ITI Promoting Innovation Worldwide

April 29, 2022

Via email to: AIframework@NIST.gov

RE: ITI Response to National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework: Initial Draft

The Information Technology Industry Council (ITI) appreciates the opportunity to continue its engagement with the National Institute of Standards and Technology as it seeks to develop an *Artificial Intelligence Risk Management Framework.* As such, we are pleased to provide comments on the *AI Risk Management Framework: Initial Draft*.

ITI represents the world's leading information and communications technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises leading innovative companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, and other internet and technology-enabled companies that rely on ICT to evolve their businesses. Artificial Intelligence (AI) is a priority technology area for many of our members, who develop and use AI systems to improve technology, facilitate business, and solve problems big and small.

ITI is actively engaged on AI policy around the world. We issued a set of *Global AI Policy Recommendations* in 2021, aimed at helping governments facilitate an environment that supports AI while simultaneously recognizing that there are challenges that need to be addressed as the uptake of AI grows around the world.[1] We have also actively worked to inform NIST's efforts to foster trust in AI technology, including responding to NIST's RFI on an AI Risk Management Framework[2] and the RFI on the AI RMF Concept Paper.[3]

ITI and our members share the firm belief that building trust in the era of digital transformation is essential and agree there are important questions to address regarding the responsible development and use of AI technology. As this technology evolves, we take seriously our responsibility as enablers of a world with AI, including seeking solutions to address potential negative externalities and helping to train the workforce of the future. To be sure, our

[1] Our complete *Global AI Policy Recommendations* are available here: https://www.itic.org/documents/artificial-intelligence/ITI_GlobalAIPrinciples_032321_v3.pdf

[2] See ITI response to RFI on AI RMF here: https://www.itic.org/documents/artificial-intelligence/NISTRFIonAIRMFITICommentsFINAL.pdf

[3] See ITI response to RFI on AI RMF Concept Paper here: ITI Comments on AI RMF Concept Paper FINAL.pdf

members are aware of and are taking steps to understand, identify and treat the potential for negative outcomes while leveraging opportunities that may be associated with the use of AI systems. As such, we appreciate that NIST is working to establish an AI Risk Management Framework (RMF) and that we can provide input to the Initial Draft of this framework.

Below, we highlight some overarching recommendations that we believe will be helpful in strengthening the AI RMF. Following that, we provide feedback on the questions NIST poses in the Initial Draft.

Overarching Recommendations

At the outset, we would like to thank NIST for considering our previous feedback to the Concept Paper. We also provide additional general comments for NIST to consider as it further builds out the AI RMF, in some instances reiterating our previous recommendations, which we continue to believe will strengthen the ultimate RMF.

NIST should seek to maintain coherence with prior works, clearly establishing a linkage between the AI Risk Management Framework and the Cybersecurity and Privacy Frameworks. We appreciate NIST acknowledging that the RMF aims to fill the gaps related specifically to AI as any software or information-based system includes risks related to cybersecurity, privacy, safety, and infrastructure. However, it would be helpful for NIST to articulate more clearly what the overlap or interplay between the AI RMF and Cybersecurity and Privacy Frameworks looks like. This could appear in the form of a Venn diagram, such as included in the Privacy Framework, demonstrating the overlap between the three Frameworks, or as a more detailed crosswalk akin to the one between the Privacy and Cyber Frameworks, where the AI Risk Management, Privacy, and Cyber Frameworks are mapped to each other.

NIST should seek to leverage and align the RMF with published standards or those currently under development in international standards bodies. In the Initial Draft, NIST has recognized that certain risks can be positive, which is in alignment with Guide 73:2009; IEC/ISO 31010. However, we would like to reiterate that NIST should seek to align the RMF with other standards and frameworks, such as the ISO/IEC DIS 23894 – Information technology — Artificial intelligence — Risk management and ISO/IEC CD 5338 — Information Technology — Artificial Intelligence — AI system life cycle processes, which are currently under development.

