July 31, 2024

The Information Accountability Foundation (IAF) offers these comments on the NIST Privacy Framework Version 1.1 Concept Paper. The IAF is an independent non-profit think tank whose research and education mission focuses on accountability and risk and governance frameworks.

We support updating the NIST Privacy Framework and encourage consistency and alignment between the Privacy Framework and the Cybersecurity Framework as described in the key focus areas. Rather than treating the PF and CSF Frameworks as standalone, they should operate as complementary elements of a larger risk management and governance whole.

- IAF member companies often use NIST Frameworks not only for compliance, but as part of a larger governance strategy.
- Additionally, IAF strategists at time provide consulting services (independent of the IAF) for small and mid-size companies to help them build out compliance and governance programs. In these situations, security and privacy teams work in tandem out of time, cost and credible necessity, assessing against both Frameworks at the same time.

It only makes practical sense to align the two Frameworks.

Section 2 Topics and Examples.
The introduction of an Oversight Category in the CSF, combined with a new Oversight Category in the Govern-P Function is a crucial addition which could enhance the overall status of NIST - emphasizing the importance of leadership, identifying strategic opportunities and governance as the strategic foundation of operational compliance. Given the broadening roles of privacy, security and risk leaders who are dealing with the onslaught of data-driven algorithmic and AI innovations and attack vectors, it's important to incorporate strategic governance.

Section 3 Topics and Examples.
Aligning the Awareness and Training category reflects how many, many organizations already approach these efforts today as part of privacy and security programs. Often, privacy and security training programs are fully integrated and delineated along business role/functional lines (vs. privacy and security).

We think it is useful to align the categories of Cybersecurity Supply Chain Risk Management and Data Processing Ecosystem Risk Management. The IAF and some of its member companies prefer the use the concept of "data supply chain risk management" or "data ecosystem risk management", which is reflective of the impact of data-driven algorithmic and AI innovations, where there is not really a separation between the handling and controls for Personal

Information (or, Personal Data) and other types of data. We do appreciate the goals of the concept "data processing ecosystem risk management", although it's a bit of a mouthful.

The significance of data-driven algorithmic and AI innovations underscores the importance of the expanded Technology Infrastructure Resilience Category - supporting both data-driven innovation and the demands on cybersecurity to protect, detect and respond to attacks.

Closed loop systems are an important part of governance, therefore the adding this concept to the Monitoring and Review to Governance for Privacy Programs.

Other Potential Updates.
As suggested in our comments throughout above, the IAF encourages NIST to incorporate AI technology risks into the relevant PF Framework subcategories. We see this as the logical next step, reflected in other organizations evolution, such as the IAPP. Both Privacy and Cybersecurity programs are taking on AI governance responsibilities, given the cross-organizational expertise of these functions. This is especially true for the Privacy Function.

It would then be useful to take a fresh look at how the three Frameworks – the AI Risk Management Framework, the Privacy Framework and the Cybersecurity Framework can be more tightly aligned into one overall governance framework. Such an effort may provide more opportunities to map to the EU AI Act obligations, helpful to U.S. multinationals.

Over the last few years, the IAF has developed, in conjunction with business and in multi-stakeholder sessions, a normative assessment framework for demonstrating accountability and compliance with U.S. State Privacy Laws. We see an opportunity to leverage and align our work with NIST's plans, and welcome the opportunity to discuss in more detail.

Regards,
Barb Lawler

Barbara Lawler
President
blawler@informationaccountability.org
www.informationaccountability.org
IAF