Mike Britton, Chief Information Officer
Abnormal Security
8474 Rozita Lee Ave, Suite 420
Las Vegas, Nevada 89113

https://abnormalsecurity.com/

March 14, 2025

Faisal D'Souza, NCO
Office of Science and Technology Policy
Executive Office of the President
2415 Eisenhower Avenue
Alexandria, VA 22314

Submitted by email to ostp-ai-rfi@nitrd.gov

This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing the AI Action Plan and associated documents without attribution.

Re: Request for Information (RFI) on the Development of an Artificial Intelligence (AI) Action Plan

Introduction

Abnormal Security strongly supports the Office of Science and Technology Policy (OSTP) in its efforts to develop a robust AI Action Plan that safeguards national security and protects critical infrastructure. Our submission outlines policy recommendations that emphasize the dual-use nature of AI technologies, and the need for proactive defensive measures against AI-enabled cyber threats.

AI's scalability, automation, and adaptability have rapidly shifted the cybersecurity threat landscape. Attackers are leveraging AI to develop capabilities once limited to well-funded nation-state actors, enabling them to launch more sophisticated, targeted, and larger-scale attacks with unprecedented speed.

The increasing adoption of AI within cyberattack methodologies necessitates a parallel evolution in defensive capabilities, centered on the adoption of AI-native cybersecurity. This will enable the federal government to increase its level of innovation to meet the pace at which the adversary operates.

We advocate for strategic investments in AI-driven security infrastructure to mitigate the risks of offensive AI, and cross-sector collaboration to fortify American enterprises against adversarial cyber threats.

About Abnormal Security

Abnormal Security is a leader in AI-native cybersecurity solutions, leveraging advanced machine learning to stop sophisticated cyber attacks and detect compromised accounts across email and connected applications.

Our AI-native approach leverages identity and context to understand human behavior and analyze the risk of every cloud email event – detecting and stopping sophisticated, socially-engineered attacks that target the human vulnerability.

By using AI to identify and mitigate emerging threats – including AI-powered threats – that evade traditional security measures, Abnormal ensures that businesses, government agencies, and critical infrastructure operators remain protected against evolving attack methodologies.

Key Consideration: Defensive AI to Counteract AI-Powered Threats

AI-driven cyber threats, including AI-generated social engineering attacks, are rapidly evolving. AI's ability to understand, mimic, and manipulate human behavior has created an unprecedented crisis, leading to a rise in successful phishing, business email compromise (BEC), account takeovers, and deepfake exploits.

The impact of these attacks can be devastating – for businesses and critical infrastructure, for consumers, and for national security. Account compromise, for example, has been the culprit behind major attacks in recent years, from the Colonial Pipeline ransomware attack in 2021, to Uber's data breach in 2022, and the U.S. State Department's email breach by Chinese hackers last year. And according to the FBI's latest Internet Crime Report, business email compromise resulted in over $2.7 billion in reported losses in 2023 alone.

AI doesn't just increase attack volume; it transforms every social engineering attempt into a hyper-personalized, contextually aware manipulation that can convince even the most security-conscious individuals. **The U.S. government must prioritize investments in AI-native cybersecurity solutions that detect and neutralize AI-generated threats in real time**.

In other words, the U.S. government must move to the forefront of using good AI to fight bad AI.

Recommendations

1. **Invest in AI-Native Cybersecurity**

"AI-native" refers to security platforms that have been designed from day one with artificial intelligence at the core of its architecture and functionality, rather than as an added feature to legacy technology. We believe that AI-native platforms are the future of cybersecurity, offering a more robust, adaptable, and effective defense against evolving cyber threats.

AI-native platforms will have the following properties:

- The ability to deeply understand the nuances of human communication, including the intent, sentiment, and context of language, allowing for more accurate detection of social engineering tactics used in sophisticated phishing attacks.

- The ability to continuously learn and adapt to new threat patterns in real-time, enabling proactive defense against novel and unknown attacks, including zero-day exploits.

- The ability to analyze vast amounts of data across various sources, including email content, user behavior, and historical attack data, to identify subtle anomalies and indicators of compromise that traditional rule-based cybersecurity systems would miss.

- The ability to automate threat detection and response processes, reducing the burden on security teams and enabling faster, more efficient mitigation of security incidents.

- The ability to provide comprehensive visibility and insights into the threat landscape, empowering security teams to make informed decisions and strengthen their overall security posture.

The power of AI-native cybersecurity has been proven in the commercial sector, but has seen slower adoption in the public sector. A key contributor to the growth of the private sector's strategy in cybersecurity is their willingness to embrace and pilot emerging technologies, empowering these organizations to adequately combat modern adversaries. As a result, this approach continues to put private sector companies in an optimal position to fight cybercrime.

Governments must be empowered to adopt innovative technologies that have otherwise been commercially validated. The U.S. government must now promote the rapid procurement of essential technologies specific to securing the nation's infrastructure and systems against modern AI-driven cyberthreats.

2. Establish a Federal AI Security Task Force

We recommend the establishment of a task force of interdisciplinary professionals with technical AI and cybersecurity expertise to analyze the scope of potential security vulnerabilities of existing government networks and systems. With a dedicated task force, the federal government can better assess and counteract offensive AI threats, integrating expertise from both the private sector and intelligence agencies.

We further recommend expanding the NIST National Cyber Center of Excellence to establish a program to test new and emerging AI security technologies and recommend new requirements in connection with the adoption of AI-native technologies in the government's cybersecurity initiatives.

3. **Increase AI-Driven Threat Intelligence and Information Sharing**

   AI-powered attacks primarily target humans, leveraging social engineering tactics that bypass traditional cybersecurity defenses. The federal government should strengthen intelligence-sharing mechanisms between private cybersecurity firms and national security agencies to facilitate early threat detection and mitigation.

Conclusion

Cybersecurity remains a cornerstone of national security, and the proliferation of AI has rapidly shifted the cybersecurity battlefield, creating a high-stakes and rapidly evolving competition between good AI and bad AI.

AI attacks operate at machine speed, overwhelming conventional defenses and exploiting human vulnerability. The rise of these AI-driven cyber threats necessitates a paradigm shift in cybersecurity strategy.

The U.S. must act decisively to harness the defensive potential of AI. By investing in AI-native cybersecurity, the U.S. government can ensure that AI strengthens American security and economic resilience.

Abnormal Security appreciates the opportunity to contribute to this critical discussion and stands ready to support OSTP in the development and implementation of a national AI security strategy.