AERSTONE

ICD 503 Compliance

FISMA Compliance for the Intelligence Community

DCID 6/3

The United States Intelligence Community (IC) has a unique set of information security requirements, requiring the highest levels of confidentiality and integrity, coupled with the need to manage access to secure compartmented information based on both clearance level and an established need to know. These requirements have led to the establishment of a common InfoSec policy for all member agencies. Dating back to the 1970s, Director of Central Intelligence Directives (DCIDs) were the primary instrument for defining IC-wide policies. DCID 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," defined a series of policies related to information security. The DCID 6/3 implementation manual specifically defined a series of five "protection levels," each of which delineated the audit requirements for systems operating at increasing levels of confidentiality.

ICD 503

In 2008, the Director of National Intelligence signed IC Directive 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation." ICD 503 replaced DCID 6/3, and is today the relevant guidance for the risk management and certification of information systems across the IC.   This standard specifically requires the IC to use NIST or CNSS standards for security certification assessment and testing. CNSS Policy No. 22, "Policy on Information Assurance Risk Management for National Security Systems," specifically points to FISMA for security audit controls, reinforcing the move to a NIST/FIPS based approach to information security across the IC.

Expert Capabilities

Aerstone's deep subject matter expertise in the area of information security, including risk management and systems auditing, makes us extremely well poised to help IC agencies continue their implementation of ICD 503 requirements, as formerly accredited systems come up for reaccreditation, and as new systems are implemented. Aerstone understands all aspects of FISMA, including the newest requirements specified in the most recent guidance, such as continuous monitoring. Our specific services to support ICD 503 compliance include:

- System risk assessment and management, in accordance with NIST SP 800-37 and NIST SP 800-39
- Security assessment and authorization (SA&A), in accordance with NIST SP 800-53
- FISMA training and process consulting

Our Experience Sets Us Apart

Aerstone approaches each engagement with a combination of professionalism, determination, and creativity honed by years of working with security professionals throughout the military, civil government, and commercial sectors. More than a cybersecurity services vendor, Aerstone develops enduring relationships with clients and helps build long-term value through process improvement.

Contact our sales team at sales@aerstone.com for more information.