NIST should seek to maintain and foster consistency internationally to the extent possible. As we have noted in our earlier submission to NIST on the AI RMF, international consistency is essential, particularly as countries around the world are beginning to consider how to address risks and harness benefits that may stem from the use of AI.

In considering risks, NIST should clarify how risks differ for human facing and non-human facing AI systems, as well as appropriate risk evaluation criteria. We suggested this in response to the initial Concept Paper and continue to believe this is imperative for the Framework to address moving forward. While some AI applications are human facing (e.g., face recognition systems, recommender systems, or hiring systems) many AI applications are not (e.g., analysis of weather information, defects on the factory floor, bottlenecks in networks, or state of the roads). AI systems that are not human facing typically do not have PII (Personally identifiable information) in the data sets and frequently feed analytics to other machines, not human end users. As a result, human facing and non-human facing AI system have distinct types of risks associated with them. For example, considering privacy risks is essential for human facing systems. But privacy risks are not present in weather sensor data analysis fed to another system that uses the analytics to assess climate patterns over a longer period of time. Applying the same risk management requirements to both types of AI systems would not allow the technologists and evaluators to assess the risks for the AI systems in an actionable fashion and would also be onerous to organizations – disproportionately hindering innovation.

NIST should add a function that accounts for contingencies. We continue to believe that adding a separate "Respond" function to account for contingencies would be helpful. Although NIST briefly references "incident response" in the context of the proposed Manage function and as a subcategory in the Governance function, we continue to believe that a separate function that maps practices that organizations might undertake to respond to an AI-related incident would be useful. While we understand the intent of the Manage function is likely to capture activities such as response and contingencies, in the AI context it may be appropriate to include both Respond and Govern functions. Furthermore, it might also be useful to create a database with best practices gathered from the results of such a Respond function so that organizations can leverage such data to anticipate new incidents and deploy mechanisms (some of which may be automated, i.e., MLOps) to consistently check for risk factors. This may also help to encourage stakeholder alignment. Furthermore, it is also worth noting that the OECD is planning to also develop a common framework for reporting on AI incidents, and a Respond function would help feed into and help align with that process.[4] The current incident database curated by the Partnership on AI may also yield useful insights.[5]

Specific Responses to Questions Posed in the Concept Paper

Below, we also offer discrete thoughts on the questions that NIST poses in the Initial Draft

1. *Whether the AI RMF appropriately covers and addresses AI risks, including the right level of specificity for various use cases.*

As a general matter, we appreciate that NIST has widened the meaning of risk to include positive occurrences and acknowledged that such occurrences can result in opportunities. While we recognize that NIST's definition of "risk" is aligned with NIST SP 800-160 vol. 1, which notes that risk outcomes can be positive (and can in some cases can provide an opportunity) and with the International Organization for Standardization (Guide 73:2009; IEC/ISO 31010), we encourage NIST to make clear in conversations with international stakeholders that that is how

[4] See more information on the OECD Risk Classification Framework here: https://oecd.ai/en/wonk/classification

[5] See more information here: https://partnershiponai.org/workstream/ai-incidents-database/

positive risk should be interpreted. Oftentimes, risk is only associated with the likelihood of a negative outcome. Alternatively, NIST could consider using the word “opportunity” in the Framework itself. We also encourage NIST to further differentiate between “risk” and “impact,” as the RMF confuses the two terms at times. If NIST decides to use both terms in the document, it should either clearly define both terms up front, or clarify that they are used interchangeably throughout the document, or both.

