Kiteworks

COMPLIANCE BRIEF

Complying With White House Memo for Administration Cybersecurity Priorities for the FY 2025 Budget

Kiteworks helps federal agencies meet cybersecurity priorities for zero-trust adoption, secure software procurement, and modernized defenses

Memorandum M-23-18, titled "Administration Cybersecurity Priorities for the FY 2025 Budget," is a memorandum issued by the Office of Management and Budget (OMB) that outlines the United States government's strategic approach to cybersecurity and its investment priorities for the upcoming fiscal year. The memo was released on June 27, 2023, and emphasizes departments and agencies should prioritize five cybersecurity effort areas: Defend Critical Infrastructure; Disrupt and Dismantle Threat Actors; Shape Market Forces to Drive Security and Resilience; Invest in a Resilient Future; and Forge International Partnerships to Pursue Shared Goals to remain consistent with the five pillars of the National Cybersecurity Strategy. The memo provides guidance to federal agencies on how to prioritize their cybersecurity investments and align their efforts with the government's broader cybersecurity strategy. The memo also highlights the importance of cross-agency collaboration and information sharing in the fight against cyber threats. The Kiteworks-enabled Private Content Network (PCN) can help federal agencies achieve some objectives outlined in the memo by providing a secure and compliant platform for sharing sensitive information, and by establishing secure software development.

Modernize Federal Defenses With the Zero-trust Security Model

To comply with the cybersecurity guidance in White House memo M-23-18, federal agencies must modernize defenses and budget submissions to achieve progress on zero-trust architecture deployment. Agencies should explain efforts to meet zero-trust maturity model goals, close gaps in zero-trust requirements, and prioritize upgrading legacy systems, especially FISMA high-value assets, to meet modern security and functionality standards. As directed, agencies must continue strengthening national security systems, leveraging shared services where appropriate to fill capability gaps, and building federal cybersecurity unity. Following this memo will improve the cybersecurity of sensitive government systems through upgraded technology, zero-trust architecture adoption, and unified modernization efforts across agencies.

The Kiteworks-enabled Private Content Network (PCN) can assist federal agencies in meeting the modernized cyber defense requirements outlined in memo M-23-18. Kiteworks enables a zero-trust environment with role-based access controls to sensitive content. Integration with enterprise identity providers supports least-privilege access controls including SSO, MFA, Active Directory/LDAP, and SAML 2.0, allowing organizations to leverage their existing identity management infrastructure.

Solution Highlights

Robust access controls

Anomaly detection

Encryption at rest and in transit

Secure software development

FedRAMP Authorized deployment

Robust DRM, encryption, and watermarking safeguard content to protect sensitive files, control access and usage, and deter unauthorized sharing. Real-time alerts detect abnormal activity. Kiteworks is also FedRAMP Moderate Authorized and is authorized to provide cloud services to federal agencies. These measures work together to provide a robust defense against a wide range of cybersecurity threats.

Secure Software With Kiteworks' SSP Best Practices

To comply with memo M-23-18, agencies must budget to fully implement OMB memo M-23-18 and forthcoming Federal Acquisition Regulation changes under EO 14028. This includes contracting staff and training to enforce new software producer attestations to using secure development practices. Budgets should cover meeting enhanced cybersecurity acquisition standards agency-wide and pilot innovative procurement methods where needed. Adopting regulated secure software practices and updated procurement requirements will improve supply chain security and contractor accountability.

Kiteworks was built using secure software development best practices that align with memo M-23-18 guidance. Kiteworks enforces least-privilege access, defense in-depth, secure-by-default settings, input/output validation, versioning, and industry standards like OWASP and CIS benchmarks. Multiple security layers like role-based access, encryption, security reviews, penetration testing, and automated QA defend against threats. Secure coding and validating all inputs/outputs prevent code injection and data loss. Versioning retains file integrity and access to the latest updates. Following these software development and operational principles makes Kiteworks measurably more secure and accountable than the competition. This reduces supply chain risk and meets the enhanced security requirements for federal procurement and software producers outlined in the memo.

White House memo M-23-18 outlines cybersecurity priorities for federal agencies' 2025 budget submissions. It directs modernizing defenses via zero-trust architecture adoption, meeting new secure software requirements, and updating procurement regulations. Compliance requires budgeting for zero-trust deployment, upgrading legacy systems, strengthening national security systems, leveraging shared services, and unifying efforts. It also necessitates enforcing developer attestations to using secure coding practices, piloting innovative procurement methods, and adopting enterprise solutions. Kiteworks can assist agencies in complying by enabling zero-trust environments with robust access controls, encryption, and anomaly detection. Kiteworks is also built using industry-leading secure software best practices for access controls, validation, and security testing. This aligns with memo guidance on reducing risk and enhancing accountability.