as a subject matter expert on information security, and as a global company familiar with the wide range of cybersecurity regulatory and assessment approaches being pursued around the world.

Our response to the RFI is provided in the enclosed attachment. We look forward to continue working with NIST and other agencies on promoting awareness and encouraging use of the Framework, and on developing the next generation of security solutions to improve critical infrastructure cybersecurity. If you have any questions or comments, please contact Jamie Brown (jamie.brown@ca.com).

Sincerely,

Jamie Brown
Director, Global Government Relations
CA, Inc.

Table of Contents

Section 1: Use of the Framework:

Cybersecurity is vital to the continued development and success of the application economy. Indeed, the application economy depends on user trust. Effective cybersecurity, which helps secure transactions, protect data, and safeguard industrial control systems, helps build this trust. The Framework for Improving Critical Infrastructure Cybersecurity (the "Framework") provides owners and operators of critical infrastructure with a risk management-based, flexible approach to addressing cybersecurity threats. CA Technologies values the Framework because it provides a common language for us to discuss cybersecurity risks and priorities across our entire enterprise, and with customers and suppliers.

CA Technologies is utilizing the Framework to assess, prioritize, and improve our own cybersecurity program. CA initiated its use of the Framework by conducting an internal mapping of our cybersecurity program controls. This helped us become familiar with the terminology and approach of the Framework. CA maintains an ISO 27001 certification as part of its enterprise-wide information security governance. ISO 27001 is a key informative reference used throughout the Framework. We contracted with a major third party consulting firm to assess our controls against the categories and subcategories of the Framework. Our leadership team felt it was important to conduct an independent assessment, as this would help provide an objective picture of our overall cybersecurity posture. Our information security team is currently reviewing the recommendations and action plans with company leadership, and we intend to implement continuing improvements to our cybersecurity plan in the new fiscal year.

Our use of the Framework reaffirmed and validated a number of the controls and processes that we had in place, and it also aligned with areas where we were investing to improve technology processes. Our plan is to use the Framework to continuously evaluate and measure how the enhancements we implement are improving our overall posture in a continuously changing cyber threat landscape.

Overall, we've found the Framework Core and Profiles to be most helpful in our efforts. The Core provides a set of cybersecurity outcomes and best practices for potential implementation. The Profiles enable an organization to assess its own unique environment and to establish a target state. The implementation tiers are helpful to communicate an overall, quantifiable assessment within an organization. However, CA recommends against relying on the implementation tiers to determine an external "score" for an organization due to their subjectivity.

We plan to continue using the Framework on a recurring basis to help us develop new target states and to prioritize action plans to address the dynamic cyber threat environment and our unique priorities. We are also exploring other areas within CA where we may expand our use of the Framework beyond our own internal information technology environment.

CA Technologies has also been active in helping our customers and other interested stakeholders understand and use the Framework. CA provides a wide range of IT management tools that organizations worldwide use to manage, monitor and secure their IT systems. CA has developed a comprehensive solutions guide, an e-book, and other marketing materials to demonstrate how customers can deploy CA security and other IT management solutions in their adoption of the Framework.

CA has also conducted webinars through both CA and through the Information Systems Audit and Control Association (ISACA), describing the goals and contents of the Framework, and including a particular focus on how organizations can leverage identity and access management tools as part of the “Protect” function of the Framework.

CA has blogged extensively about the usefulness of the Framework approach for critical infrastructure organizations both in the US and abroad. In addition, CA experts have participated in multiple US and international cybersecurity panels focused on use of the Framework and on the principles which underpin it.

Section 2: Possible Framework Updates

CA Technologies believes that NIST and its Federal agency partners’ efforts should remain focused on promoting understanding and adoption of the Framework, rather than on updating the Framework at this point. The Framework is beginning to gain traction in a range of sectors, and across international borders. CA’s recent adoption of the Framework approach, as outlined above, is a good example of this traction.

NIST, and its Federal agency partners, would risk undermining the progress being made on several fronts by changing or expanding the functions, categories and subcategories of the Framework Core. However, CA supports the inclusion of additional informative references that help organizations achieve the security outcomes in the Framework subcategories, if they have broad support and are underpinned by global, industry-driven standards.

CA recommends that NIST continue to work with sector-specific agencies and independent regulators in developing sector-specific use cases and implementation guidance for the Framework. Pre-existing sector-specific regulatory requirements should be incorporated in these sector-specific guidance documents, in a way that does not undermine or contradict the cross-sectoral categories and subcategories of the Framework Core.

Section 3: Sharing Information on Using the Framework

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, so as to avoid a patchwork of cybersecurity compliance requirements across multiple states.

Further, NIST and its Federal agency partners should expand their promotion of these approaches with their global government partners. 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 off of an aligned approach exemplified by the Framework, and should not create alternative and potentially contradictory approaches.

Section 4: Private Sector Involvement in the Future Governance of the Framework

CA Technologies believes that global, industry-led, multi-stakeholder governance of the Framework will be a key component of the future success of the Framework. However, CA believes that a governance transition at this time is premature. NIST has earned a position of trust with key stakeholders across US and global industry, federal, state and local government officials, the privacy and civil liberties community, and global government officials. NIST's ability to convene stakeholders in a transparent, inclusive process is paramount to continued success of the Framework process as broad adoption is gaining traction. CA supports efforts to outline a future process by which governance of the Framework would transfer over time to the stakeholder community, though we believe NIST should continue to play a central, driving role in the short to medium term.

Conclusion

The burgeoning Application Economy provides significant opportunities to increase efficiency and improve quality of life. However, we will not be able to maximize the benefits of digital transformation unless there is strong user trust, underpinned by effective cybersecurity. CA Technologies appreciates NIST's efforts in driving the development and promotion of the Framework for Improving Critical Infrastructure Cybersecurity. We look forward to continued engagement with NIST, global industry, and other key stakeholders as we work together to promote efforts to improve critical infrastructure cybersecurity.