EXTRAHOP

AI in Federal Government

How RevealX™ Helps Agencies Comply with Executive Order 13960

On December 3, 2020, the White House issued **Executive Order 13960**, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government." This order laid out policies and principles that government agencies should follow when implementing artificial intelligence (AI). Specifically, the order requires federal agencies to conduct annual inventories of the AI tools they use and share these inventories with other agencies and with the public. The goal of the order: to promote responsible use of AI and foster public trust in these systems.

Since the Executive Order was announced, use of AI as a service (AIaaS) has exploded, thanks in large part to the release of ChatGPT in November 2022. The instant popularity of ChatGPT and other generative AI tools renewed public concerns over security, privacy, and bias in these systems and their impact on jobs. It also prompted the White House to further define American policy toward AI via a **Blueprint for an AI Bill of Rights**.

Both the Blueprint and the Executive Order call for the ability to continuously monitor AI tools for safety and effectiveness. The Executive Order further calls on federal agencies to implement and enforce "appropriate safeguards" for ensuring "the proper use and functioning of their applications of AI" and to monitor, audit, and document compliance with those safeguards. If an agency finds, during the course of its testing and monitoring, that AI applications demonstrate performance or outcomes inconsistent with their intended use or the democratic principles underlying the executive order, the agency must have mechanisms in place to "supersede, disengage, or deactivate" those AI applications.

A Single Solution for AI Inventory and Monitoring

As noted above, federal regulations require agencies to inventory and monitor the ways they use AI tools. However, some AI use cases are exempt from inventory on the grounds of privacy or the sensitive nature of the data involved, such as law enforcement or national security information. The EO does not exempt these use cases from monitoring; in fact, they will require more intense scrutiny than other applications, as data leaks could be catastrophic to public safety or national security.

To help federal agencies inventory and monitor their AI applications in compliance with the EO, RevealX provided comprehensive visibility into employee usage of ChatGPT and other public generative AI tools, including DALL-E, GitHub Copilot, and Google Gemini, as well as into all applications, assets, and endpoints connecting to and communicating with agency networks. Through its Threat Briefing for Generative AI, RevealX provides customers with visibility into the devices and users on their networks that are connecting to AIaaS domains.

This capability is essential as federal agencies move quickly to adopt policies governing the use of large language models and generative AI tools, since it will give them a mechanism to audit compliance with those policies. ExtraHop is taking this step as part of a larger security platform approach, incorporating the AIaaS monitoring with our existing, industry-leading network detection and response (NDR) capabilities.

By tracking which devices are connecting to AIaaS domains, identifying the users associated with those devices, and the amount of data those devices are sending to those domains, RevealX enables organizations to assess the risk associated with employees' ongoing use of ChatGPT and other AIaaS tools, like the leakage of personal data or national secrets.

In addition, because RevealX shows the amount of data being sent to and received from these domains, federal agency security leaders can evaluate what falls within an acceptable range and what indicates a potential data leak. For example, simple user queries to a chatbot should fall within a range of bytes to kilobytes. If security teams see MBs of data flowing to these domains, that volume may signify employees are sending sensitive or protected data with their query. Federal agencies will be able to identify the type of data and individual files that employees are sending to AIaaS domains if the traffic in question is not encrypted and RevealX is able to identify related data exfiltration and data staging detections.

Network Telemetry: Key to Exposing Data Leaks

RevealX is able to provide this deep visibility and real-time detection because ExtraHop uses network packets as the primary data source for monitoring and analysis. Using a real-time stream processor, RevealX transforms unstructured packets into structured wire data and uses AI and machine learning to analyze payloads and content from OSI Layers 2–7 for complete network visibility. From device discovery to machine-learning-powered behavioral analysis, network telemetry is the immutable source of truth for understanding an organization's hybrid environment. Logs can tell you that two devices talked to each other, but RevealX provides rich context about the communication.

At ExtraHop, we can't underscore the importance of this capability enough as organizations grapple with the popularity and proliferation of AIaaS and the data leakage risk associated with it. ExtraHop believes the productivity benefits of these tools outweigh the risks, provided organizations and employees understand how these services will use their data (and how long they'll retain it), and provided organizations not only implement policies governing use of these services but also have a control like RevealX in place that allows them to assess policy compliance and spot risks in real time.

See It in Action

See how RevealX can help your agency assess the scope of data leaks and generative AI use in your agency.

Schedule a Personalized Demo

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at extrahop.com.

EXTRAHOP®

info@extrahop.com
extrahop.com