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 5 functions are somewhat useful for reporting on organizational readiness to Identify, Protect, Detect, Respond, Recover. However, cybersecurity efforts are better organized around how organizations accomplish the work. For our organization, there's a many-to-many mapping between one of our "Workstreams" and a NIST CSF Function or a "Workstream" and a NIST CSF category. Our "Access Management Workstream", for example, is accountable for ~4 of the 7 PR.AC security objectives and our "Asset Management workstream" is accountable for security objectives within ID.AM, PR.DS, PR.IP, and PR.PT. Therefore, we map security objectives to Workstream or 'how-we-work' for calculating maturity scores, Implementation Tiers and creating profile targets. We look to manage risk and increase maturity per Workstream – which is of course also the way that projects and budgets are aligned. That said, at the end of the day we do look at scores per function and sometimes look at scores per category but we drive work based on scores per Workstream or custom subsets of security objectives. This also helps us to work across organizational functional areas to achieve desired CSF Function maturity targets.

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

We have made our NIST CSF maturity scores more actionable by standardizing maturity levels based on a CMMI scale and 4 aspects of the score: (1) Policy (are policies sufficient to meet the security objective), (2) Supporting Procedures (do we have procedures sufficient to ensure compliance, achieve the security objective or operate within agreed upon risk tolerances for some/key/all assets), (3) Shared Services or Common Controls (to what extent are common controls used to achieve the security objective and to ensure compliance to policy), and (4) Metrics (do we have centralized oversight of ongoing compliance or centralized insight into risk). With this insight, we see where we can reduce risk (or increase maturity!) by increasing uptake of common controls, expanding policy, improving procedures or implementing more security measures. Additionally, where we have Key Risk Indicators, we can map them back to security objectives and see where we need to work harder across the 4 aspects of those scores.

It is interesting for us to know how our scores compare to the scores of our industry peers - even if we are calculating our scores differently. BETTER would be knowing that we are using a consistent approach to scoring. However, we score in a way that's actionable for us. Also, by periodically using 3rd party assessments we can determine whether we are grading ourselves more strictly or more leniently than our peers and make adjustments if needed.

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).

Tracking can be done in a spreadsheet but it's much easier and more effective if you have a tool that allows you to:

- Automatically calculate scores based upon entered responses
- Link to artifacts
- Use CSF assessment responses and artifacts to pre-populate other assessments (e.g. NERC CIP, ransomware readiness, Supply Chain security)
- Export assessment results or conclusions to standardized reporting templates
- Establish targets and forecast scores based on anticipated projects
- Interface with GRC tools

The level of complexity of the framework is good for organizations who are able to take a risk-based approach in providing different levels of assurance for different environments. We can assess the entire organization against the NIST CSF – and only drill down to 800-171 or 800-53 or FedRAMP or HIPAA or NERC CIP or _____ as needed in order to provide assurance that the security objectives are met for a specific subset of the environment.

Still, it's a heavy lift for organizations who are not accustomed to living with 800-53. One has to find a way to get buy-in from the organizational functions that support the security objective but who don't have "security" as their day job. The NISTIR 8286 approach of considering how cyber positively or negatively impacts the risk to strategy, operations, reporting and compliance has been useful in starting conversations.

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.

There's no easy way (that we've seen!) to use the Framework to take credit for timely, well planned system refresh; strategic planning and replacement of end-of-life systems; or technology updates to pace with changes in business requirements or changes in the threat landscape. And yet these are key to improving security and minimizing risk. One would expect organizations to improve in these areas as they mature.

There's also no easy way to talk about the balance between maturity and security. There are many ways to increase your maturity score but only some of those paths also minimize risk – and sometimes it's better to prioritize the projects that have a minimal (or no) impact on your maturity score because they also address some of your biggest risks.

Once you get the buy-in of IT and Audit, and Legal and Communications and … others will want to show how their non-security related projects are all driving down Enterprise and or cyber

risk or otherwise improving operations in general. It's a good problem to have but the CSF does not help you to solve it.

It would be great to have a standardized way to talk about Implementation Tiers in terms of an organization's ability to perform against the security objectives. We have customized a way to do so that makes sense for our organization – and which allows us to evidence performance at our target Implementation Tier. However, since most organizations are not using the Framework in this way, we aren't yet able to compare ourselves to our industry peers.

It would be great to have a security objective /subcategory that spoke to an organization's ability to identify and manage system-of-system risks – whether it's one Business Unit's impact on another; impact from the supply chain; impact from a partner; or impact to your customer. This would pair well with the Implementation Tier scoring.

It would be nice to have change management called out separately from configuration management since the scope of "changes" or "configurations" can be very broad on their own.

Taking the Function names at face value, it's tempting to expect incident response and disaster recovery capabilities to fall within Respond and Recover respectively. However, some "resilience" related capabilities are scored in Identify. It's not necessarily a bad thing – especially if you customize your organizational profile. Respond and Recover still beg to be combined into one Function. You might consider a Resilience function.

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.

Backward compatibility would be most severely impacted by changes to the subcategories because that's where the mapping to other frameworks happens. Additions, just as you'd make to 800-53, should be low impact.

6. Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.
Rationale for the provided mapping to 800-53 would be useful.