We do however have questions related to Section 5: AI Risks and Trustworthiness and the structure that NIST uses to classify different characteristics. Likely every aspect (or almost every aspect) of an AI system has a socio-technical component because of the way that AI interacts with society, so it seems unhelpful to break out the characteristics into two other categories, without referencing this potential overlap. For example, the characteristics that constitute “Guiding Principles” bridge across several socio-technical components, which should not be overlooked. Mapping the overlap between the guiding principles and other characteristics could be helpful and provide a more accurate representation. Beyond that, it is somewhat unclear how this taxonomy is leveraged in the AI RMF itself, as it is not into the Framework in a meaningful way, aside from a brief mention that organizations should consider all three classes of characteristics in executing of the functions. Additionally, we were pleased to see that NIST incorporated considerations around adversarial influence as we had recommended in our submission to the Concept Paper but encourage NIST to add content to Section 5.1.4 Resilience or ML Security to further reflect the breadth of considerations necessary to sufficiently map security risks in AI/ML systems. It may be helpful to leverage the MITRE ATLAS Matrix, or at least reference it as a starting point, as it provides a solid overview of the myriad of security/resiliency risks that may be useful for organizations to consider in identifying their risk profile.[6]

As currently drafted, we also do not believe that the Framework appropriately captures AI risks. Indeed, the nature and severity of risks can dramatically vary based on whether a system is human-facing or non-human facing, but the Framework lack any clear distinction between the two. As such, we encourage NIST to include a discussion around the distinction between human and non-human facing AI systems, whether an AI system can impact a person’s safety and fundamental human rights, and how that determination might feed into an organization’s overarching risk assessment process.

In the Map phase, NIST addresses the need for organizations to understand the intended purpose of the system, the setting in which the system is to be deployed, and the specific tasks supported; however more time could be spent addressing the need to understand the potential *unintended* uses of the system. How could the system be used inappropriately and/or *outside* of the bounds of its currently scoped intended purpose? If the system is in place, what else could be done with it outside of the current scope? In later phases of the AI RMF, more time could be spent addressing how likely such scenarios would be, and ways to mitigate these unintended uses of the system.

[6] See MITRE ATLAS Matrix here: https://atlas.mitre.org/

Additionally, it would be helpful to clarify the distinction between fairness and the absence of harmful bias. Section 5.3.1 notes that "(f)airness is increasingly related to the existence of a harmful system, i.e., even if demographic parity and other fairness measures are satisfied, sometimes the harm of a system is in its existence." The section then goes on to state that "[w]hile there are many technical definitions for fairness, determinations of fairness are not generally just a technical exercise." The statement is quite broad, implying an expectation to do more than mitigate harmful bias, yet fails to elaborate on what else this should encompass.

Finally, we do not believe that the Framework is currently specific enough to enable effective implementation. The Practice Guide will be imperative to making the Framework functional and implementable. We offer additional thoughts on this in response to Question 8.

2. *Whether the AI RMF is flexible enough to serve as a continuing resource considering evolving technology and standards landscape.*

We believe that the AI RMF is flexible enough to serve as a continuing resource. We understand the Framework can be updated as things change and the landscape evolves, in the same way that the Cybersecurity Framework has undergone periodic updates. That being said, it is also important to develop the Practice Guides in a similarly flexible way because AI is such a nascent technology and standards and best practices to address many of the subcategories are still under development. Indeed, it may be that there are no existing standards to address some of the subcategories, and NIST should reflect that in the Practice Guide/companion document. Furthermore, NIST should construct the Practice Guide/companion in such a way that it is simple for diverse stakeholders to use.

We also urge NIST to develop a similar online AI Informative Reference program for to the one that currently exists for Cybersecurity Informative References. The web-based nature of the Online Informative Reference (OLIR) Program makes it easy to update. New resources can be added as they become available, and the database is evergreen in a way that a published pdf document is not. Something similar would be immensely helpful for AI Informative References, recognizing how rapidly things will likely evolve in this space.

3. *Whether the AI RMF enables decisions about how an organization can increase understanding of, communication about, and efforts to manage AI risks.*

We believe that the Framework is fairly comprehensive, though as referenced above, the companion document will be imperative to facilitating its implementation. That said, we believe several areas of the document could be strengthened to foster additional understanding, which we outline in response to Question 7.

