

## CREDANT Solutions for FISMA Compliance

A strategic solution is essential for ongoing compliance and data protection.



### CREDANT SOLUTION

*CREDANT Mobile Guardian (CMG) ensures that FISMA encryption and security requirements are consistently and efficiently enforced – regardless of where the data resides.*

#### Only CMG enables organizations to:

- › Encrypt and secure data across multiple, diverse platforms from a single console.
- › Create automatic audit trails that offer proof of end-to-end data security.
- › Provide a transparent end-user interface that supports user productivity while keeping data safe.

*CMG's Intelligent Encryption provides centrally-managed, highly scalable and architecturally flexible security to manage all data endpoints. With CREDANT, organizations can:*

- › Develop a strategic solution for data protection.
- › Encrypt data using FIPS-140-2 compliant algorithms.
- › Ensure data security without the risk of users placing data in areas that are not encrypted.
- › Provide confidentiality, privacy and auditing of data residing on any endpoint.
- › Protect sensitive data from unwarranted access, thus reducing risk of internal breaches.

### Regulatory overview

The Federal Information Security Management Act (FISMA) provides the framework for securing the federal government's information technology. All agencies covered by the Paperwork Reduction Act must implement the requirements of FISMA and report annually to the Office of Management and Budget (OMB) and Congress on the effectiveness of the agency's security programs. The reports must also include independent evaluations by the agency Inspector General.

The National Institute of Standards and Technology (NIST) develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and in managing cost-effective programs to protect their information and information systems.

### The compliance challenge

To promote the development of key security standards and guidelines, FISMA requires federal agencies to:

- › Develop an agency-wide security program, categorizing information and information systems by mission impact.
- › Implement and adhere to security configuration standards developed by NIST.
- › Select appropriate security controls for information systems.
- › Perform ongoing assessment and testing.
- › Conduct annual reviews on the effectiveness of the agency's information security and privacy programs, with results reported to the OMB annually.

Reporting to the OMB is a key element in demonstrating FISMA compliance. The report must contain proper evaluations of the effectiveness of the information security programs, including evidence that the agency has developed a coordinated strategy of addressing security threats.

If an agency implements a technology solution to raise their score in one year, they may score lower the following year if they fail to demonstrate how the solution fits into the agency's overall information security strategy.

### CREDANT

More than 700 enterprises and government agencies -- including 50 of the Global 500 – rely on CREDANT to ensure security compliance, protect their brand and enhance IT and end-user productivity.