REQUEST FOR COMMENT RESPONSE

CONSULTATION ON ARTIFICIAL INTELLIGENCE (AI) STRATEGY

October 31, 2025

I. INTRODUCTION

In response to the Government of Canada's (Government) request for comment on the development of the next artificial intelligence (AI) strategy (AI Strategy), CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, AI-native, 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 the Government's efforts to create an AI Strategy that prioritizes innovative and secure AI. The request for comment correctly notes that AI is evolving at a rapid pace and creating benefits, and considerations of risks, across many sectors and aspects of life. The cybersecurity sector is no different with AI enhancing security capabilities while also creating new threats that require mitigation.

We welcome the opportunity to offer several points that may be of value to the Government as it drafts the AI Strategy.

A. *Where is the greatest potential for impactful AI adoption in Canada? How can we ensure those sectors with the greatest opportunity can take advantage?*

AI has transformed cybersecurity, and has the power to further strengthen cybersecurity outcomes. CrowdStrike has deployed AI at scale across tens of millions of endpoints for prevention, dating back ten years. Other vendors are also experimenting

with these tools. As a community, we should continue to leverage AI for cybersecurity use cases.

AI can help improve cybersecurity functions. The use of AI to detect cyber threats is an enormous advantage. Today, security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments, and AI can help defenders process this data and make detections more actionable. AI is the best tool defenders have to identify and prevent zero-day attacks and malware-free attacks, because AI can defeat novel threats based on behavioral cues rather than known signatures. AI can also significantly reduce response and mitigation times. This is crucial in an era where attacks can spread across networks in seconds.

AI-native tools provide continuous monitoring and automated scanning for security weaknesses, assisting in vulnerability management. It can prioritize vulnerabilities based on real-world threat intelligence, ensuring resources are focused on the most critical issues. Finally, AI-assisted threat hunting enhances the work of human analysts, combining human intuition with AI's data processing capabilities. This synergy allows for more effective and proactive threat hunting.

Leveraging best-in-class cybersecurity technologies deploying AI is essential to meeting constantly-evolving threats. As Canada drafts its AI Strategy, we recommend cybersecurity practices that leverage AI be encouraged.

B. *What are the emerging security risks associated with* AI*, and how can Canada proactively mitigate future threats?*

Unfortunately, AI is also accessible to potential cyber bad actors. Thwarting AI-enabled attacks can start with understanding how adversaries are currently using AI. One concern is that it enables unsophisticated threat actors to achieve nation-state level cyber capabilities in certain contexts. However, at this point, it does not appear to be broadly elevating threats from actors that are already sophisticated. We anticipate further evolution in the use of AI for defensive and malicious purposes over the coming years.

In CrowdStrike's 2025 *Global Threat Report*, we examined adversary use of AI, particularly generative AI. Generative AI has emerged as an attractive tool for adversaries with a low barrier to entry that makes it widely accessible. Recent advancements in generative AI have enhanced the efficacy of certain cyber operations,

particularly those using social engineering. Adversaries increasingly adopted generative AI over the past year, particularly in support of social engineering efforts and high-tempo information operation campaigns.[1] Both were supported by generative AI tools that can create highly convincing outputs without precise prompting, custom model training, or fine-tuning.

In order for defenders to maintain their AI cybersecurity advantage and stay ahead of adversaries, both public and private sectors must be encouraged to continue innovating. As adversaries continue to evolve and find new ways to target victims, organizations must increase their emphasis on cybersecurity practices that leverage the most effective technologies - and that includes AI.

C. *How can Canada strengthen cybersecurity and safeguard critical infrastructure, data and models in the age of* AI*?*

In addition to leveraging AI to strengthen cybersecurity, as described above, safeguarding critical infrastructure and protecting data are also priorities of CrowdStrike.

Unfortunately, critical infrastructure (CI) providers are popular targets for adversaries and their uneven cybersecurity capacity often makes them vulnerable to these attempts. Cyber risk management in the CI sector is particularly difficult. The integration of standard information technologies (IT) and operational technologies (OT) presents a broad attack surface. In many cases, operators are aware of the threat environment, but face resourcing and workforce constraints that impinge upon their response.