4. *Whether the functions, categories and subcategories are complete, appropriate, and clearly stated.*

As we referenced at the outset, it is our view that the Functions are incomplete and that they could better account for contingencies. In cybersecurity, for example, practitioners do their best to avoid, mitigate, share, transfer, and accept risks. However, organizations also establish incident response practices given the inevitability that incidents will occur. In the same way, organizations should also ensure they are adequately prepared to respond should they be unable to avoid, mitigate, transfer, or accept an AI-related risk. We reiterate our recommendation that NIST develop a Respond function, which would map to practices that organizations might undertake to respond to an AI-related incident. In so doing, as we mentioned above, it would be useful to also consider developing a database or other mechanism to log and/or share best practices across organizations, where applicable, as well as engage with the OECD as it embarks on its effort to develop a common framework to report on AI-related incidents.

Furthermore, documentation (or even technical traceability) is missing from the draft's "technical characteristics" of trustworthy AI. NIST should include documentation as a standard along with accuracy, reliability, robustness, and resilience. If not documenting the thresholds for accuracy, reliability, robustness, and resilience, along with the intended uses and limitations of the AI, will create unnecessary risk.

We also note that one of the functions in the AI RMF focuses specifically on measurement. We appreciate that NIST has included Section 4.2 Challenges for AI Risk Management, and that it includes a discussion around challenges in measuring AI risk. Beyond the fact that some AI risks may not be well-defined or well-understood, or that opaqueness of an AI system may contribute to measurement challenges, we also think it is worth adding content that further emphasizes the fact that risks might only be able to be described in a qualitative or semi-quantitative manner due to the current lack of measurements or lack of robust and verifiable measurement methods.

In developing qualitative and quantitative measurements and monitoring, it might be helpful for NIST to look to *ISO/IEC 31010 Risk management – Risk assessment techniques*. *Annexes A and B* in particular provide an exhaustive list and comparison of risk assessment methods, some of which could be leveraged or adapted. Both annexes also provide selection criteria and considerations. Leveraging such tools for AI would allow organizations to integrate AI risk management (both of organizations and of AI systems) directly into existing cultures and practices, if any; this would lessen the burden on functions such as engineering quality assurance or internal auditing, and limit overall cost while improving effectiveness.

AI is an emerging technology area, and standards, guidelines, and best practices are still under development. Because of this, we are also still learning about the range of potential risks, their likelihood, and how to measure them. Thus, we continue to believe that it would be helpful for NIST to indicate how the RMF might address a situation where such risks cannot be appropriately measured. We continue to encourage NIST, in developing the AI RMF, to specifically address situations where risk cannot be measured and offer guidance on reasonable steps for treating that risk, without limiting innovation and investments in new, and potentially beneficial, AI technologies. And importantly, NIST should note that the inability to measure AI risk does not imply that an AI system poses high or infinite risk. To put it another way, the absence of data should not be treated as justification for halting all use or development of a technology or use. In the same vein, not every measure of risk is meaningful. NIST should consider these inherent limitations in measuring risk which could lead to certain harms being overlooked.[7]

5. *Whether the AI RMF is in alignment with or leverages other frameworks and standards such as those developed or being developed by IEEE or ISO/IEC SC42.*

As we mentioned in our overarching recommendations section, NIST should seek to further align with international standards to encourage consistency in the way organizations are implementing risk management processes. We particularly encourage NIST to utilize ISO/IEC DIS 23894 AI Risk Management, and it would be helpful for NIST to reference this standard in the body of the AI RMF itself, in addition to including it as an informative reference in the forthcoming Practice Guide.

We also encourage NIST to seek to further align with ISO/IEC 5338 – Information technology – Artificial intelligence – AI system life cycle processes ISO/IEC DIS 38507 Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations and ISO/IEC DIS 23894 Table C.1 Risk Management and AI System Lifecycle. As we mentioned in our prior response to the Concept Paper, it would be helpful for NIST to further illustrate the stages following deployment, including the post-market stages, which may engender certain risks across a longer period of time, and the retirement phase, which marks the end of the lifecycle and may also have a different set of risks associated with it. Indeed, risk management does not cease with the deployment of an AI system. NIST should take interdependencies between risks and residual risks into consideration to an appropriate degree.

