REQUEST FOR INPUT RESPONSE

DOJ's Assignments Under Sections 7.1(b) of the Executive Order Concerning Artificial Intelligence

May 24, 2024

In response to the Department of Justice's ("DOJ") request for input ("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 this response from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

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.

As the DOJ is considering the use of artificial intelligence ("AI") in the criminal justice system, we recommend the Department leverage cybersecurity tools that utilize AI to protect the sensitive data managed by the DOJ. Today, the DOJ has specific designations for certain types of data like Criminal Justice Information (CJI) and accompanying requirements (CJIS Security Addendum), but this is not sufficient. AI-powered cybersecurity is fundamentally necessary to protect this data even when such safeguards are in place. 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. Leveraging these technologies is essential to meeting constantly-evolving threats.

While the public discourse around AI has grown exponentially in the last year, 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. CrowdStrike also leverages generative AI to assist analyst workflows and to make other security analyst tasks more efficient, providing important benefits given the cyber workforce shortage. This capability (coined "*Charlotte*") utilizes CrowdStrike's highest-fidelity security data, to make cybersecurity responsibilities more broadly acceptable. Other vendors are also experimenting with these tools. We recommend leveraging AI for cybersecurity and data protection use cases, especially when sensitive data, like what pertains to the criminal justice system, is managed by an organization.

I. 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
Senior Manager, Public Policy

Email: policy@crowdstrike.com

***