From: Martella, Joseph
Sent: Wednesday, April 20, 2022 12:37 PM
To: CSF-SCRM-RFI <CSF-SCRM-RFI@nist.gov>
Subject: Request for Information about Evaluating and Improving Cybersecurity Resources: Response from American Airlines

Greetings,

Please find attached an MS-Word document with response information to the questions that were put forth as a request for information regarding the use and opinions of the NIST Cybersecurity Framework (CSF).

Joseph (Joe) Martella
[redacted]
Sr Architect, IT Security Assurance
Cybersecurity
SkyView 8E.6E.098A
American Airlines

Response provided by American Airlines in response to:

National Institute of Standards and Technology

[Docket Number: 220210–0045]

Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice; request for information

Use of the NIST Cybersecurity Framework:

1. The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.

   The CSF five functions gives us better optics into where we succeed & fail in detecting/identifying risks, protecting our processes and data, and responding to & recovering from exposed vulnerabilities. Reviewing the categories/subcategories with our product teams gives us the opportunity for retrospection into our own process to determine strengths and weaknesses.

   CSF seems more like a ground level path for establishing a security program for businesses that have nothing or limited capability to implement a viable cybersecurity program. The very high-level nature of CSF categories and sub-categories essentially ‘gets the ball rolling’ focusing more on the ‘what’ rather than the deeper ‘how’ of a cybersecurity framework.

2. Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)?

   While CSF establishes a common ground that ‘could’ enhance communications within organizations in establishing a ‘platform’ approach to cybersecurity, between organizations does not inherently seem improved or enhanced due to the sheer number of framework solutions that companies can independently choose to implement (e.g. 800-171, 800-53, CMMC, COBIT, ISO, etc.)

   Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks?

   In the sense that the framework categorizes and sub-categorizes cybersecurity controls, CSF adds a level of ‘organization’ to help organizations ensure that critical areas of cybersecurity are not overlooked. CSF is more of a plan to manage risks rather than an actual tool to manage risks insofar as actual controls manage risks to a much greater level than categories or sub-categories.

What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?

Metrics for cybersecurity improvements are much more of an individual company output than a framework output. As written, the NIST CSF, lacking the 'how' depth, is not conducive in its present form to be a tool useful to articulate relevant metrics.

3. Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).

   The subcategories can be rather vague in their meaning. When reviewing with our support teams we learned that certain subcats may have different meanings and the degree of detail to document controls would be difficult to identify.
   i.e.: PR.AC-2: Physical access to assets is managed and protected – Discussing with different support teams the term "physical access" had different meanings based on the type of assets we were discussing (on-prem vs distributed vs remote).
   PR.AT: Awareness and Training - To what degree of "informed & trained" is implied? No real definable control other than users (new hires, existing employees, consultants) are required to take security awareness education upon hire and annually. And it was difficult to explain and identify controls for subcats that required personnel (3rd party, senior executives, and physical/cybersecurity) to "understand their responsibilities".

   Mike P. Organizations tend to respond to requirements much more than recommendations. Currently, unlike 800-171 requirements for organizations conducting business with the US Government, CSF is more viewed as a 'best practice' oriented document. Best practice often does not rise to the level of funding allocation (e.g. cybersecurity controls funding) in many businesses at a basic wants vs. needs perspective.

4. Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.

   If the intent of the Framework is to be broad in its coverage, then do not add other frameworks or references. Rather, expand mapping related categories/sub-categories to pertinent documentation.

   The Framework can be improved by adding more specifics for areas that do not have formal frameworks defined (such as 800-53, 800-171/172, NIST Privacy). Possible considerations: Zero Trust Architecture may have their own Cats/Sub-cats in each of the Functions; expand supply chain into other Functions other than just Identify.

5. Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.

   Insofar as CSF's general alignment with 800-series frameworks, changes to the CSF functions, categories, subcategories, etc., should either maintain or enhance that alignment rather than distance alignment.