NIST should also seek to align the terminology used in the AI RMF with the terminology specified in ISO 31000:2018, IEC/ISO 31010:2009, ISO/IEC DIS 23894 (Clauses 6 to 6.7) and ISO/IEC 22989. Alternatively, NIST could map the RMF terminology with these international standards. By doing so, NIST could serve as an example for other regional efforts, demonstrating the importance of alignment with international standards. Additionally, a misalignment in terminology, nomenclature, processes, and methods with those used in international standards will make it difficult for both industry and government to understand and apply the AI RMF. By mapping and seeking to reconcile terminology, guidelines, and requirements across multiple jurisdictions, NIST can help to prevent duplication of efforts, prevent different interpretations of key terms and requirements, and help to facilitate seamless

[7] See Fazelpour and Lipton's "Algorithmic Fairness from a Non-Ideal Perspective" (https://arxiv.org/abs/2001.09773).

integration into existing organizational risk governance (e.g., Safety, Security, Quality, Environmental, Ethical risk management systems).

For example, “Map -> Measure -> Manage” does not seem to align with the ISO/IEC terminology, though it covers some of the same elements:

- “Map” is covered by ISO/IEC 23894 under *6.2 “Communication and consultation”* + *6.3 “Scope, context and criteria.”*
- “Measure” is referred to in ISO/IEC 23894 as the iterative *6.4 “Risk Assessment = Risk identification, risk analysis, risk evaluation”* cycle.
- “Manage” corresponds to Risk Treatment in ISO/IEC 23894 and ISO 31000.
- ISO/IEC 23894/ISO 31000 include a response function as part of “implementing risk treatment plans”, inclusive of verification of effectiveness.
- It is our view that elements of ISO/IEC 23894 such as “Monitor and Review” and “Recording and reporting” are not sufficiently emphasized throughout the risk management process set forward by the NIST AI RMF, so we would encourage additional alignment there.

NIST should also consider leveraging the definition of AI stakeholders described by *ISO/IEC 22989 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology 5.17 AI Stakeholders roles* defines AI provider, user, customer, partner, and subject roles. In addition, SC 42 work particularly considers the complexity of the AI value chain. AI RMF requirements might thus not apply uniformly across the value chain. Assignment of risk accountability and responsibilities, for example, should consider several factors, such as where the stakeholder is located in the value chain and the type of AI system (e.g., general purpose, custom- or special-purpose). The stakeholder roles could also be part of a single organization or broken down across multiple organizations. All these factors could impact implementation of the AI RMF.

Lastly, we encourage NIST to align with terminology in ISO/IEC 22989 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology around the AI lifecycle. In particular, we point NIST toward *ISO/IEC 22989 Figure 3 — Example of AI system life cycle model stages* and *Figure 4 — Example AI system life cycle model with AI system-specific processes*:

- NIST specifies the “pre-design” stage as “Inception” by ISO/IEC 22989, and the “Data collection” activity in the AI RMF is part of the ISO/IEC Design and development stage.
- Additionally, NIST uses the term “Deployment” to describe the entire stage after release of the AI system. On the other hand, ISO/IEC 22989 breaks the post-deployment lifecycle down into several stages: “Deployment” which is the initial release to operation; “Operation & monitoring” (which is the longest, sustaining stage); “Re-evaluation”; “retirement”. Each of these stages incur different risks, challenges, and opportunities.

- Finally, ISO /IEC 22989 uses the term “retirement”, where “decommissioning” is only one of several retirement options of the system.

NIST could also consider leveraging the *OECD Framework for the Classification of AI Systems*. It is a highly practical and instructional document. In particular, the OECD document provides a detailed matrix which matches contexts, technical and socio-technical characteristics/principles, and lifecycle sub-stages, which could be useful to informing the AI RMF.

