REQUEST FOR COMMENT RESPONSE

Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum

Docket ID: OMB-2023-0020

December 5, 2023

I. INTRODUCTION

In response to the Office of Management and Budget's ("OMB") request for comment ("RFC") to develop a governance, innovation, and risk management memorandum for Agency use ("memorandum"), 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

CrowdStrike welcomed the release of the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence ("E.O."). The E.O. will not only affect the U.S. government's Executive Branch, but more broadly inform industry best practices, and can even potentially inform subsequent laws and regulations in the U.S. and abroad.

We appreciate the OMB's quick response to the E.O. and their efforts to create a comprehensive agency-wide strategy on Artificial Intelligence ("AI"). The RFC 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.

While we do not have feedback on every question in the RFC, we do want to offer several points that may be of value to the OMB as it refines the draft memorandum.

A. *Question 1)* The composition of Federal agencies varies significantly in ways that will shape the way they approach governance. An overarching Federal policy must account for differences in an agency's size, organization, budget, mission, organic AI talent, and more. Are the roles, responsibilities, seniority, position, and reporting structures outlined for Chief AI Officers sufficiently flexible and achievable for the breadth of covered agencies?

And

Question 2) What types of coordination mechanisms, either in the public or private sector, would be particularly effective for agencies to model in their establishment of an AI Governance Body? What are the benefits or drawbacks to having agencies establishing a new body to perform AI governance versus updating the scope of an existing group (for example, agency bodies focused on privacy, IT, or data)?

The RFC correctly notes that the differences across agencies in size, budget, mission, etc., require flexible requirements to comply with the tasks outlined in the memorandum. The requirements to establish a Chief AI Officer and AI Governance Body seem logical from CrowdStrike's perspective and there seems to be an appropriate amount of room for agencies to adopt the new positions to fit the specific agency. However, like with any new initiative, room for improvement will be discovered as the new roles and groups progress. We recommend that OMB empower agencies to make slight readjustments to the roles of their Chief AI Officer and AI Governance Body as new best practices are discovered.

Perhaps more important than the new roles and groups, is the guidance and requirements that will come from them. CrowdStrike urges alignment where possible with existing rules and regulations created by other agencies. Any new guidance or requirement on AI from agencies has the opportunity to improve AI, which plays critical roles in the everyday lives of many Americans as well as the economy writ large. Nonetheless, new regulation will not be issued in a vacuum but instead amongst a venn diagram of regulations across agencies, sectors, states, other technology areas, and other countries.

The draft memorandum states:

> *"This memorandum does not supersede other, more general Federal policies that apply to AI but are not focused specifically on AI, such as policies that relate to enterprise risk management, information resources management, privacy, Federal statistical activities, IT, or cybersecurity."*

This language provides clarification and we recommend that it remain in the final version. As implied, there is often overlap between cybersecurity technologies and AI because, from a cybersecurity standpoint, the use of AI to detect threats is an enormous advantage. 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. Leveraging these technologies is essential to meeting constantly-evolving threats. In cybersecurity, there are already a myriad of competing and overlapping regulations; continued clarification on how new AI regulations will interact with cybersecurity regulations will be needed.

Finally, as agencies complete their AI strategies and other tasks from the memorandum, CrowdStrike encourages agencies to leverage a risk management approach as seen in AI Risk Management Framework (NIST AI 100-1).

B. *Question* 3) How can OMB best advance responsible AI innovation?

The memorandum and RFC's focus on ensuring innovation, even with new requirements for AI going into effect, aligns with CrowdStrike's views. 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. 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.

The proposed memorandum defines safety-impacting AI and right-impacting AI and determines only AI applications that meet one of those definitions are subject to the minimum practice. This risk-based approach is welcome; however, OMB should be cautious to not expand these definitions to encompass any AI application.

Innovation often comes from competition. The memorandum requires the following:

> *"Promoting Competition in Procurement of AI. Agencies should take appropriate Steps to ensure that Federal AI procurement practices promote opportunities for competition among contractors and do not improperly entrench incumbents. Such steps may include promoting interoperability and ensuring that vendors do not inappropriately favor their own products at the expense of competitors' offerings."*

CrowdStrike supports promoting competition in the procurement of AI and encourages this language to remain in the final memorandum.

C. *Question* 4) With adequate safeguards in place, how should agencies take advantage of generative AI to improve agency missions or business operations?

CrowdStrike leverages generative AI to assist analyst workflows and to make other security analyst tasks more efficient. This capability (coined "*Charlotte*") utilizes CrowdStrike's highest-fidelity security data, which includes the trillions of security events captured in the CrowdStrike Threat Graph, asset telemetry from across users, devices, identities, cloud workloads, and threat intelligence. The use of this knowledge base drives efficacy, actionability, and relevance, as well as addresses the risk of "hallucination."

Further, the natural language interface seeks to make cybersecurity responsibilities more broadly accessible. Our goal with *Charlotte* is to help close the cybersecurity skills gap and improve the response time so users can stay ahead of adversaries – boosting security across organizations. Today, we see this use of generative AI as one of the most relevant to improving security outcomes in the near- to mid-term.

Agencies should leverage generative AI that uses models that are trained using validated sources and sound data, like *Charlotte*.

D. *Question* 8) What kind of information should be made public about agencies' use of AI in their annual use case inventory?

The draft memorandum requires a publicly released compliance plan, an inventory of its AI use cases, and an agency strategy. While CrowdStrike recognizes the intent around these efforts, we caution against publicly disclosing this information. While it could be a helpful exercise for an organization to review their AI use cases, publicly disclosing what technologies are in agency networks could enable threat actors to conduct malicious activities. Adversaries are innovative and smart – threat actors could intentionally target listed AI applications or monitor for a vulnerability they could leverage. For those reasons, public disclosure in these instances may have an adverse effect on security.

III. CONCLUSION

The OMB's memorandum, and the broader E.O., provides a thoughtful analysis of a complex, constantly evolving, policy area. As the memorandum, and other tasks from the E.O., move forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend that the strategy focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike®, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about 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	**Elizabeth Guillot**
VP & Counsel, Privacy and Cyber Policy	Manager, Public Policy

Email: policy@crowdstrike.com

***