**REQUEST FOR INFORMATION RESPONSE**

**AMERICAN AI EXPORTS PROGRAM**

**December 12, 2025**

## I. INTRODUCTION

In response to the Department of Commerce's (Department) request for information on the development of the American AI Exports Program (Program), 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 Executive Order 14179 *Removing Barriers to American Leadership in Artificial Intelligence* and the complementary AI Action Plan, both of which promote innovation. Importantly, throughout the AI Action Plan, security is mentioned and prioritized.

The Department's initiative to establish the Program has the potential to strengthen U.S. leadership in AI while also facilitating responsible global adoption of secure AI technologies. As the program develops, we believe that cybersecurity—specifically the security of AI systems themselves—must be a fundamental consideration for several reasons:

- Prevention of Model Manipulation: Adversaries may attempt to manipulate AI systems, through techniques like prompt injection, potentially compromising their reliability or integrity.

- Data Protection: AI systems process vast amounts of sensitive data, creating new vectors for data theft if not properly secured.

- Supply Chain Security: As AI components are integrated across global supply chains, ensuring the security of these systems becomes essential to maintaining integrity.

We welcome the opportunity to offer several points that may be of value to the Department as it develops the Program.

> 5. *What factors should guide the evaluation of each component of the tech stack when included in a proposal?*

The Department has identified that the full-stack AI technology package will include measures to ensure the security and cybersecurity of AI models and systems. CrowdStrike applauds this inclusion and echoes the importance of protecting AI models and systems. AI systems depend on a complex tech stack that includes software, hardware, GPUs, cloud workloads, training data, etc. Each layer of this stack, as well as the vendors that produce it, must ensure security from development through deployment and use. Further, security may be a layer of the stack in its own right. As the United States promotes AI exports, ensuring comprehensive security will be essential to maintaining trust in American AI technologies.

AI has transformed cybersecurity, and has the power to further strengthen cybersecurity outcomes. Leveraging best-in-class cybersecurity technologies deploying AI is essential to meeting constantly-evolving threats. In addition to leveraging AI for cybersecurity, we must simultaneously address the security of AI systems themselves and the data leveraged by AI.

The following are high-level principles CrowdStrikes uses to frame our approach in protecting AI systems.[1]

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

[1] *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/

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.

More broadly, AI systems must be defended through the 'last-mile;' that is, enterprises, applications, and users. Security teams increasingly require specialized capabilities to achieve this. An emerging security category called AI Detection and Response (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.

> *17. Which U.S. federal support mechanisms would be most useful to consortia and why? In addition to those identified in E.O. 14320, support mechanisms might include regulatory guidance, legislative proposals, identifying export opportunities, assisting navigation of foreign regulatory environments, and assisting with permits and export licenses, among others.*

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 Department 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. With respect to the latter, we recommend NIST 800-53 as a general baseline.

## III. CONCLUSION

We believe the AI Export Program has the potential to accelerate responsible global adoption of secure AI technologies. As the Program 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

***