From: Landfield, Kent <Kent_Landfield@McAfee.com>
Sent: Thursday, October 24, 2019 4:47 PM
To: privacyframework <privacyframework@nist.gov>
Subject: McAfee Privacy Framework Preliminary Draft Comment Submission

Hello,

Enclosed are McAfee's comments in response to the National Institute of Standards and Technology's Request for Comments on the NIST Privacy Framework Preliminary Draft dated September 6, 2019.

NIST is playing an important role in the efforts to improve privacy. McAfee would like to sincerely thank NIST for the opportunity to contribute our thoughts, and we look forward to continued engagement with NIST on this and other topics.

Thank you, Gracias, Grazie, 谢谢, Merci!, Спасибо!, Bedankt,Danke!, ありがとう, ϶ !

--

Kent Landfield

+1.817.637.8026

kent_landfield@mcafee.com

October 24, 2019

VIA EMAIL: privacyframework@nist.gov

Attn: Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: McAfee's comments in response to NIST's Request for Comments on the "Preliminary Draft of the NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management"

McAfee LLC appreciates the opportunity to respond to the National Institute of Standards and Technology's Request for Comments on the NIST Privacy Framework Preliminary Draft dated September 6, 2019.

McAfee, a world leading independent cybersecurity company, is focused on accelerating ubiquitous protection against security risks for consumers, businesses and governments worldwide. Inspired by the power of working together, McAfee creates cybersecurity solutions that make the world a safer place. For consumers, we help secure their digital lifestyle at home and away. For businesses, McAfee cloud security extends from device to cloud with data visibility, data loss prevention and advanced threat protection on a platform that supports an open ecosystem. Our holistic, automated, open security platform allows disparate products to co-exist, communicate and share threat intelligence with each other across the digital landscape. We enable the convergence of machine automation with human intelligence so our customers can streamline workflows more efficiently, be freed from operational burdens and be empowered to strategically combat threats from adversaries.

McAfee agrees with the approach and goals NIST has taken in developing the Privacy Framework. The voluntary Privacy Framework focuses on helping organizations properly address their privacy needs and risks through the use of privacy best practices. As a tool, it will help organizations understand how to improve their privacy programs, while being compatible with and supporting an organization's ability to operate under the various legal or regulatory regimes. We believe this is a significant step forward in positioning organizations to better address current and future data protection and privacy needs. We are highly supportive of NIST's efforts to develop this risk-based, outcome-based, voluntary and non-prescriptive Privacy Framework, and we welcome the opportunity to add our comments to those of other stakeholders and champions.

Individuals and corporations must be able to trust technology for it to be the most effective. We believe that trust in the integrity of systems – whether a corporate firewall or a child's cell phone – is essential to allowing individuals and corporations to benefit most from the power of technology. McAfee is committed to enabling the protection of customer, consumer and employee data by providing robust security solutions.

Our response includes answers to the specific document concerns we have, as well as general comments and suggestions on aspects of the proposed Privacy Framework.

Before beginning our comments, we want to express how pleased we are to see NIST leveraging its abilities as a successful convener of industry, academia and governments to solve a problem whose solution is long overdue. Thank you.

Document Comments

Executive Summary:

The statement on line 88:

"*The Privacy Framework can drive better privacy engineering and help organizations protect individuals' privacy by:"* This sentence does not seem like the most important thing to put up front as the value of the Privacy Framework. The term 'privacy engineering' is not going to be familiar to many and should be described further to avoid ambiguity. We recommend focusing on Privacy Risk Management and improving organizational privacy programs, processes and communications instead. This would set up the topics for further explanation in subsequent paragraphs..

The paragraph starting on line 100:

"The Privacy Framework – through a risk- and outcome-based approach – is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and enterprises, and stay current *with technology trends, including artificial intelligence and the Internet of Things.*"

The following is a bit more understandable. "The Privacy Framework – through a risk- and outcome-based approach – is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and enterprises, and stay current *with the privacy impacts of emerging technologies such as artificial intelligence and the Internet of Things.*"

1.0 Privacy Framework Introduction:

The paragraph starting on line 137:

"The National Institute of Standards and Technology (NIST) has developed this voluntary NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework) to help organizations manage privacy risks by:"

While NIST is developing the Privacy Framework, it is important to assure that the community aspects of the development and creation are included since the private and public sectors, as well as members of academia actively participated in the development and were a critical aspect of the Framework's development. Appearing as if NIST developed the Framework on its own will not go over well internationally. Its development should be described as a public-private partnership in the same manner

as the Cybersecurity Framework. This preliminary draft is the result of work done in three public workshops, well attended by industry, academia and the privacy community.