6. *Whether the AI RMF is in alignment with existing practices and broader risk management practices.*

Some of the key modules of a risk management framework are not visible in the AI RMF. Firstly, as we further note below, the Respond function is not currently included in the AI RMF. This Function is critical, as it is not possible to control for all risks and vulnerabilities.
We also note that Record & Report is missing in this Framework – non-external reports should cover internal reporting and awareness. This may fit underneath the Manage function.

We also note that in many instances throughout the Framework, impact is defined as adverse. However, it is important to consider the fact that there may be impacts due to AI risk, which may not be adverse at the initial stages, but may require fixing to avoid having an adverse effect when merged with other security vulnerabilities

7. *What might be missing from the AI RMF*

Something we have advocated throughout NIST’s development of the AI RMF is establishing risk evaluation criteria to help guide organizations as they seek to establish risk thresholds and understand their risk tolerance/appetite. While we recognize this is a significant undertaking, we continue to believe that such a methodology would be helpful for organizations in determining the risk-level of a specific AI use case, informing the steps that they should take to mitigate or treat the risk. Such a methodology should also identify the appropriate roles for AI developers, deployers, users, and other stakeholders in making risk determinations. These determinations are also crucial for helping stakeholders identify specific technological mechanisms for measuring, mitigating, and controlling high-risk attributes of AI systems, where applicable. We are not saying that NIST should bucket specific uses of AI into a “high-risk” category, but instead that it should develop criteria that can help the relevant roles with responsibilities and authorities to figure out what level of a risk a particular use case may pose. Including illustrative examples may be helpful, with the clear caveat that the examples are just that, illustrative, and not meant as a categorical determination. If NIST deems it unfeasible to include evaluation criteria in the AI RMF itself, then we strongly encourage NIST to launch a process with the goal of working with stakeholders to develop such criteria.

As we mentioned in our introductory recommendations, we also think it would be useful for NIST to add additional discussion around the linkage between the Privacy and Cybersecurity Frameworks and the AI RMF. Both privacy and cybersecurity characteristics are discussed in the taxonomy NIST lays out in the AI RMF, but it is not clear how an organization might leverage the AI RMF in conjunction with the other NIST Frameworks, or if there are aspects of the AI RMF that map to either (or both) the Privacy and Cyber Frameworks. Section 1.2.1 of the Privacy Framework, for example, discusses the relationship between cybersecurity and risk management, and offers a helpful Venn diagram that very clearly illustrates where cyber and privacy risks overlap.[8] We strongly encourage NIST to add a similar section on cyber and privacy risk management and AI risk management so as to help organizations understand how these risks appear in the context of AI and how they might use other Frameworks to address these risks together with the AI RMF.

NIST should also consider the implications of including all AI systems within the AI RMF framework. Due to the ubiquitous use of AI systems across organizations, it would likely be burdensome to include all AI systems within the AI RMF. Ideally, organizations should have the ability to decide which of their systems is covered by the AI RMF. We recommend that NIST include this as a category or sub-category under the Governance Function.

We also think it would be useful for NIST to add to Section 1 Overview (lines 18-23), where NIST discusses federal and/or legislative initiatives that the AI RMF is consistent with and/or otherwise supporting, it would be useful to also explain how the AI RMF is also aligned with the principles laid out in OMB Memo M-21-06, *Guidance for Regulation of AI Applications.*

Finally, on p. 10, NIST notes that "organizations need to establish and maintain the appropriate accountability mechanisms, roles and responsibilities, culture, and incentive structures for risk management to be effective." Specifically, on creating incentive structures, we NIST can include more content about how to help people understand how they themselves are stakeholders in the RMF process.

