February 23, 2016

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899

Re: Response to "Views on the Framework for Improving Critical Infrastructure Cybersecurity"

Dear Ms. Honeycutt,

Merck encourages the continued success of the NIST Cybersecurity Framework by providing the RFI response below. If you need additional information or clarification on this response, please do not hesitate to contact me directly.

Sincerely,

Terry Rice
VP, IT Risk Management & CISO
Merck & Co., Inc.

Use of the Framework

1. Describe your organization and its interest in the Framework.

Merck discovers, develops, and provides innovative products and services that save and improve lives around the world. Through our prescription medicines, vaccines, biologic therapies, and consumer care and animal health products, we work with customers and operate in more than 140 countries. Cybersecurity standards and frameworks are essential components of our information risk management strategy to ensure the quality and integrity of our clinical, laboratory, manufacturing, and supply chain processes. These processes deliver critical medicines to patients and the nation's workforce across all sectors.

Merck has adopted the NIST Cybersecurity Framework as our primary security framework. We have assessed our current state relative to the Framework, determined our desired future state, and begun execution of a 5 year program to improve our cybersecurity maturity across all Framework functions.

2. Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.

Merck is a Framework user and represents only Merck in this RFI response.

3. If your organization uses the Framework, how do you use it? (*e.g.,* internal management and communications, vendor management, C-suite communication).

In addition to maturing our cybersecurity capabilities, Merck uses the Framework in several ways:

- The Framework is used as an underlying reference to describe cybersecurity activities to all levels of management.
- Our internal IT security platforms are aligned to the Framework functions.
- Projects in our annual portfolio are mapped to NIST CSF functions and categories.

4. What has been your organization's experience utilizing specific portions of the Framework (*e.g.,* Core, Profile, Implementation Tiers, Privacy Methodology)?

We experienced a fairly straight forward mapping into the core, profile and implementation tier. It is challenging when attempting to map common program investments that span tiers. We leverage SDLC as a core element of our IT development and life cycle processes including cybersecurity. The NIST CSF aligns with SDLC to ensure quality from initiate, through development, and into operations to retirement. The security controls required in our SDLC map to multiple CSF areas to demonstrate the required controls/ capabilities are included during the development and deployment of systems. To measure cybersecurity coverage and maturity we mapped the implementation tier methodology to specific control sets and metrics.

5. What portions of the Framework are most useful?

The most useful feature is the ability to map from high level functions through categories and sub-categories into external reference standards. This complete mapping allows the definition of controls relevant for our organization and enables the definition of metrics to demonstrate improvement in our maturity profile.

6. What portions of the Framework are least useful?

The measures were useful but we need additional guidance on what should be considered per sector, i.e. Finance vs. Healthcare vs. Utilities, etc. with objective measures.

7. Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (*e.g.,* sector circumstance, organizational factors, Framework features, lack of awareness)?

Merck has found it challenging to define specific and objective measures that confirm a level of maturity relative to the Framework. The lack of reference points for these measures has slowed adoption.

8. To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.

Merck had previously aligned to the ISO27001/2 standards for information security. The adoption of the NIST CSF by itself did not reduce our risk. Measuring ourselves against the Framework and executing projects to address gaps increases our level of cybersecurity maturity resulting in measurable risk reduction.

9. What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the CyberSecurity Enhancement Act of 2014?

All new and updated regulations, standards, and guidance that contain cybersecurity requirements should link back to NIST function, category, and subcategory. This will reduce overlapping cybersecurity requirements and redundant control implementation.

Possible Framework Updates

10. Should the Framework be updated? Why or why not?

Yes, the Framework should be extended with free, public implementation guidance that is sector-specific. This guidance should not require additional cost such as the licensing of proprietary implementation approaches. There are also large gaps in how to address immature areas such as medical devices and industrial control environments where security improvements are required but the ability to achieve them is elusive in the near term. We recommend specific thought be given to how the framework can be used to balance new technologies which bring unknown risks but low adoption presents the risk of lost business opportunity to companies.

11. What portions of the Framework (if any) should be changed or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

Perhaps not the Framework itself, but NIST-sponsored guidance on the use of the Framework would be helpful. For example guidance to regulators on a common way to map regulatory requirements into the Framework would reduce confusion for entities subject to multiple regulatory bodies. Those entities would have better assurance that a common set of controls can satisfy multiple regulatory requirements. It would also be useful for NIST to provide a standard approach for mapping technology solutions into the sub-categories. This is often confusing with solutions meeting multiple objectives and significant overlapping capabilities across solutions. Customers could demand that vendors use the NIST-provided approach to reduce misunderstanding and demonstrate where specific product features apply to the Framework.

12. Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?

Merck recommends the addition of references for medical device submission (pre/post market).

13. Are there approaches undertaken by organizations—including those documented in sector-wide implementation guides—that could help other sectors or organizations if they were incorporated into the Framework?

Sector coordinating councils in concert with NIST should develop free and publicly available implementation guidelines specific to their sector.

14. Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?

Yes, free and publicly available conformity assessment criteria and expectations should be made available within each sector.

15. What is the best way to update the Framework while minimizing disruption for those currently using the Framework?

Map the alignment between the current and proposed Framework. Identify the gaps or improvements and suggest methods to make the transition. Provide a reasonable time to transition before the old Framework will be retired and no longer supported or accepted.

Sharing Information on Using the Framework

16. Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?

The public workshops used to create the NIST CSF were a great resource to build awareness and understanding of the Framework. NIST should continue to host quarterly or semi-annual workshops on Framework changes and implementation.

17. What, if anything, is inhibiting the sharing of best practices?

Merck is aware of concerns over sharing specific vulnerabilities and gaps that could become public and leveraged by adversaries. There are also emerging concerns that known gaps, if exposed, could be used in litigation should a compromise/breach occur.

18. What steps could the U.S. government take to increase sharing of best practices?

The U.S. government should focus on incentives to increase the adoption of the Framework and sharing of best practices. An example would be the development of sector-specific conformity assessments which would result in reduced liability for conforming entities.

19. What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (*e.g.,* peer-recognition, trade association, consortia, federal agency)?

A program for independent, objective attestation of Framework conformity would limit organizational liability and increase information sharing.

Private Sector Involvement in the Future Governance of the Framework

20. What should be the private sector's involvement in the future governance of the Framework?

The private sector should be involved in semi-annual workshops to update the Framework and improve implementation guidance.

21. Should NIST consider transitioning some or even all of the Framework's coordination to another organization?

No. NIST has the experience, expertise and independence through its history of developing standards/frameworks that will ensure a well-balanced CSF that is widely accepted. However, to gain international acceptance, NIST should consider partnering with an international body which would benefit US-based global organizations.

22. If so, what might be transitioned (*e.g.,* all, Core, Profile, Implementation Tiers, Informative References, methodologies)?

N/A

Ownership/Governance

23. If so, to what kind of organization (*e.g.,* not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?

NIST could rely more heavily on sector coordinating councils for future governance.

24. How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?

If industry does not feel comfortable with the transition, less collaboration will occur and a shift to another framework could emerge. Any party that governs and owns the Framework must be a trusted, neutral entity.

25. What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?

A transition partner should have demonstrated ability and acceptance by the global community without incentive to profit from the CSF.