Kiteworks

COMPLIANCE BRIEF

Advancing Secure AI Development With White House AI Memorandum

Kiteworks' Private Infrastructure and FedRAMP-authorized Content Security for AI Development and Communications

President Biden's October 24, 2024 memorandum outlines a comprehensive strategy for U.S. leadership in artificial intelligence (AI) development and national security. The directive impacts all U.S.-based organizations developing or deploying frontier AI models, with specific attention to those creating dual-use applications that could affect national security. While the memorandum focuses primarily on government agencies, it establishes voluntary testing and safety protocols for private sector AI companies through NIST's AI Safety Institute (AISI). Organizations can begin participation in voluntary pre-deployment testing immediately, though specific guidance from AISI will roll out over the next 180 days. Though the memo does not mandate private sector compliance, it signals likely future regulations and emphasizes the U.S. government's commitment to partnering only with organizations that prioritize AI safety and security. Kiteworks' secure content communications platform enables organizations to meet the memo's data security, privacy, and governance requirements through its comprehensive private infrastructure and granular controls.

AI Talent & Infrastructure Development Supported With Private Infrastructure and Automated Compliance Reporting

The U.S. government's AI talent acquisition and infrastructure development initiatives require secure data sharing and collaboration across multiple federal agencies, private organizations, and international partners. These requirements include protecting sensitive visa applicant data, safeguarding economic assessments of the AI ecosystem, and securing the distribution of computational resources through the National Artificial Intelligence Research Resource (NAIRR) pilot project. Kiteworks supports these mandates through its private infrastructure that enables secure content communications between agencies and stakeholders. The platform's FedRAMP-authorized secure file sharing system ensures confidential distribution of sensitive talent acquisition documents. The platform's automated compliance reporting generates detailed activity logs and governance records, helping agencies track and monitor all content communications and maintain regulatory compliance.

Solution Highlights

- FedRAMP Moderate Authorized
- Strong encryption
- Automated audit logs
- Granular access controls
- Role-based permissions
- Workflow automation

AI Safety Testing & Evaluation With Secure File Transfer and Access Controls

The memorandum outlines extensive requirements for AI safety testing, evaluation, and cross-agency collaboration, with NIST's AI Safety Institute (AISI) serving as the primary contact for private sector AI testing. Key mandates include facilitating voluntary pre- and post-deployment testing of frontier AI models, sharing safety test results within 30 days, and secure communication of findings to model developers. Kiteworks enables secure transfer of AI models and test data between AISI and AI developers through its unified secure transfer protocols. The platform's granular access controls ensure only authorized personnel can access sensitive test results and findings. Kiteworks' end-to-end encryption protects data both in transit and at rest, maintaining security during inter-agency and public-private collaborations.

AI Policy & International Collaboration via Cross-border Data Governance and Secure Content Communications

The memorandum establishes comprehensive requirements for AI policy development, workforce training, and international collaboration. Federal agencies must revise hiring policies, create AI training programs, and develop frameworks for responsible AI governance within strict timelines. Cross-border partnerships and co-development initiatives with allies demand secure international data sharing capabilities. Kiteworks supports these mandates through its private tenant architecture that maintains data sovereignty during international collaborations. The platform's comprehensive audit logs create immutable records of all document access and modifications. Kiteworks' secure messaging system enables protected real-time communication among international partners while maintaining compliance with cross-border data protection regulations.

AI Coordination & Reporting Protected by Workflow Automation and Content Tracking

The memorandum mandates the formation of an AI National Security Coordination Group to harmonize policies and establish talent recruitment strategies across federal agencies. The directive requires specified agency heads to submit annual reports for five years detailing their AI activities and plans, while also creating a National Security AI Executive Talent Committee to develop comprehensive talent acquisition procedures. Kiteworks offers secure report collaboration capabilities that protect sensitive agency reports during preparation and submission. The platform's built-in workflow automation streamlines the review and approval processes for multi-agency documents. Kiteworks' content tracking capabilities create immutable audit logs of document access and modifications, essential for maintaining accountability in collaborative report development. The platform's role-based permissions ensure each agency and committee member accesses only authorized content, while its secure messaging features enable protected real-time discussions among Coordination Group and Committee members.

The White House memorandum establishes a framework for secure AI development, testing, and collaboration that requires robust data protection and governance across federal agencies and private sector partners. Kiteworks delivers a comprehensive secure content communications platform that addresses requirements through multiple integrated capabilities. The platform's private infrastructure and FedRAMP Moderate Authorization provide the foundation for protecting sensitive AI models, test data, and policy documents. Kiteworks enables agencies and organizations to maintain data sovereignty while sharing critical information across organizational and national boundaries. From talent acquisition to international collaboration, the platform's security features ensure compliance with the memorandum's data protection mandates while facilitating essential cooperation between government agencies, private AI developers, and international partners.