Kantara Initiative Anchored Notice and Consent Receipt Work Group

The Anchored Notice and Consent Receipt (ANCR) Work Group submits the following comments on the Interim Public Draft of the Cybersecurity Framework

https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd

The Cybersecurity Framework (CSF) 2.0 highlights the following as objectives, several of which are of particular interest to the efforts over time and currently underway at the Kantara Initiative and the ANCR WG.

- **Recognize broad use of the Framework**

The broad use of the framework stems from "the fact that the high-level outcomes it seeks to achieve can be used by any organization." (lines 3 and 4). Even broader use of the framework would be achieved if it had the ability to be used by and for any person. A human risk perspective, not risk of (personally Identifiable) information capture and use by an organization. The ANCR WG and our ANCR Framework is a human concentric approach that complements organization risk management frameworks.

- **Relate CSF to other Frameworks and resources**
    - Privacy Framework
    - SP-800-181 Workforce Framework for Cybersecurity
    - SP-800-218 Secure Software Development
    - SP-800-161r Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
    - SP-800-55 Performance Measurement Guide for Information Security
    - NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management
    - AI 100-1 Artificial Intelligence Risk Management Framework

Inclusion of the Privacy Framework and the other frameworks and resources is a welcome addition and companion to the CSF. Risk exists and finds its way throughout ecosystems, expanding the CSF framework particularly with respect to privacy and specifically digital privacy is a critical step forward.

- **Increase guidance on CSF implementation**

See comments below on transparency and digital privacy.

- **Emphasize cybersecurity governance**

The ANCR WG has developed a Transparency Performance Scheme and Indicators that can be used to measure the legal conformance of the organizations governing information systems. It builds on the Kantara Initiative Consent Receipt v.1.1 incorporated by ISO into ISO/IEC 29184 Online privacy notices and consent and 27560 Consent record information structure. Transparency of authority is critical to trust in cybersecurity systems and the provenance of their governance. It can also be used to create a credential for the authority that can be used by people independently of service providers, so-called data controllers.

ANCR Framework includes

- Personal Data Control
- Data Protection
- Co-Governance

Traditional cybersecurity has primarily focused on data protection. These other vectors are also critical in assessing, providing notice, and managing risk. We welcome the opportunity to contribute and collaborate on the Transparency Performance Scheme and Indicators and other components in the ANCR framework and its controls to expand assurance and governance to cover these aspects of trust.

- **Emphasize cybersecurity supply chain risk management**
- **Clarify understanding of cybersecurity measurement and assessment**

The framework is missing much of the language we have use in measuring trusted systems. We believe these are critical terms and need to find their way into the framework.

Transparency 0 mentions
Transparent 0 mentions
Consent 0 mentions
Notice 0 mentions
Authority 0 mentions
Authorization 2 mentions

Only one control, which is very general requirement for identity and access management.

Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)

PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties (formerly PR.AC-01, PR.AC-03, PR.AC-04)

The CSF must include guidelines on the assessed risk of unauthorized access (formerly PR.AC) as mentioned in PR.AA-05.

This risk assessment should adopt the risk vector outlined above, again in the same vein of it being necessary and beneficial to adopt a wide risk management framework.

One aspect of our work involves the notice that must be provided associated with the assessed risk. The CSF MUST include a requirement for a notice of the risk to be presented, created from the assessed risk. The assessed risk needs to be expanded to address data control impacts, in addition to data protection in the assessment and notice.

By putting governance at the center of the CSF in its latest rendition NIST is very much aligning with the need for conformance and compliance governance at the center of the CSF and de facto the Privacy Framework as well.

Fig. 2. Framework Functions

I'd like to also mention support and the opportunity to present the ANCR WG work at IEEE in following:

IEEE Cybersecurity for Next Generation Connectivity Systems
IEEE Privacy Initiative

Respectfully submitted,

Salvatore D'Agostino

Salvatore (Sal) D'Agostino
Chair
On behalf of the ANCR WG