As a practical matter, managed security services and managed threat hunting services are among the most efficient ways to improve CI operators' security programs. Private sector providers are making efforts to offer packages specifically for small and medium sized entities, but policymakers should proactively consider mechanisms like tax credits, rebates, or grants to further incentivize adoption.

The most sophisticated private sector security teams are leveraging Agentic AI agents on the path to achieving an Agentic Security Operations Center (SOC). Already, Agentic

[1] 2025 *Global Threat Report*, CrowdStrike, https://www.crowdstrike.com/explore/2025-global-threat-report?tab.consessionscheduledday=1730400114135003mEeJ&utm_medium=dir

AI can be applied to eliminate some of the biggest bottlenecks in an organization's SOC–including triaging alerts, malware analysis, and threat hunting. This scales expertise, drives consistent outcomes, and allows operations to act at machine speed.[2] Ultimately, CI and public sector organizations must consider methods to modernize cybersecurity programs that utilize these technologies in order to keep pace with private sector capabilities, but more importantly, outpace the adversary.

Over time, AI is going to increasingly integrate into the modern enterprise tech stack. Because of this, it is important to prioritize both the security of AI systems and the data leveraged by AI. The following are principles CrowdStrikes uses to frame our approach in protecting AI systems.[3]

- *Data Operations*: Ensuring the integrity of AI models through carefully curated training data. This includes rigorous processes for protecting our corpus against adversarial machine learning attacks.

- *Continuous Improvement*: Constant refinement of models to adapt to new threats. Our adversarial pipeline, for instance, allows us to generate new adversarial samples to train our machine learning models, increasing their effectiveness against evolving threats.

- *Privacy-by-Design*: Developing AI systems with Privacy-by-Design principles in mind. This helps to leverage AI in a manner designed to respect user privacy while delivering robust security.

- *Transparency and Accountability*: Clear documentation of AI systems' capabilities and limitations. This transparency is crucial for building trust with users and complying with emerging AI regulations.

D. *What frameworks, standards, regulations and norms are needed to ensure AI products in Canada are trustworthy and responsibly deployed?*

---

[2] *CrowdStrike Launches Agentic Security Workforce to Transform the SOC*, September 16, 2025. https://www.crowdstrike.com/en-us/blog/crowdstrike-delivers-seven-agents-to-build-agentic-security-workforce/

[3] *The Evolving Role of AI in Data Protection*, January 29, 2025. https://www.crowdstrike.com/en-us/blog/the-evolving-role-of-ai-in-data-protection/

Fixed technical requirements may quickly become obsolete given the pace of AI advancement and the adaptive nature of threat actors exploiting AI systems. Prescriptive standards can lead to a compliance-first mindset, where meeting narrow criteria takes precedence over meeting the desired security outcomes. If the Government moves forward with AI regulations, we recommend an adaptive, risk-based approach that prioritizes flexibility, encourages innovation, and allows organizations to tailor implementation to their risk profile and domain-specific needs. Any regulations should aim to proactively harmonize with applicable privacy, data protection, and cybersecurity standards (see below).

E. *What are the key barriers to AI adoption, and how can government and industry work together to accelerate responsible uptake?*

The AI Strategy should actively promote regulatory harmonization and coherence across existing sectoral laws and emerging international best practices. Today, the fragmented and overlapping regulatory environment creates uncertainty, increases compliance burdens, and risks deterring AI adoption—particularly among Small and Medium Enterprises (SMEs), startups, and non-digital native sectors.

New requirements or regulations should not stifle innovation and new technologies. Regulating AI, and its use, for the sake of the technology rather than its application is not the best approach to foster innovative solutions to difficult problems. Canada's AI Strategy presents an opportunity for Canada to be a leader in both AI and the security of AI, if the AI Strategy creates an environment of innovation and fostering best-in-class technology use.

III. CONCLUSION

We believe the AI Strategy will be a thoughtful analysis of a complex, constantly evolving, policy area - AI. As the AI Strategy 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 focus on principles rather than prescriptive requirements and 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/.

V. 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

***