8. *Whether the soon to be published draft companion document citing AI risk management practices is useful as a complementary resource and what practices or standards should be added.*

The soon-to-be-published draft companion document will absolutely be useful and is equally as important as the AI RMF itself. Indeed, without this document, the AI RMF is not practically implementable. Organizations may not know what practices they can reasonably undertake to achieve the outcomes associated with each Function. For example, the practices that make up the Measure function will be important, particularly given many of the points we raised previously around systems that are not easily measured. Additionally, it may be the case that measurements and metrics do not exist yet. As NIST further develops the Practice

[8] See p. 3 of NIST Privacy Framework, available here: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

Guide/companion document, it may be helpful for it to categorize measurement criteria for mapping specific measurement mechanisms proposed by NIST, as well as individual AI risks and use cases, for each of the categories described: analysis, quantification, tracking, and response. We encourage NIST to draw inspiration from existing practice guides in similar fields, (e.g., safety RM, environmental RM, quality RM, medical RM, financial RM; energy, oil and gas RM), considering in particular that *ISO 31000 is the basis for a number of standards and practices in a variety of sectors (e.g., Industrial; automotive; aerospace; medical).*

The companion document could focus on the specific differences of AI risk management activities, versus existing risk management methods, tools, and expertise across sectors. For example, it might be helpful to explore the specifics of:

- determining likelihood, severity, detectability
- which treatment options to select, how to implement them and when (e.g., measures and test methods, documentation templates, peer-reviews, audits, etc.).
- what to report, when and to who

At the very least, NIST should include in the Practice Guide the slate of AI risk management standards under development in ISO/IEC JTC 1 SC 42, including ISO/IEC DIS 23894 and CD ISO/IEC 5338. We also encourage NIST to add the AI Risk Classification Framework to the Practice Guide, which organizations can use as a starting point for implementing the categories associated with the Map function.

As we have mentioned in all our submissions thus far, one of the key challenges to making the AI RMF implementable is the fact that many standards are still under development to address many of the categories and sub-categories. So, it may be that there are not Informative References or practices available for some of the categories yet. NIST should explicitly note areas where practices and/or references are still under development or not yet available.

Furthermore, it is important that the Practice Guide includes examples for entities that build and deploy their own AI systems as well as examples for entities that use other vendors' AI models.

9. *Others?*

There is a significant expertise and body of knowledge related to risk management among various industry sector organizations. We encourage NIST to reach out and consult further with these industry organizations. For example, connecting with American Society for Quality (ASQ) could be beneficial. More specifically, we note that several key points surfaced during the March NIST Workshop on the AI Risk Management Framework, which are common to quality assurance across the board. ASQ and the Quality Profession have vast expertise in establishing a risk culture; accountability and governance; lifecycles; continuous improvement, measurement, and monitoring; closed-loop effective problem solving. ASQ also has expertise in safety, environmental and social responsibility.[9] ITI, through its members, could provide a connection to engage a discussion with ASQ.

We also think it might be useful for the AI RMF to include an approach to continuously communicate with communities of AI developers about new risks in AI, and share information on ways to identify, mitigate said risks, if possible, reporting back to the larger community.

Finally, regarding Profiles, it is important to understand the use cases and patterns by which organizations deploy AI systems today, and how those systems might be deployed in the future. In some cases, organizations may develop their own models, but in many cases, third party software vendors provide "out-of-the-box" models to organizations to solve specific use cases. We should separately address the profile of risk inherent in the deployment of models for which the end user may not create, understand the true performance of, or be able to audit themselves. Organizations may find a different set of challenges when implementing an off-the-shelf solution as opposed to developing the solution in-house, and it would be beneficial for the Profiles to encapsulate those challenges and associated risk of deploying systems not completely under first-party control.

***

We appreciate the opportunity to provide feedback to NIST as it continues to hone the AI Risk Management Framework. We believe this tool has the potential to be incredibly useful, but NIST must further work to align the Framework with existing standards and continue to consider key questions in the context of the Framework. The Practice Guide will be fundamental to the effective use of the Framework, so we encourage NIST to make the development of that document a priority moving forward as well. ITI and its members take seriously AI risk management and look forward to continuing our engagement with NIST moving forward.

[9] See more about ASQ here: https://asq.org/