FLASHPOINT

June 10, 2025

The Honorable James Comer
Chair
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, DC. 20515

The Honorable Stephen Lynch
Ranking Member
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Nancy Mace
Chair
Subcommittee on Cybersecurity, Information Technology and Government Innovation
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

RE: Statement for the Record by Flashpoint – Hearing on "The Federal Government in the Age of Artificial Intelligence" – June 5, 2025

Dear Chair Comer/Chair Mace/Ranking Member Lynch:

Flashpoint thanks you for the opportunity to submit comments for the record relating to the Federal Government in the Age of Artificial Intelligence. Flashpoint is the world's largest private threat intelligence firm, providing public and private sector companies with accurate, timely, and thorough open-source cyber threat intelligence. The company combines human-powered data collection and intelligence with intuitive technology to help the world's leading organizations protect people, places, and assets.

As members of this Committee have properly noted, the use of artificial intelligence (AI) by businesses and governments alike is fully underway. AI of course brings with it enormous potential for exponential leaps forward in efficiency and effectiveness. With regard to the Federal Government this can and should mean material improvements in the provision of services, fraud reduction efforts, and of course increasing our national security.

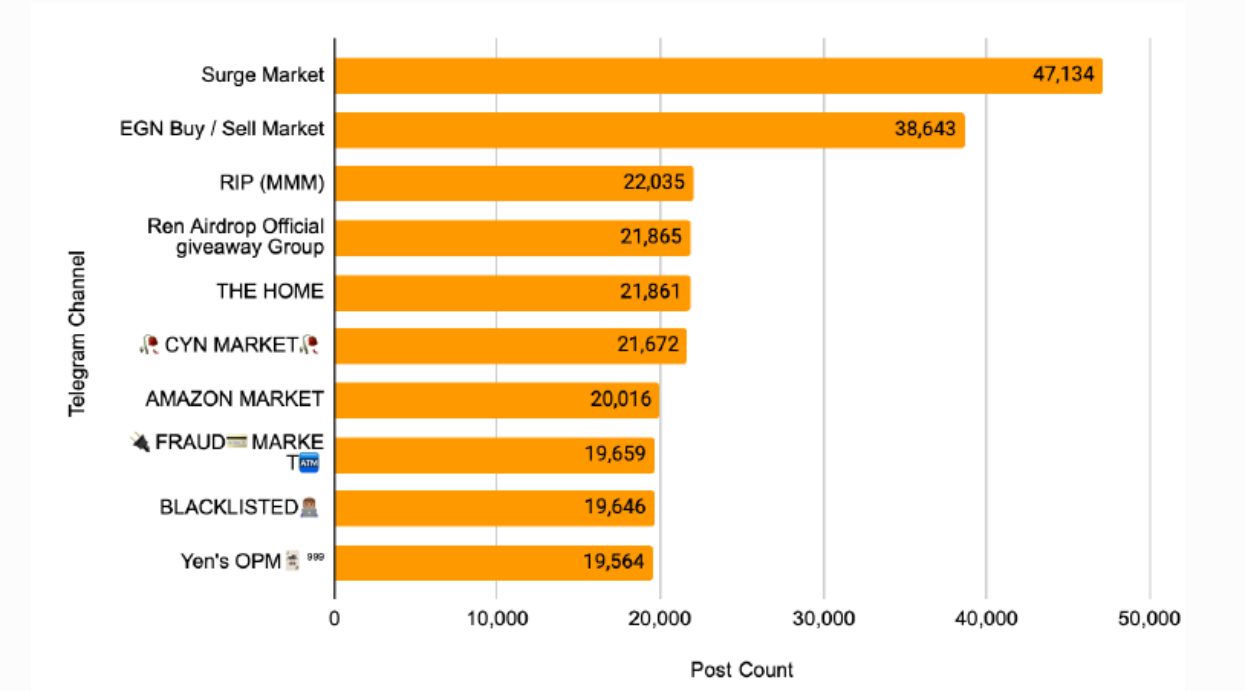
The U.S. Federal Government however is not the only entity that has plans to utilize AI systems. American adversaries, whether nation states or individual criminals,

unfortunately have also recognized the massive potential leaps in effectiveness associated with AI tools – in their case potentially massive improvements in the ability to conduct damaging cyberattacks and steal information.

Flashpoint would like to take this opportunity to share with the Committee for the record recent threat intelligence it has discovered that illustrates the high degree to which threat actors are engaged in both utilizing AI for nefarious activity as well as their efforts being undertaken to hack/corrupt AI systems, including large language models (LLMs).

As one example Flashpoint is now seeing well over 500,000 unique posts in online forums frequented by cybercriminals/hackers that advertise the ability to use AI as part of hacking operations or exchanging information how to do so. Unfortunately such advertisements/knowledge exchanges are increasing, not decreasing, on a monthly basis, and are being shared on (but not limited to) sites and messaging services such as Telegram, GitHub, Reddit, Mastodon, Discord, and others.

Of particular interest to the Committee should be the fact that one of the most popular techniques/capabilities being shared by threat actors online is how to use AI to bypass know-your-customer (KYC) controls using generative AI such as deepfake technology. In April 2025 along over 466,000 such posts were spotted on Telegram alone:



Top 10 Telegram channels advertising KYC bypasses using AI in April 2025

FLASHPOINT

Another area of intense focus for threat actors are the previously mentioned LLMs. By way of review, LLMs are AI programs that can perform language processing tasks by learning from data input and ingestion. LLMs can generate text, images, videos, and code based on text or audio input from users. Threat actors have been observed creating their own LLMs or bypassing safeguards for other LLMs. Using malicious LLMs allows threat actors to generate phishing links and pages, create harmful code, or generate offensive text and media.

As LLMs become more integrated into everyday technology, threat actors are developing tactics to bypass safeguards in LLMs, such as ChatGPT and Gemini, and perform illicit prompts. This tactic is known as "jailbreaking." Threat actors may identify vulnerabilities in an AI or LLM model so that they can remove the model's safeguards.

Threat actors may also conduct a "roleplay" scenario in which they instruct AI models to bypass restrictions or safeguards that were installed into the model. Threat actors may leverage a prompt injection tool called DAN ("Do Anything Now") that requests an AI model to roleplay as a malicious AI model called DAN. Interest in jailbreaking LLMs appears to be intense: in April 2025 alone Flashpoint analysts identified well over 2.3 million posts advertising, discussing, and referencing jailbreaks for LLMs.

As the Committee can imagine, the above represents only a small portion of the threats and efforts being undertaken by threat actors related to AI. Flashpoint wanted to bring these threats to the attention of the Committee in order to highlight the need for rigorous security controls and governance programs as the Federal Government moves ahead in using AI. Properly utilizing AI will be an obvious boon for the American taxpayer, and Flashpoint stands by to lend its expertise to the Committee and the Federal Government writ large in helping make that successful outcome occur.

Respectfully submitted,

Andrew Borene
Executive Director of International Markets and Global Security
Flashpoint