6. Additional ways in which NIST could improve the Cybersecurity Framework or make it more useful.

   Annual workshops to determine continued applicability.

   CSF's current model of Category, Subcategory, Informative References could be supplemented with a guidance and/or testing procedures column. The Informative References are useful such that they point to other frameworks and documents from which a reader can infer the intent of a CSF category/subcategory, it would be much nicer to read a testing procedures column to better contextualize the intent of a requirement.

Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

7. Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework. These resources include:
    - Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).
    - Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.
    - Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.

    See Responses 1-6

8. Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources?

    Other frameworks that seek a common language provide commonalities with NIST CSF (and 800/171 also). For example, CSA's Cloud Control Matrix organizes their documentation as Control Domains and Control Titles like CSF's Category and Subcategory. Both frameworks provide descriptions of each element to where the reader determines applicability in their environment. I completed an exercise that mapped CSA CCM controls to NIST 800/171 subcategories. As we continue to migrate more applications & systems into the Cloud environment, it will become more imperative for us to know how our cybersecurity controls map between on-prem and Cloud environments using both NIST and CSA (or other frameworks that use a common language).

    Update the Derived Relationship Mapping tool to include non-NIST frameworks as Focal and Informative Reference documents.

    No obvious conflicts are apparent. Commonalities are well mapped in the Informative References section for NIST and non-NIST approaches.

    Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies?

    No obvious conflicts are apparent. Commonalities are well mapped in the Informative References section. Commonalities are much more relevant to companies that conduct business with the US Government. Companies that are not Federal Contractors are not required nor incentivized to meet government agency mandates and resources.

Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000- series, including ISO/IEC TS 27110?

Talk to each other, conduct collaborative workgroups to identify actual and potential synergies. Work with other framework standards organizations to collectively establish and align marketing implementation efforts across organizations. Identify common compliance tiers across standards organizations (e.g., Companies that conduct business internationally, companies that conduct business with the US Government, companies that align in critical infrastructure towers).

Update the Derived Relationship Mapping tool to include non-NIST frameworks as Focal and Informative Reference documents.

9. There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?

   Provide incentives for companies who's cybersecurity programs and initiatives align with international standards organizations in the form of reduced tariffs, reduced cyber insurance premiums (due to the reduced risk of a compliant business), reduced compliance assessments (e.g, if company 'a' becomes certified through an internationally adopted cybersecurity framework, that certification carries through other multiple parallel but disparate assessment and compliance documents)., etc.

10. References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800–53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.

    No comment to provide

Cybersecurity Supply Chain Risk Management:

11. National Initiative for improving Cybersecurity in Supply Chains (NIICS).
What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address?

The supply chain is a large surface area attack vector. Often from manufacturer to distributor to end consumer, supply chains often contain disparate elements that all require protection in order to protect the supply chain overall. From component producers through assembly and warehousing, multiple individual points of contact can cause disruption. Distribution often occurs via multiple land, air and sea vectors. End point consumers often do not have security protections available that may be present in a small business to enterprise like environment. The vastness of 'supply chain' provides multiple opportunities for cover and concealment that threat actors are able to exploit.

How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?

From a software security perspective, continue and double down on securing from the ground up. Secure coding practices are essential under consideration that end user consumers are still primarily focused on convenience over security. The greater the emphasis on software enhancements focused primarily on functional convenience typically open additional vectors for attack. We must get away from the archaic concept of passwords as a security control. Multi-Function Authentication should be elevated to a higher level of focus as it relates to software security. Multi-Factor authentication should be implemented in a default on – opt out scenario rather than a "Do you want to use MFA" opt-in scenario. Secure communication channels must become the default vs an optional after-thought in protecting data exchange within and between software applications.

12. Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g. pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.

No comment to provide

13. Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT?

No comment to provide

In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software?

No comment to provide

Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?

No comment to provide

14. Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.

    No comment to provide