wiley

NEWSLETTER

Breaking Down NIST's Draft Privacy Framework

September 2019

Privacy in Focus®

Slightly shy of a year from kicking off the Privacy Framework effort, the National Institute of Standards and Technology (NIST) has released a preliminary draft of the document, entitled *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management* (Draft Framework or Draft). This Draft comes amidst a continued flurry of privacy activity at both the state and federal levels.

The Draft Framework is intended to help organizations understand, communicate, and manage privacy risks. The document is "agnostic to any particular technology, sector, law, or jurisdiction"[1] and is meant to be a practical implementation tool for organizations to manage risks. In short, while other parts of the federal government are considering various privacy policy approaches, NIST's goal has been "to deliver a tool that could help organizations communicate better about privacy risks when designing and deploying products and services, provide more effective solutions that can lead to better privacy outcomes, and facilitate compliance with their legal obligations."[2]

Below is what you need to know about the Draft Framework, as well as next steps for engagement.

The Framework Basics: Like NIST's popular Cybersecurity Framework, the Draft Framework has 3 main parts: the Core, Profiles, and Implementation Tiers.

- The **Core** consists of 5 high-level "privacy protection activities and outcomes" known as Functions:[3] Identify-P, Govern-P,

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Control-P, Communicate-P, and Protect-P. The first 4 Functions are intended to help to manage privacy risks that arise from data processing, and the final Function is intended to help manage privacy risks that arise from privacy breaches. However, NIST makes clear that the final Function, Protect-P, is "not the only way to manages privacy risks associated with privacy breaches," and that organizations can use the Privacy Framework in conjunction with the Cybersecurity Framework to address privacy and cybersecurity risks together.[4] Additionally, each Function has corresponding Categories and Subcategories of various privacy outcomes.

- A **Profile** is an organization's selection of specific Functions, Categories, and Subcategories, based on the organization's "business requirements, risk tolerance, privacy values, and resources," and other factors, such as "legal/regulatory requirements and industry best practices."[5] NIST makes clear that an organization "may not need to achieve every outcome or activity reflected in the Core" and that instead, and organization may tailor the Framework when developing its Profile or Profiles.[6]
- Implementation Tiers "support organizational decision-making about how to manage privacy risk by taking into account the nature of the privacy risks engendered by the organization's systems, products, or services and the sufficiency of the processes and resources the organization has in place to manage such risks."[7] NIST reiterates that the Tiers should not be thought of as maturity level; in fact, as NIST describes, Tier 2 could be sufficient for some organizations.

Key Characteristics of the Framework: The Draft Framework proposes a **voluntary** and **flexible** tool for organizations to manage privacy risk. These characteristics support NIST's goal for the document to be "widely usable by organizations of all sizes."[8] In its drafting, NIST makes clear that "managing risks to individuals' privacy is not well-suited to a one-size- fits-all solutions,"[9] so it explains that "[t]he Privacy Framework . . . is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and enterprises, and stay current with technology trends, including [AI and IoT]."[10]

How to Use the Framework: Further driving the characteristic of flexibility, NIST highlights that "[d]ifferent types of entities . . . can use the Privacy Framework for different purposes."[11] Depending on the "unique needs of an organization,"[12] some potential uses include: mapping to Informative References, strengthening accountability within the organization, establishing or improving privacy programs, and informing buying decisions, among others.

Next Steps: The current Draft Framework is open for public comment, with comments due by October 24. NIST has welcomed feedback on the Framework from the start of this process, but the opportunity for interested stakeholders to weigh in is winding down, as NIST hopes to finalize the Privacy Framework by the end of the year. If your organization would like to engage with NIST on this important document, now is the time!

For additional information, please contact:

Megan L. Brown
202.719.7579 / mbrown@wiley.law

Kathleen E. Scott
202.719.7577 / kscott@wiley.law

[1] Draft Framework at 4.

[2]Naomi Lefkovitz, *The Preliminary Draft of the NIST Privacy Framework is Here!*, Cybersecurity Insights—a NIST blog (Sept. 9, 2019), https://www.nist.gov/blogs/cybersecurity-insights/preliminary-draft-nist-privacy-framework-here.

[3] Draft Framework at 5.

[4] *Id.*

[5] *Id.* at 10-11.

[6] *Id.*

[7] *Id.* at 12.

[8] *Id.* at 4.

[9] *Id.* at 3.

[10] *Id.* at 3.

[11] *Id.*at 9

[12] *Id.* at 12.