# How ZeroTrusted.ai Meets the Requirements of OMB Memorandum M-24-18

**Waylon Krush**
**CEO of ZeroTrusted.ai**

**October 7, 2024**

ZEROTRUSTED.AI

# INTRODUCTION

On September 24, 2024, the Office of Management and Budget (OMB) issued Memorandum M-24-18, titled Advancing the Responsible Acquisition of Artificial Intelligence in Government. The directive aims to enhance federal agencies' AI capabilities while emphasizing responsible acquisition practices that address AI's unique risks. By setting guidelines for cross-functional collaboration, risk management, and fostering a competitive AI market, M-24-18 advances the broader objectives of the Advancing American AI Act and Executive Order 14110.

ZeroTrusted.ai is a AI cybersecurity company dedicated to securing AI systems with a focus on privacy, security, and reliability. Led by CEO Waylon Krush and CTO Femi Fashakin, ZeroTrusted.ai brings over 25 years of experience in cybersecurity, AI ansd secure system development and is committed to supporting government agencies in meeting the standards set forth in M-24-18. With solutions such as AI Health Check and AI Governance System (AGS), ZeroTrusted.ai ensures agencies' AI systems adhere to rigorous risk management, data privacy, and performance standards.

## 1. Ensuring Cross-Functional and Interagency Collaboration

### M-24-18 Requirements:

Agencies must establish and update acquisition policies to promote cross-functional collaboration throughout the AI acquisition lifecycle. This includes ensuring agency-wide alignment with OMB M-24-10 and fostering information sharing across the executive branch.

### How ZeroTrusted.ai Aligns:

ZeroTrusted.ai's AI Governance System (AGS) enables federal agencies to implement robust oversight and control over AI acquisition and usage. AGS integrates with agency governance frameworks, facilitating collaboration across acquisition, IT, legal, and privacy teams to address the unique challenges of AI. ZeroTrusted.ai also supports secure information sharing, ensuring consistent risk management across the government AI ecosystem.

## 2. Managing AI Risks and Performance

### M-24-18 Requirements:

Agencies are directed to adopt risk management practices for AI that address privacy, security, data ownership, and interoperability. M-24-18 supplements existing requirements, establishing practices for managing risks associated with generative AI, AI-enabled biometrics, and rights-impacting AI.

### How ZeroTrusted.ai Aligns:

ZeroTrusted.ai's AI Health Check provides ongoing monitoring of AI systems to ensure compliance with security, reliability, and privacy standards. By continuously assessing AI models, including LLMs, SLMs, and AI-enabled biometric systems, AI Health Check proactively identifies vulnerabilities, mitigating risks before they impact agency operations.

Additionally, ZeroTrusted.ai's solutions emphasize data sovereignty and interoperability, aligning with OMB's emphasis on preventing vendor lock-in. Agencies can deploy ZeroTrusted.ai across Azure, AWS, and air-gapped environments, ensuring flexibility and compliance with federal standards.

## 3. Promoting a Competitive AI Market with Innovative Acquisition

### M-24-18 Requirements:

M-24-18 encourages agencies to promote a diverse and competitive AI marketplace. This includes prioritizing interoperability and adopting innovative acquisition practices to prevent vendor lock-in and ensure ongoing access to the best AI solutions.

### How ZeroTrusted.ai Aligns:

ZeroTrusted.ai enables AI data portability and ensures that agencies retain ownership of fine-tuning data and AI configurations, reducing vendor dependency. By adhering to open standards and offering API-based integrations, ZeroTrusted.ai ensures that agencies can maintain interoperability across diverse AI systems, supporting a competitive federal marketplace.

ZeroTrusted.ai's AI Governance System (AGS) further enables agencies to standardize AI acquisition practices, allowing seamless transition between vendors and preventing long-term dependency on proprietary solutions.

## 4. Supporting Privacy, Civil Rights, and Civil Liberties

### M-24-18 Requirements:

M-24-18 mandates that agencies address privacy risks associated with AI acquisition and ensure that rights-impacting AI does not result in unlawful discrimination. Privacy programs must be involved in the AI acquisition lifecycle, and vendors should protect personally identifiable information (PII).

### How ZeroTrusted.ai Aligns:

Privacy is central to ZeroTrusted.ai's mission. The platform implements advanced encryption and anonymization to protect sensitive data, including PII and PHI, at every stage of the AI lifecycle. ZeroTrusted.ai complies with GDPR, HIPAA, and CCPA, ensuring that federal agencies meet stringent privacy standards.

Through ZeroTrusted.ai's algorithmic bias assessments and disparity testing, agencies can ensure that their AI systems operate fairly, addressing potential biases that could lead to discrimination. This supports agencies in meeting M-24-18's goal of ensuring equitable AI deployment.

## 5. Ensuring Human Alternatives, Consideration, and Fallback

### M-24-18 Requirements:

The memorandum requires agencies to provide human alternatives and enable individuals to contest decisions made by AI systems. This ensures that automated decisions impacting individuals' rights can be reviewed by human operators.

### How ZeroTrusted.ai Aligns:

ZeroTrusted.ai's Zero Trust Architecture supports agencies in offering human oversight for AI-driven decisions. Through its governance framework, ZeroTrusted.ai allows agencies to incorporate human review processes into AI workflows, ensuring transparency and accountability in decision-making.

ZeroTrusted.ai's solutions are designed with built-in escalation processes, allowing timely human intervention in high-risk scenarios, especially in sensitive domains such as healthcare, employment, and law enforcement. It also provides a feedback loop where users can rate data along with an AI judge to ensure consensus across multiple different types of AI and AI Agents.

## 6. Leveraging Innovative Practices for Risk Management

### M-24-18 Requirements:

The memorandum emphasizes performance-based acquisition techniques, requiring agencies to implement risk management practices that ensure AI performance and safety. Agencies are also encouraged to adopt innovative practices to meet federal AI acquisition standards.

### How ZeroTrusted.ai Aligns:

ZeroTrusted.ai's AI Health Check offers real-time performance tracking and risk assessments to ensure AI systems meet performance standards. The platform's modular design allows agencies to leverage the latest AI innovations, enhancing scalability and adaptability. It conducts a deep enumeration and ongoing baselines identifying anomalies, data drift, data drift, and security and privacy relevant issues.

ZeroTrusted.ai's Comprehensive Logging and Incident Reporting support transparent risk management, allowing agencies to document AI performance and identify areas for improvement. This aligns with OMB's goal of utilizing data-driven approaches to assess and mitigate AI risks.

## Conclusion

ZeroTrusted.ai is uniquely positioned to help federal agencies comply with OMB Memorandum M-24-18 and advance responsible AI acquisition. By focusing on cross-functional collaboration, privacy protection, risk management, and interoperability, ZeroTrusted.ai supports the responsible acquisition of AI systems, ensuring they are secure, effective, and aligned with federal standards.

For more information on how ZeroTrusted.ai can support your agency in meeting OMB M-24-18 requirements, please contact us at contact@zerotrusted.ai or visit our website at www.zerotrusted.ai.