

CREDANT Solutions for OMB Directive Compliance

Continued agency funding requires full compliance with OMB security guidelines.



CREDANT SOLUTION

CREDANT Mobile Guardian (CMG) ensures that requirements included in the OMB Directive for encryption and security are consistently and efficiently enforced – regardless of where the data resides.

Only CMG enables organizations to:

- › Encrypt and secure data on laptops and mobile devices 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:

- › 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

In June, 2006, the White House Office of Management and Budget (OMB) issued a Data Security Directive that instructed all federal agencies to comply with specific data security guidelines issued by the National Institute of Standards and Technology (NIST). Compliance with NIST guidelines and the OMB directive requires four specific steps to safeguard Personally Identifiable Information (PII) at remote locations:

- › Confirm identification of PII protection needs.
- › Verify adequacy of organizational policy.
- › Implement protections for PII being transported and/or stored offsite.
- › Implement protections for remote access to PII.

The compliance challenge

The Directive applies to all data contained on laptops and mobile devices that are not specifically classified in writing as “non-sensitive” by a Deputy Secretary or other designated superior. Therefore it defines PII very broadly to include virtually all data that relates to the physical, physiological, mental, economic, cultural, or social identity of a person.

For compliance, agencies must require two forms of authentication to access the information, such as a password and key card system. Government employees must also employ “time-outs” that require the user to re-authenticate every 30 minutes for both remote access and mobile devices. All data downloads must be logged, and sensitive data may remain on a laptop or handheld for a maximum of 90 days, unless specifically permitted for a longer period.

The original Directive required agencies to quickly report all security incidents involving PII. In July, the OMB strengthened the Directive to require agencies to report security incidents within one hour of discovery.

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.