Feedback from CertiKit Limited on Cybersecurity Framework V2.0 Draft Dated August 8th 2023

We are a small business based in the UK, focusing mainly on providing materials to support the implementation of ISO standards, including ISO27001. See www.certikit.com.

We welcome the evolution of the Cybersecurity Framework into V2.0 and would make the following points about the current draft, mainly from the point of view of an organization that is new to the Cybersecurity Framework (CSF), but familiar with other standards such as ISO27001, UK Cyber Essentials and PCI DSS:

1. Overall, the addition of the Govern function is a good idea and moves the CSF higher up the value chain for information security. The emphasis on cybersecurity supply chain risk management is a definite plus too.
2. We realize that the purpose of the CSF is to provide guidance to organizations large and small in all industries, and that it is not a certifiable standard. However, for a small business particularly this makes the CSF rather nebulous and vague in places, and more difficult to engage with than it could be. The implementation examples are a big help in understanding what is meant by some of the subcategory statements, and further development of these will be a very useful part of the CSF.
3. We found it difficult to understand the purpose of the tiers; apparently they are not intended as maturity levels in the same way as CMMI, but some of the guidance does seem to suggest they may be used as such, for example when defining the current and target profiles. Although the guidance does try to explain them fully, we feel that new users will still struggle to fully understand their purpose. More examples of their use would be helpful.
4. The only reference we could find to a recommended implementation plan for the CSF was the document "Commercial Facilities Sector – Cybersecurity Framework Implementation Guidance" dated May 2020 by the US DHS CISA. This sets out a seven step process. A more "NIST-Official" methodology could be useful here, perhaps along the lines of the PCI DSS "Prioritised Approach".
5. It is foreseeable that existing certification companies may start to offer certification to the CSF in order to offer a competitive advantage to organizations that use the Framework. We have seen this even with ISO standards that are only intended for guidance, such as ISO/IEC 27017. It may be worth bearing this in mind when making decisions about the structure and wording of the CSF, as such schemes may be outside the control of NIST (as they are outside the control of ISO for their standards). Maybe it's worth NIST making some arms-length provision for certification schemes in the same way that these are allowed for within the GDPR for example. Having a completely unregulated certification industry growing up around the CSF may not be good for NIST and the reputation of the Framework longer term.
6. As we are currently within the transition period from the 2013 to the 2022 version of the ISO27001 standard, it may make sense to provide informative references for both versions of that standard.
7. We noticed that the link to the ISO27001(2013) standard (https://www.iso.org/standard/54534.html) within the National Online Informative References Program is currently broken.