REQUEST FOR INFORMATION RESPONSE

NIST's Assignments Under Sections 4.1, 4.5 and 11 of the Executive Order Concerning Artificial Intelligence

Docket Number: 231218-0309

February 2, 2024

I. INTRODUCTION

In response to the National Institute of Standards and Technology's ("NIST") request for information ("RFI") to carry out its responsibilities under the October 2023 Executive Order on Safe, Security, and Trustworthy Development and Use of Artificial Intelligence ("E.O."), 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 E.O. 14110. 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 NIST's quick response to the E.O. and their efforts in identifying existing standards and practices of Artificial Intelligence ("AI"). The RFI 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 note that NIST assignments related to cybersecurity will have a separate process, because cybersecurity is relevant to all aspects of AI, we do want to offer several points that may be of value to NIST.

A. *Question 1 (1)*: What roles can or should be played by different AI actors for managing risks and harms of generative AI?

Generative AI can be a positive tool for cybersecurity. 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. One 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*. There is a difference between a generative AI capability like *Charlotte*, and generative AI that draws from a public, user-based data set. As NIST develops a companion resource to the AI Risk Management Framework for generative AI, we recommend positive use cases of generative AI be taken into account.

B. *Question 1 (2)*: How should NIST create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities and limitations through which AI could be used to cause harm, including enhancing or otherwise affecting malign cyber actors' capabilities, such as by aiding vulnerability discovery, exploitation, or operational use?

Unfortunately, AI, and generative AI, is also accessible to potential bad actors. One concern is that it enables unsophisticated threat actors to achieve nation-state level cyber capabilities in certain contexts. However, at this time, it does not appear to be 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 order to maintain our AI cybersecurity advantage, U.S. public and private sectors must be encouraged to continue innovating. 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.

III. CONCLUSION

NIST's RFI, and the broader E.O., provides a thoughtful analysis of a complex, constantly evolving, policy area. As these NIST assignments, 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
VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot
Manager, Public Policy

Email: policy@crowdstrike.com

***