

U.S. Federal Agency Adopts GenAI Responsibly, Achieving Maximum Benefit with Minimum Security Risk

Challenge

A U.S. federal agency, tasked with administering lawful immigration, was challenged by the need to utilize Generative AI (GenAI) tools in their daily operations without exposing the agency to Large Language Model (LLM)-related cyber risks or misinformation. Additionally, the agency sought to empower employees to leverage GenAI tools to enhance efficiency in tasks such as analyzing large datasets, drafting policy documents, and streamlining inter-agency communication but with sufficient guardrails.

Solution

As an agency involved in our nation's homeland security, the necessity for secure use of GenAI tools was paramount. A long time customer of Swish, the agency reached out for recommendations. Swish highly recommended Lasso for Applications and Lasso for GenAI Chatbots, from Lasso Security to ensure:

- Immediate response and blocking to protect classified or sensitive information.
- Real-time threat detection to block unauthorized access, risky behavior, misinformation, as well as prevention of external cyber attack attempts.
- Context-based access control limiting GenAI interactions to authorized users.
- Comprehensive audit trails to monitor and log all GenAI interactions for compliance and incident response.



“GenAI is enabling automation in phishing, deepfake creation and other sophisticated exploits and is increasing in scale. While 66% of organizations recognize AI’s transformative potential, only 37% have processes in place to assess the security of AI tools before deployment.”

World Economic Forum’s Global Cybersecurity Outlook 2025

Outcomes

By deploying Lasso, the agency was able to enhance the security and monitoring of its LLM-based solution. This allowed employees to fully leverage GenAI chatbots while preventing data leakage. Additionally, it enabled the development of GenAI-powered chatbot services designed for internal and external use. These services were equipped with robust defenses against data breaches, malicious manipulation, and other LLM-related attack vectors as well as supporting agency governance and use policy. Through this approach, the customer adopted GenAI responsibly, achieving maximum benefit while minimizing security risks.

The Trusted Choice for Securing GenAI in Government Operations

Government agencies are under immense pressure to protect critical information, prevent risks, and maintain strict control over sensitive outputs and inputs. With the rapid adoption of Generative AI (GenAI), these challenges have become more complex, requiring advanced solutions to mitigate potential vulnerabilities without hindering innovation.

Lasso's solutions are purpose-built to address these needs, enabling agencies to adopt GenAI tools securely and confidently. The platform provides robust safeguards against data leakage, malicious manipulation, and unauthorized access, ensuring compliance with all governance standards. Whether it's through real-time monitoring, tailored access controls, or proactive risk mitigation, Lasso empowers agencies to leverage the transformative potential of GenAI while maintaining the highest levels of security and trust.



Lasso Security is a GenAI security platform that enhances security posture by autonomously monitoring all GenAI interactions, detecting risks in real-time, and enabling organizations to effortlessly safeguard their GenAI activities. Lasso is on a mission to empower organizations to confidently adopt GenAI without compromising on security or performance.

To learn more, please visit:
www.lasso.security



Swish is a provider of technology solutions and engineering services to the U.S. Federal Government with a focus on high-quality outcomes for customers. Since 2006, Swish has delivered high-performance solutions and services to the Federal Government market ensuring that customer's digital service capabilities, performance, and security exceed expectations and requirements. Swish is a Service-Disabled, Veteran-Owned and HUBZone certified Small Business.

www.swishdata.com

1420 Spring Hill Road Suite 320 McLean, VA 22102

P 703.635.3324 / E info@swishdata.com