



Mobilizing Governmental Data with Secure USB Flash Drives

to Protect the Privacy and Security of Individuals

SanDisk®



With millions of USB flash drives in use, digital data is constantly on the move. Flash drives let users easily store, transport and share their photos, videos and text files. But when it comes to government agencies, the very same benefits that enable employees to work effectively outside the office pose risks of the loss, theft or misuse of unprotected, confidential data.

The SanDisk® Cruzer® Enterprise USB flash drive provides an unparalleled level of safety and security for sensitive government information and its management.

Combating Data Loss

Today's headlines recount the grim realities of various government and private organizations losing data or having their data compromised. Examples of these accounts include security breaches in the U.S. Department of Veterans Affairs related to lost or stolen portable data devices that have resulted in class action suits on behalf of 28,600,000 veterans.¹

The extremely devastating consequences of data compromise and security breaches are no less severe with smaller but more frequent data losses. Research of data breaches by the Ponemon Institute has established that, on average, a single loss of 30,000 individuals' personally identifiable information can cost an organization nearly \$6 million in internal investigation, notification and regulatory compliance expenses.² Federal agencies have even been held liable in class action suits on behalf of those whose personal information has been compromised. In the private enterprise sector, potential damage resulting from non-compliance to security standards may also result in fines, loss of business and/or legal sanctions.

For government agencies, loss of data or a security breach can pose a national security risk. Because of this, many government agencies are now developing compliance strategies to secure confidential data.

Satisfying All Industry Requirements

Recently, the US government has taken a tougher stance in enforcing security standards for sensitive information. Security measures are being put in place to protect sensitive data, particularly people's identity data, from being lost or stolen. This is a relatively new crime that impacts millions of Americans.

On July 3, 2007, John Grimes, the CIO for the Department of Defense, issued a new policy requiring that all sensitive but unclassified (SBU) data stored on mobile devices be encrypted according to NIST's Federal Information Processing Standard (FIPS) 140-2. The prior year, the Office of Management and Budget issued Memorandum M-06-16, directing all Federal agencies and departments to encrypt all sensitive data on mobile computers and devices.

The challenge that government agencies are facing to secure sensitive data can become daunting when taking into account how much information is transported on personal storage devices. The majority of personal storage devices are neither built to keep data completely secure nor to give government agencies the control they need to audit files being copied or deleted from various networks. Rather than undergo time-consuming data classification exercises in all cases, it is apparent from the recent government policies mentioned below that encryption of data is the best choice for mobile devices.

Central Control, Increased Protection

SanDisk Cruzer Enterprise FIPS Edition USB flash drive with central management and control (CMC) software is designed to meet the requirements of government agencies by complying with regulations such as FISMA and PCI that require secure storage of sensitive information.

CMC is an innovative, client-server software solution that utilizes the unique hardware and embedded software capabilities of SanDisk Cruzer Enterprise FIPS Edition USB flash drives. The CMC device agent resides on the USB flash drive, enabling IT departments to centrally manage company-issued Cruzer Enterprise FIPS Edition USB flash drives – locally and remotely, within and outside the corporate environment.

¹PC World, "Laptop losers hall of shame," Carolyn Duffy Marson, May 26, 2008, <http://www.pcworld.idg.com.au/index.php/id;105254216;img;5220;ssid;1>

²Price Waterhouse Coopers, "Quarterly in law," Feb 2008, p. 3, http://www.pwc.co.uk/pdf/quarter_in_law.pdf

CMC provides many functions such as constant monitoring, auditing and tracking. Depending on an organization's particular needs, these functions can incorporate various parameters set for various levels of restrictions and monitoring.

Attaining centralized deployment and provisioning is another feature with tremendous benefits. IT departments can also deploy centralized updates and configurations of all drive parameters, administer passwords and remotely deactivate lost or stolen drives.

Encryption That Ensures the Ultimate Protection

SanDisk Cruzer Enterprise FIPS Edition USB flash drive uses a number of powerful security features, including: hardware-based 256-bit AES encryption, the most secure block cipher encryption standard adopted to date, complex password protection and a lock-down mechanism. This mechanism is activated when a set number of incorrect password attempts is exceeded in order to ensure that data on lost or stolen drives cannot be hacked into. These security features protect confidential data and at the same time enable authorized employees to transfer data freely, even when sensitive information needs to be transferred to different computers or workstations.

Increasing Productivity

Government agencies do not want to be forced to choose between mobility, ease of use, productivity and security. Complex mobile encryption that is not embraced by users decreases security and hinders worker efficiency. The SanDisk Cruzer Enterprise FIPS Edition USB flash drive, when used with SanDisk CMC software, increases overall enterprise data security by providing centrally managed, secure mobile storage that is transparent to the end user. In this way, both productivity and security remain at high levels.

Privacy Monitoring Throughout the System

The Cruzer Enterprise FIPS Edition USB flash drive, when managed by CMC software, could be set to limit the use of government-issued USB flash drives to only government-owned PCs. It also maintains a full audit trail of files copied, modified or deleted both on and off the network. Protection this thorough is essential not only to meet legal requirements but to provide government agencies with ultimate protection.



In addition, circumventing reliance on users through mandatory 100% data encryption of all files helps prevent human error. The Cruzer Enterprise FIPS Edition flash drive also enables business continuity through seamless backup of drive content and the ability to restore or recreate data resident on lost or stolen drives.



Mobilizing Governmental Data with Secure USB Flash Drives

to Protect the Privacy and Security of Individuals

Key Mandates to Protect Data in the U.S. Government

Federal Information Security Act (FISMA) of 2002

established broad security requirements for U.S. Federal Government agencies and contractors. Encryption controls are required as a result of risk assessments according to NIST guidelines.

OMB Memorandum M-06-16 requires that agencies encrypt all data on mobile devices unless the agency has determined that data to be non-sensitive.

The Department of Defense (DoD) issued tightened policies in July 2007 requiring encryption for sensitive but unclassified data on mobile devices.

FIPS 140-2 establishes cryptographic requirements and defines four increasing robust security levels for encrypting data.

Payment Card Industry / Data Security Standards (PCI/DSS) requires encryption of credit card encryption. (Ver 1.1, Section 3), which applies to several governmental agencies.

Product Highlights

Central Management & Control (CMC) software:

- Manages the complete lifecycle of company-issued USB flash drives
- Protects against unauthorized use of sensitive company data
- Protects against possible regulatory compliance failure and associated damages caused by data breaches due to lost or stolen USB drives
- Supports regulatory compliance by tracking and auditing activity, as well as demonstrating the use of strict encryption measures

SanDisk Corporation

Corporate Headquarters
601 McCarthy Blvd.
Milpitas, CA 95035

For more information,
please visit
www.sandisk.com/enterprise
or email enterprise@sandisk.com

SanDisk and the SanDisk logo are trademarks of SanDisk Corporation, registered in the United States and other countries. TrustedFlash is a trademark of SanDisk Corporation. microSD and SD are trademarks. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).

© 2008 SanDisk Corporation. All rights reserved. xx-xx-xxxx Rev. 2.0, March 2008

SanDisk