REQUEST FOR COMMENT RESPONSE

CYBERSECURITY FRAMEWORK PROFILE FOR ARTIFICIAL INTELLIGENCE (CYBER AI PROFILE)

January 30, 2026

I. INTRODUCTION

In response to the National Institute of Standards and Technology's ("NIST") stakeholder feedback opportunity on the Cybersecurity Framework Profile for AI ("draft Profile"), 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 better protect the nation from cybersecurity threats. NIST's frameworks have a legacy of being useful tools and this update is timely. CrowdStrike previously commented on the Concept Paper of this effort.[1] We do not have feedback on every aspect of the draft Profile, but we do want to offer several points that may be of use as NIST finalizes the Profile.

A. *When thinking about applying the Cyber AI Profile, how useful (or not) is it for all three Focus Areas to be shown alongside each other (as they are currently reflected)? What value might there be in providing Profile content for each Focus Area separately?*

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

While the draft Profile acknowledges that "each Focus Area enables the other two" and describes some interrelationships, CrowdStrike recommends strengthening this section with clearer guidance that explicitly states organizations should implement all three focus areas concurrently rather than selecting individual areas.

The current document includes valuable content on how these areas interrelate (e.g., "when AI systems are well secured, AI-enabled defenses are better able to find and react to threats targeting those systems"), but does not sufficiently emphasize the critical importance of implementing a holistic approach that encompasses all three focus areas simultaneously.

CrowdStrike recommends adding a new subsection to Section 2.1 titled "Implementing Focus Areas as an Integrated Whole" that explicitly states organizations should aim to implement controls across all three focus areas. Organizations that implement only one or two focus areas will have significant blind spots in their AI security posture. For example, an organization that secures its AI systems but doesn't leverage AI for defense will miss opportunities to detect sophisticated threats, while an organization that uses AI for defense without adequately securing those AI systems creates a gap in the organization's security posture.

B. *Table 1. Cyber AI Profile*

GV.RM-03: CrowdStrike recommends elevating this to Priority 1 across the focus area, as AI systems require risk management processes that address their unique characteristics. Risk management processes can include monitoring AI behavior and interactions, leveraging AI defensive systems, methods to discover shadow AI, and threat hunting for AI-enabled attacks. These processes should be continuously updated based on the evolving AI threat landscape and new capabilities.

GV.RR-02: CrowdStrike recommends this category be designated Priority 1 for all three focus areas. Organizations need regularly updated risk response procedures for AI systems that may behave differently from traditional security incidents. Risk responses should include procedures for human intervention and capability to remediate AI systems that show signs of compromise or manipulation.

GV.SC-02: AI SBOMs need further development and guidance from government agencies, like NIST or CISA, before being broadly recommended. However,

organizations should still implement robust supply chain security measures for AI components, including evaluation of third-party models, assessment of training data sources, and monitoring of third-party AI services for security issues while industry standards for AI SBOMs continue to mature.

ID.AM-02: Organizations should be able to maintain visibility and apply controls across AI systems. Security teams increasingly require specialized capabilities to protect the enterprise throughout the AI lifecycle. An emerging security category called AI Detection and Response (AIDR) enables security teams to monitor and govern AI systems - including identifying shadow AI. An approach like AIDR, that allows real visibility into AI use and relationships, is actionable for Secure, Defend, and Thwart focuses unlike a static inventory.

ID.RA-02: Threat intelligence is an important part of an organization's security strategy; however, proactive hunting is a leading indicator of the strength of an enterprise cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. The more well-instrumented the environment, the more opportunities defenders give themselves to identify malicious activity as an attack progresses through phases. A strong threat hunting program will incorporate AI-specific threat intelligence, including emerging attack techniques targeting AI systems and patterns of AI-enabled attacks. CrowdStrike recommends this category be designated Priority 1 for all three focus areas and include reference to the importance of threat hunting in addition to gathering intelligence.

PR.AA-01: The draft Profile correctly notes that identity principles can be applied to AI. CrowdStrike recommends strengthening this section to note identity best practices that can be applied to agentic AI systems and raising the Priority to 1. Organizations must implement identity-centric approaches to security to stay ahead of adversary threats using a combination of real-time authentication traffic analysis, telemetry from endpoints, and AI-enabled analytics to quickly identify and prevent identity-based attacks. For example, organizations should be able to monitor identity risk in real time and grant, deny, or revoke access as threat conditions change across human and AI identities. Identity security must account for both human and AI identities with appropriate controls.

PR.DS-01: CrowdStrike agrees with the Priority 1 designation of this control. Data privacy principles apply across various uses, including AI. Data protection involves

integrity, confidentiality, and availability. Accordingly, the context of data processing activities will decide the best ways for protection. An organization's data privacy framework should be extended to address AI systems and their data.

PR.PS-04: CrowdStrike agrees that logging and continuous monitoring are essential for securing AI tools and strengths of AI-enabled cybersecurity. We recommend this control retain its Priority 1 designation.

DE.CM-01 and DE.CM-03: CrowdStrike recommends these controls be designated Priority 1 across all focus areas. AIDR enables security teams to: monitor AI behavior and interactions; secure AI agent identities and access; discover shadow AI; prevent sensitive data leakage to AI systems; protect cloud-based AI applications; and implement guardrails on AI system actions. We recommend a more holistic approach to monitoring and detection - like AIDR - be recommended throughout the controls.

DE.AE-07: CrowdStrike recommends this category be designated Priority 1 in the Defend focus. The draft Profile notes, "AI improves monitoring and strengthens threat detection by flagging anomalies, correlating suspicious behaviors, and spotting unusual patterns faster than humans." AI enables security teams to match the accelerating pace of attacks, a key advantage to AI in cybersecurity.

RS.MA-02, RS.MA-03, and RS.MA-04: CrowdStrike recommends these controls incorporate specific benefits provided by Agentic AI systems in the Defend focus. Sophisticated security teams are leveraging Agentic AI agents on the path to achieving an Agentic Security Operations Center (SOC). Already, SOCs can leverage Agentic AI capabilities to eliminate bottlenecks like triaging and prioritizing alerts, malware analysis, and threat hunting.

III. CONCLUSION

NIST's Cyber AI Profile represents a valuable step forward in helping organizations manage the opportunities and risks presented by AI. As AI continues to evolve rapidly, it is crucial that security guidance remains flexible while addressing core security principles. As NIST moves forward with finalizing this Profile, we recommend continued engagement with stakeholders.

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
VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot
Senior Manager, Public Policy

Email: policy@crowdstrike.com

***