The bulleted list starting on line 140 should be reordered:

The impression given by the list ordering is that privacy engineering seems to take precedence over active integration of privacy best practices into existing organizational practices. The list should be reordered to assure the business focuses are always stated first. The second bullet and the first bullets should be swapped. While minor, where possible, we want to focus the reader on the organizational improvements first.

1.2.1 Cybersecurity and Privacy Risk Management:

The statement starting on line 211:

Figure 2 *illustrates how NIST considers the overlap and differences between cybersecurity and privacy risks.*

The extensive use of "NIST this" and "NIST that" makes the wrong impression on the reader. This diagram was discussed at the Boise Workshop and it seemed to have agreement across the board. There is concern this is beginning to look too much like a U.S. government document and not a document that is meant to have an international impact. It is understandable that there are places where it is important to call out NIST, but where it can be reworded or removed, it should be. This statement could be rewritten as:

Figure 2 *illustrates the overlap and differences between cybersecurity and privacy risks*

Additionally, on line 215, the statement "*The NIST approach to privacy risk is to consider…"*

Could be rewritten as "*The Framework's approach to privacy risk is to consider…"*

It is vitally important to global acceptance that this Privacy Framework does not look as if NIST is telling people what is best for them. This framework was developed as a public-private partnership with international participation. As such, where we can use "Framework" instead of NIST, please do.

2.2 Profiles

Figure 5: Profile Development Process:

It is unclear looking at Figure 5 just what it is depicting. For those familiar with the Cybersecurity Framework, this basically shows that an organization can pick and choose those entries they need/want in any specific profile they may be developing. The diagram also seems to indicate organizations should use the assessed Current Profile to develop the Target Profile from. This is backwards in that usually there needs to be some baseline definition agreed to by management as to what should be assessed. Labeling this as the Profile Development Process is confusing. Some additional language might help in explaining the diagram fully.

The discussions of Profiles and Tiers:

There needs to be a better explanation as to what a Target Profile is. It is the embodiment of what the organization has decided is the level of privacy risk the organization is willing to accept. With some subcategories, an organization is willing to accept a Tier 2; in others they may need to achieve a Tier 3 level. Tiers are not a maturity level. When used in a Target Profile, they are an indicator of the level an organization wishes to achieve on that specific subcategory, in keeping with the privacy risk the organization has agreed to. In a Current Profile, Tiers are used as an indicator of the 'as-is' assessed state of the organization for that specific evaluated subcategory.

The discussion in section 2.2 and 2.3 should be expanded to address the fact that Tiers are used both for having a discussion around the acceptable level of privacy risk and reporting where the organization stands.

3.1 Mapping to Informative References

As currently noted in the Framework, the only real informative references are NIST references. An active effort needs to be made to solicit mapping of international standards and professional privacy organizations such as the IAPP and others to the individual subcategories. It is important that current privacy best practices be mapped to assure those wanting to use the Privacy Framework can get the needed background to properly understand and address the identified subcategories.

3.3 Establishing or Improving a Privacy Program

Set discussion starting on line 494:

"*Informed by its privacy risk assessment, the organization creates its Target Profile focused on the assessment of the Categories and Subcategories describing the organization's desired privacy outcomes*."

This is not the experience or approach we took while using the Cybersecurity Framework. We do not believe an organization should develop a Privacy Target Profile after seeing how bad or good their assessment results are. This is not a proper approach to developing a Target Profile. We believe the Target Profile should be constructed independently, with active discussions with senior and executive management to determine what the organization views as an acceptable level of risk for each of the individual subcategories. This forces the organization to take the time and have the hard discussions needed to truly understand their privacy risk and exposures. The Functions, Categories and Subcategories selected for the Target Profile, then form the basis for the Current Profile from which an assessment takes place. If created as described in the Preliminary Framework, there is too much opportunity for organizations to take shortcuts and not really address what the true privacy risk management concerns are for the organization and its mission.

