Kiteworks

COMPLIANCE BRIEF

Empowering Compliance With the DoD's Defense Industrial Base Cybersecurity Strategy 2024

Leverage Kiteworks' Robust Security Features and Industry Certifications to Strengthen Cybersecurity Posture and Resilience

The DoD's Defense Industrial Base Cybersecurity Strategy 2024 outlines a comprehensive approach to bolster the cybersecurity and resiliency of the DIB, a critical component of national security. The strategy's four goals aim to strengthen governance, enhance cybersecurity posture, preserve resiliency, and improve collaboration. Compliance with cybersecurity requirements is essential to safeguard sensitive information, maintain technological advantages, and ensure the reliability of critical capabilities. By protecting the DIB from increasing cyber threats, the strategy supports the global competitiveness of the U.S. defense industry and the integrity of the supply chain. Successful implementation will require close coordination within the DoD and robust engagement with the DIB to drive continuous improvement and adapt to the evolving threat landscape, ultimately contributing to a more secure and resilient global defense ecosystem. As a trusted provider of secure content collaboration and compliance solutions, Kiteworks is well-positioned to support the Defense Industrial Base (DIB) in achieving the objectives laid out in the Strategy document. Here's how:

Strengthen the DOD Governance Structure for DIB Cybersecurity With Industry Best Practices and Certifications

Goal 1 aims to strengthen the governance structure for DIB cybersecurity by fostering interagency collaboration and developing regulations to evaluate and enforce cybersecurity requirements. The strategy expects DIB contractors and subcontractors to comply with contractually mandated cybersecurity requirements, such as DFARS 252.204-7012, NIST SP 800-171, and CMMC, to ensure the protection of sensitive information and maintain a secure environment. Kiteworks provides a consolidated, normalized audit logging system that enables quick and comprehensive compliance reporting, aligning with the strategy's focus on developing regulations and cybersecurity requirements for DIB contractors and subcontractors. The platform's adherence to the NIST Cybersecurity Framework (CSF), FedRAMP Moderate Authorization, and other industry certifications such as SOC 2, ISO 27001, 27017, and 27018 demonstrates its commitment to best practices and supports the DoD's efforts to establish a secure subcontractor cybersecurity environment.

Solution Highlights

Audit logs and robust reporting

FedRAMP Moderate Authorized

Intrusion and anomaly detection

Hardened virtual appliance

Enhance the Cybersecurity Posture of the DIB by Complying With Industry Standards

Within the Cybersecurity Strategy, Goal 2 focuses on enhancing the cybersecurity posture of the DIB by encouraging the adoption of best practices, certifying compliance with requirements, and identifying vulnerabilities in IT ecosystems. DIB contractors are expected to comply with contractual cybersecurity requirements such as NIST SP 800-171 and participate in programs like CMMC to verify their adherence to these standards. Kiteworks provides a comprehensive security framework that supports compliance with various industry standards, including NIST CSF 2.0, FedRAMP, SOC 2, and ITAR. The platform's extensive audit logging, vulnerability management, and penetration testing capabilities enable DIB contractors to identify and address potential vulnerabilities in their IT systems. Strict adherence to the principle of least privilege, strong double encryption, and automated threat detection and response features support organizations as they maintain a robust cybersecurity posture. By leveraging Kiteworks' security capabilities, DIB contractors can demonstrate compliance with DoD requirements, and protect sensitive information.

Preserve the Resiliency of Critical DIB Capabilities in a Cyber-contested Environment via Hardened Virtual Appliance

The Strategy aims to preserve the resiliency of critical DIB capabilities in a cyber-contested environment, emphasizing the need for increased attention to supply chain vulnerabilities and dependencies within Goal 3. The strategy expects DIB contractors, especially those supporting critical production capabilities and facilities, to prioritize cybersecurity and collaborate with the DoD to assess and mitigate risks. Kiteworks' hardened virtual appliance architecture provides a secure and resilient platform that minimizes the attack surface and protects sensitive content from cyber threats. Multiple layers of protection, including an embedded network firewall, web application firewall, and intrusion detection system, contribute to the overall resilience of the DIB's critical capabilities. Kiteworks' comprehensive audit logging and reporting features enable DIB contractors to demonstrate compliance with industry standards that are essential for maintaining the security and integrity of the defense supply chain.

Improve Cybersecurity Collaboration With the DIB by Utilizing Reporting That Adheres to CSF Functions

Goal 4 emphasizes the importance of improving cybersecurity collaboration with the DIB through streamlined communication, sharing of threat intelligence, and engagement in pilot programs, training, and education initiatives. The strategy expects DIB contractors to actively participate in these collaborative efforts and leverage the resources provided by the DoD to enhance their cybersecurity posture and maintain compliance with requirements. The platform's comprehensive audit logging and reporting capabilities, which adhere to the CSF's functions, enable DIB contractors to quickly and comprehensively prove compliance to auditors and share relevant information with the DoD. Kiteworks' FedRAMP Moderate Authorization, SOC 2, and FIPS 140-2 certifications demonstrate its commitment to meeting the stringent security requirements set forth by the DoD. Robust security features and compliance certifications enable DIB contractors to actively engage in collaborative initiatives.

Kiteworks offers a comprehensive suite of features that directly support compliance with the DoD's Defense Industrial Base Cybersecurity Strategy 2024. The platform's adherence to industry standards, coupled with its robust audit logging, vulnerability management, and hardened virtual appliance architecture, enables DIB contractors to strengthen their cybersecurity posture and demonstrate compliance with DoD requirements. Kiteworks' commitment to best practices, automated threat detection and response capabilities, and strong encryption further bolster the resiliency of critical DIB organizations. By leveraging Kiteworks' secure content collaboration and compliance solutions, DIB contractors can effectively engage in collaborative initiatives, streamline communication, and adapt to the evolving threat landscape, ultimately contributing to a more secure and resilient Defense Industrial Base.