**REQUEST FOR INFORMATION RESPONSE**

**REGULATORY REFORM ON ARTIFICIAL INTELLIGENCE**

**October 27, 2025**

## I. INTRODUCTION

In response to the Office of Science and Technology Policy's ("OSTP") request for information on Regulatory Reform on Artificial Intelligence ("AI"), 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. The request for information correctly notes that AI is evolving at a rapid pace and creating benefits 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. Importantly, throughout the AI Action Plan, security is mentioned and prioritized.

We welcome the opportunity to offer several points that may be of value to the OSTP as it considers regulations that may unnecessarily hinder the development of AI.

### A. *Cybersecurity and AI*

While the public discourse around AI has grown exponentially in recent years, AI in cybersecurity is not a new concept. 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 behavior 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. New regulation or guidance on AI should incentivize strong cybersecurity practices, and the security of AI itself. Regulations that are not narrowly tailored to address specific harms and risks created by AI risk impacting positive use cases of AI such as cybersecurity.

**B.** *Regulatory Landscape*

The U.S. has long led the development of privacy principles and security standards that continue to influence robust legislation in other parts of the world. Yet, the U.S. has taken a sector-specific, federal and state level, approach in applying these principles to regulation. For example, in the absence of a unifying federal privacy law, U.S. organizations often treat data protection laws from other jurisdictions as the de facto standard. Similarly, in cybersecurity, across federal agencies, states, and sector-specific regulatory bodies there are overlapping and conflicting regulatory requirements.

Sensible, risk-based regulations for privacy and cybersecurity can have positive impacts on the AI era - especially in regards to training and implementation. Measures

that incentivize the adoption of cybersecurity technical and organizational measures to meet ever-evolving risks, reduce the attack surface, and decrease the likelihood of data breaches would not only improve cybersecurity and data privacy, but also the security of AI as it is further built and deployed. We recommend that as OSTP undertakes this effort to examine AI regulation, the larger regulatory landscape of cybersecurity and privacy rules be considered and looked at as an area for both improvement and opportunity.

### **C.** *Regulatory Mismatch*

The request for information asks about "regulatory mismatches" or situations where existing rules no longer align with AI capabilities. One example of this is the Office of the Comptroller of the Currency's (OCC) regulations on supervisory guidance on model risk management.[1] The OCC's requirements were not created with today's AI use cases in mind. The guidance, from 2011, covers models that make financial decisions directly impacting individuals. However, due to interpretation of the guidance, some entities in scope of the OCC are following this guidance for all AI technologies, and even other technologies that leverage AI in some capacity, not just in models that directly impact financial decisions. While third-parties supplying technologies and tools to banks should be expected to demonstrate a high-level of security, descriptions of all the algorithms and machine learning models used in a context such as cybersecurity is burdensome on both parties.

As the OSTP conducts its review of regulatory mismatches, we suggest that the OCC guidance on model risk management be included. The OSTP has the opportunity to encourage future guidance focus requirements on the purpose of the model itself, and appropriately narrowly scope requirements.

## III. CONCLUSION

We believe the AI Action Plan, and its accompanying tasks such as this deregulation effort, is a thoughtful analysis of a complex, constantly evolving, policy area - AI. As the OSTP has noted, there are risks of regulating the underlying technologies that enable AI, rather than the application of the AI itself. The former may limit innovation and competitiveness, while the latter ensures usage aligned with policymakers' goals.

[1] Supervisory Guidance on Model Risk Management, April 4, 2011, https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf.

Regulating AI for the sake of the technology rather than its application is not the best approach to foster-innovative solutions to difficult problems.

As the AI Action Plan implementation moves forward and evolves, 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/.

## 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

***