REQUEST FOR COMMENT RESPONSE

NIST PRIVACY FRAMEWORK 1.1 DRAFT

June 13, 2025

I. INTRODUCTION

In response to the National Institute of Standards and Technology's ("NIST") stakeholder feedback opportunity on the Privacy Framework 1.1 Initial Public Draft ("Privacy Framework 1.1"), CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

We appreciate NIST's efforts to provide resources to organizations which in turn will improve data security. NIST's frameworks have a legacy of being useful tools and this update is timely. We do not have feedback on every aspect of the Privacy Framework 1.1, but we do want to offer several points for consideration as NIST finalizes the document.

A. *Harmonization with CSF 2.0*

CrowdStrike agrees with NIST's goal of unifying the Privacy Framework 1.1 with the Cybersecurity Framework 2.0 ("CSF 2.0"). Many of the modifications made in CSF 2.0 improved the framework, and likewise will improve the Privacy Framework. We agree with the changes in the Govern function to mirror CSF 2.0. Privacy and cybersecurity cannot exist without each other and are more intertwined than ever before. Integrating the Privacy Framework 1.1 and the CSF 2.0 through the modifications of the Govern

function will be useful to organizations looking to take a holistic approach to their cyber and data security strategies.

B. *Cybersecurity and Privacy*

As the Privacy Framework 1.1 notes, cybersecurity and privacy are closely related and often overlap. Many of the most innovative technologies for protecting personal data against data breaches leverage cybersecurity technologies that transmit endpoint telemetry data, employ a cloud-native Software-as-a-Service (SaaS) delivery model, integrate 24/7 global threat hunting, and correlate indicators of attack across disparate environments. Moreover, modern IT infrastructure in general invariably involves cross-border data transfers. With this in mind, we appreciate Section 2.1 which provides users with options to use CSF 2.0 and the Privacy Framework 1.1 together and discusses how the Core of each relate and overlap.

C. *Modified Security Sections*

The Privacy Framework 1.1's new Platform Security and Technology Infrastructure Resilience categories address hardware, software, and network security. We recommend PR.PS-P2, PR.PS-P3, and/or PR.IR-P1 be amended to include holistic endpoint monitoring, stating: "*Endpoints and their data are monitored using Endpoint Detection and Response (EDR) commensurate with risk to protect from unauthorized access and usage.*" Endpoints can include servers, desktops, laptops, all-in-ones, tablets, mobile or cellular telephones, thin clients, computing peripherals, virtual containers, and cloud workloads - all of which can include data that needs to be protected. This update will encourage organizations to protect each individual element of their networks, and will present that practice more clearly given the increased prevalence across the industry of ephemeral endpoints (e.g., virtual machines and containers).

D. *Artificial Intelligence*

CrowdStrike welcomes the initiative by NIST to include Artificial Intelligence ("AI") considerations in existing frameworks and supports the idea of creating a Cyber AI Profile. As NIST pursues these various methods to incorporate AI into its resources, we recommend harmonization and mapping, where possible. Recently, we commented on

NIST's Cybersecurity and AI Workshop Concept Paper.[1] As we noted in those comments, public discourse around AI has grown exponentially in the last several years, but AI in cybersecurity and data protection is not a new concept. CrowdStrike has deployed AI at scale across tens of millions of endpoints for prevention, dating back ten years. We are now deploying Agentic AI at scale. Other vendors are also experimenting with these tools. As a community, we should continue to leverage AI for cybersecurity use cases.

We appreciate the flexibility to apply the same principles to AI that can also be used for privacy risk management. From our perspective, integrated consideration of AI, privacy, and cybersecurity is a best practice.

While Section 1.2.2 correctly implies that AI creates new cybersecurity risks, it fails to note that AI can help improve privacy and cybersecurity functions. While AI is often framed as posing a risk to privacy, it is actually critical for protecting data against cyber threats, thereby becoming critical for modern privacy. AI-powered systems can detect and respond to threats faster and more accurately than traditional methods, making them essential in our defense against sophisticated cyberattacks and data breaches.

AI-driven security and privacy protection go hand in hand to identify adversary behavior and combat sophisticated attacks. For example, CrowdStrike incorporates Privacy-by-Design principles into how we train data, and our products are designed to protect customers against data breaches that threaten privacy.[2] This approach is particularly crucial as we face the rise of dark AI, where cyber threat actors use AI to conduct faster, more sophisticated attacks that often go undetected.

With this in mind, we recommend that the positive link between privacy and AI, and cybersecurity and AI, be referenced in Section 1.2.2 to highlight the opportunities organizations have to improve their data security strategy by leveraging AI technologies.

---

[1] NIST's *Cybersecurity and AI Workshop Concept Paper Response*, CrowdStrike, https://www.crowdstrike.com/content/dam/crowdstrike/marketing/en-us/documents/pdfs/public-policy/NIST-Cybersecurity-and-AI-Concept-Paper-Comments.pdf

[2] *The Evolving Role of AI in Data Protection*, Drew Bagley and Christoph Bausewein, https://www.crowdstrike.com/en-us/blog/the-evolving-role-of-ai-in-data-protection/

III. CONCLUSION

NIST's Privacy Framework 1.1 provides a thoughtful update to a complex, constantly evolving, policy area - data protection. As the framework moves forward and evolves, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend that any final framework include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot
Senior Manager, Public Policy

Email: policy@crowdstrike.com

***