Kiteworks

COMPLIANCE BRIEF

Kiteworks Addresses UK Defence Standard 05-138

Support for the MOD Supply Chain With Strong Double Encryption, MFA Controls, and Real-Time Monitoring

Solution Highlights

FIPS 140-3
validated encryption

Double
encryption at rest

Multi-factor authentication
with PIV/CAC cards

SCIM 2.0
identity management

Real-time
SIEM integration

Embedded Managed
Detection and Response

Introduction

The United Kingdom Ministry of Defence published Defence Standard 05-138 Issue 4 on 14 May 2024, establishing comprehensive cybersecurity requirements for all defence suppliers managing government data. Organizations providing goods or services to the Ministry of Defence must comply with this standard from 3 December 2025 for all new Risk Assessments and Supplier Assurance Questionnaires under contracts containing DEFCON 658, as mandated by Industry Security Notice 2025/07. Defence Standard 05-138 builds on the UK government's Cyber Essentials scheme as its universal baseline, requiring Cyber Essentials certification at every risk level and Cyber Essentials Plus certification for suppliers operating at Level 2 (Advanced) and Level 3 (Expert). Kiteworks holds Cyber Essentials Plus certification, meeting the independent technical verification standard required of the highest-risk defence suppliers. The standard implements four tiers: Level 0 (3 controls), Level 1 (101 controls), Level 2 (139 controls), and Level 3 (144 controls), with Cyber Essentials Plus required from Level 2 upward. Kiteworks supports organizations working toward compliance with Defence Standard 05-138. Here's how:

Hardened Security Controls Through Approved Cryptography

Defence Standard 05-138 requires suppliers to implement nationally approved cryptographic methods including FIPS 140-2 or comparable standards through Control IDs 2318 and 2319, while Control IDs 2300, 2302, and 2308 mandate comprehensive protection of data at rest and in transit. The Kiteworks platform provides FIPS 140-3 validated encryption (certificate #4980) for organizations requiring government-grade cryptography. Files undergo double encryption at rest using AES-256, with customer-owned encryption keys ensuring that neither Kiteworks staff nor external actors can decrypt private data. The platform integrates with Hardware Security Modules including Thales Luna Network HSM, Entrust nShield HSM, and AWS Key Management Service to enable key management outside the Kiteworks appliances. For data in transit, Kiteworks

enforces TLS 1.2+ with AES-256 by default, while the TLS Certificate Validation feature automatically validates certificates to prevent man-in-the-middle attacks. This multi-layered encryption approach, combined with customer key ownership and external HSM integration, enables defence suppliers to meet the standard's stringent requirements for protecting sensitive government information across all data states.

Multi-Factor Authentication and Identity Management for Defence Networks

Control IDs 2200-2218 establish comprehensive identity and access management requirements, with specific mandates for multi-factor authentication (Control ID 2201) and automated password management (Control IDs 2211-2213). Kiteworks implements multiple authentication methods simultaneously within a single system, supporting RADIUS protocol, PIV/CAC cards used by U.S. Department of War personnel, native email-based one-time passwords, SMS-based OTP, and time-based OTP following RFC 6238 standard. The platform's SCIM 2.0 compliance enables centralized account management through any external Identity Management solution, while LDAP and Active Directory integration provides automatic user onboarding, offboarding, and role updates. For privileged user management required by Control ID 2203, Kiteworks provides multiple default admin roles with configurable separation of duties, enabling organizations to implement least-privilege principles mandated by Control ID 2205. The platform enforces configurable password policies covering minimum length, complexity requirements, history tracking, and expiration, while encrypted authentication tokens and replay-resistant mechanisms protect against sophisticated attacks. This comprehensive identity infrastructure enables defence suppliers to meet the standard's stringent requirements for controlling access to sensitive systems and data.

Continuous Monitoring and Threat Detection

Control IDs 3100-3110 mandate comprehensive security monitoring capabilities, while Control IDs 3200-3204 require proactive threat discovery and response. Kiteworks maintains comprehensive audit logs that capture all security and compliance-related activities, automatically cleaning, normalizing, and aggregating data into a single stream. The platform feeds real-time audit data to external SIEM systems including QRadar, LogRhythm, ArcSight, and Splunk via syslog, enabling 24×7×365 monitoring required at Level 3 by Control ID 3102. The embedded Managed Detection and Response capability connects to Kiteworks' security staff, automatically pushing WAF rule updates to Kiteworks systems worldwide when vulnerabilities are detected. AI-based intrusion and anomaly detection maintains an evolving library of patterns to identify suspicious network traffic, known attack signatures, exfiltration attempts, and unauthorized code changes. The platform integrates with advanced threat prevention solutions via ICAP protocol, supporting Trellix ATP products and Check Point Harmony Endpoint through native APIs. Kiteworks undergoes continuous automated and periodic manual penetration testing against its platform, supplemented by white and black box bounty programs and annual third-party vulnerability assessments, supporting suppliers' own obligations under Control ID 4105. The CISO Dashboard delivers real-time visualization of file activity across email, file shares, SFTP, and MFT.

Kiteworks provides defence suppliers with the technical capabilities to meet many Defence Standard 05-138's protection requirements through FIPS 140-3 validated encryption, double encryption at rest, and customer-owned keys integrated with external Hardware Security Modules. The platform addresses the standard's identity control mandates by implementing multi-factor authentication with PIV/CAC cards, SCIM 2.0 compliance for automated account management, and eight preconfigured admin roles enabling separation of duties. For continuous monitoring obligations, Kiteworks delivers real-time SIEM integration, AI-based anomaly detection, and Embedded Managed Detection and Response that connects to security staff for proactive threat mitigation. By consolidating these capabilities within a FedRAMP-authorized platform, Kiteworks helps defence organizations demonstrate compliance with the standard's technical controls while maintaining operational efficiency in their secure collaboration with the Ministry of Defence.