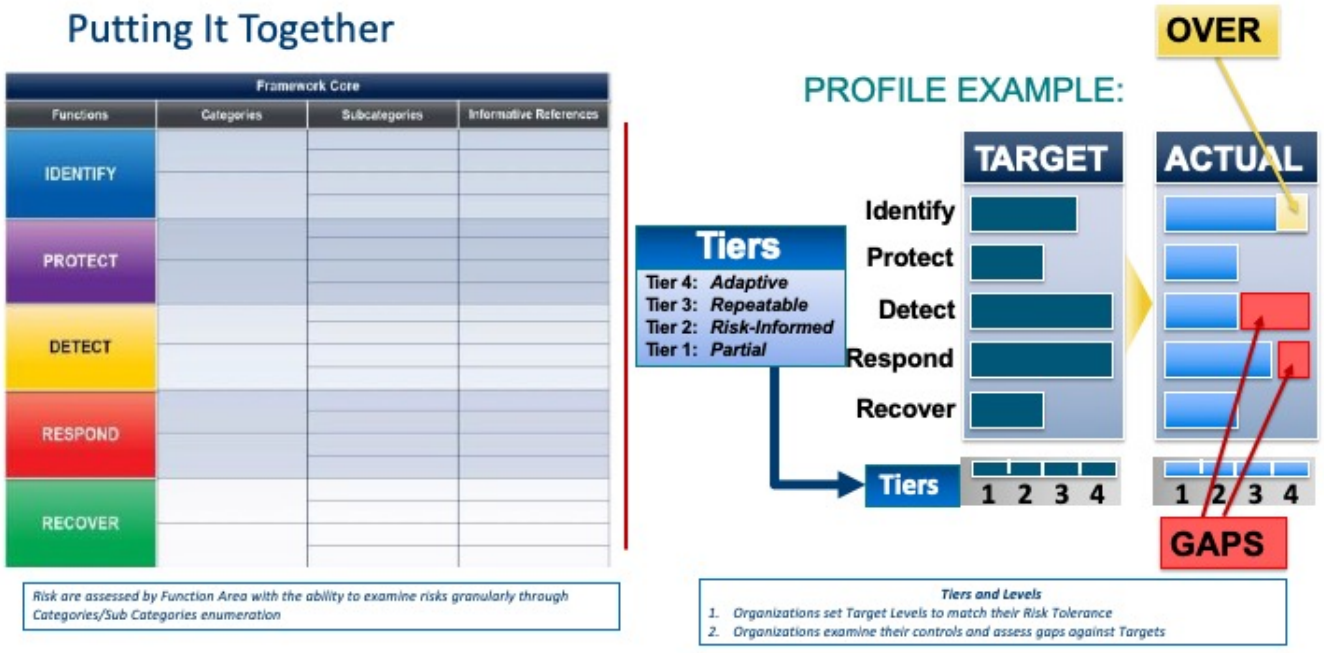
We believe no assessor should know what Target the organization is trying to achieve until after the unbiased assessment of the current state of the organization's privacy risk posture for each of the assessed subcategories. By so doing, the results will not be tainted and will be more accurate and valuable to the organization's future privacy practices and processes. This allows the organization to

create a better roadmap for future improvements while they journey to reach the levels that senior management desires for the organization. We recommend that NIST review what is written in this "Set" section and describe a process that has more integrity to the process.

Additional Considerations

Needed Graphic Representation

It would be helpful if there were a graphic that described the overall process at a high level. An example would be similar to what was often seen in Cybersecurity Framework presentations.



This is **simply an example** that needs modification to support the Privacy Framework Functions, but it could be useful in assisting with understanding the overall process.

Develop Mapping to Privacy Regimes

It was obvious at the Atlanta Workshop that there was a real need to create a mapping to the existing legal regimes that the Privacy Framework needs to be able to support. How that is to be supported is really a mapping exercise to regimes such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other appropriate international privacy regimes. It would be useful if the Privacy Framework were shown to be directly applicable. A mapping such as this would go a long way toward convincing organizations there is a better way to prepare for emerging legal privacy requirements. This is envisioned as a separate document/spreadsheet available from the NIST Privacy Framework Resource Center.

Roadmap Independence

Currently, Appendix F in the preliminary draft is slated for the Roadmap. As with the Cybersecurity Framework, the Roadmap should exist as a separate and distinct file from the actual Privacy Framework and should not be included. As with the Informative References, including it would cause the Roadmap to be too static and not the independent, living document it needs to be.

Summary

Effective consumer privacy policies and regulations are critical to the continued growth of the U.S. economy, the internet and the many innovative and life-improving technologies that rely on consumer personal data. The development of a comprehensive Privacy Framework is an important step toward increasing consumer privacy and trust and will assist in aligning thought and potentially legislation globally. We are pleased the Privacy Framework is focused on developing the means for assisting an organization to create a tool for standing up, improving, evaluating and adapting to the evolving privacy landscape.

NIST is playing an important role in the efforts to improve privacy. McAfee would like to sincerely thank NIST for the opportunity to contribute to this issue, and we look forward to continued engagement on this and other topics.