

CREDANT Solutions for Compliance with SB 3671

Personal data on mobile devices must be adequately protected at the government level.



CREDANT SOLUTION

CREDANT Mobile Guardian (CMG) ensures that SB 3671 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 provides centrally-managed, highly scalable and architecturally flexible security to manage all data endpoints. With CREDANT, organizations can:

- › Provide all the necessary audit reports required by SB 3671 policies.
- › Protect data from leaving the organization unprotected on USB flash drives or other forms of removable media.
- › Protect data from unwarranted access, thus reducing risk of internal breaches.

Regulatory overview

Tennessee Senate Bill 3671 mandates a number of rigorous penalties for state and local government entities which fail to safeguard confidential citizen information on laptops and removable storage devices. Failure to comply can result in “a cause of action or claim for damages against the state, municipality, county, public employee or other official.”

The compliance challenge

SB 3671 is similar to a number of data protection regulations in the business world. However, compliance for this bill requires a security solution that recognizes the unique conditions of the government sector.

First of all, a government security solution should include centralized management and enforcement, helping to promote a comprehensive, efficient agency-wide approach to data security. Government organizations can define and enforce data security policies from a single console for all desktops, laptops, handhelds, and removable media such as USB flash drives.

In addition, audit and compliance reporting should be supported by real-time status reports that help IT security personnel prove compliance with regulations like SB 3671. At the same time, a policy-based approach can help ensure that every part of the federal data chain – including people, processes, operations, enforcement, and management - work together to provide a complete solution with no weak links.

Finally, a compliance-ready solution should secure sensitive data on all devices, multiple levels of access, device, and end-user controls, and automatic device detection and communications port controls.

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.