



Mobilizing Governmental Data with Secure USB Flash Drives



With millions of USB flash drives in use, digital data is constantly on the move. Flash drives let private 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. In October 2007, removable media containing both personal and financial information for 25 million people was lost by HM Revenue & Customs in the United Kingdom. Experts estimate the value of this data loss at more than €21.9 billion^{1,2}. In January 2008, a stolen mobile device within the United Kingdom Ministry of Defence resulted in the potential exposure of sensitive personal information for more than 600,000 people. The consequences of data breaches are also extremely severe for smaller losses that occur more frequently. Research of data breaches occurring in the United Kingdom during 2007 by the Ponemon Institute has established that an average breach costs nearly €21.8 million³.

Satisfying Industry Requirements

In the private enterprise sector, potential damage resulting from non-compliance to security standards may result in fines, loss of business and/or legal complications.

Government agencies face the much heavier consequence of putting national security at risk. Because of this, many government agencies are now developing compliance strategies to secure their confidential data.

European governments must comply with some of the world's most rigorous data protection laws in order to implement the European Union Data Protection Directive. Although many member country regulations avoid detailed technical requirements, encryption is a leading best practice used to assert data protection and avoid the heavy fines associated with lost or stolen data devices. In January 2008, after the previously mentioned data losses occurred within the UK government, Cabinet Secretary Sir Gus O'Donnell issued a new rule prohibiting civil servants from removing mobile devices containing sensitive information which was not encrypted⁴.

The challenge that government agencies are facing to secure sensitive data can become daunting when taking into account the amount of information that is being transported on personal storage devices. The majority of personal storage devices neither keep data completely secure nor give governments 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, data encryption is becoming the security choice for mobile devices, as apparent from the recent government policies mentioned above.

Central Control, Increased Protection

SanDisk Enterprise offers a comprehensive solution to meet industry standards required for securing mobile storage.

CMC is an innovative, client-server software solution that utilizes the unique hardware and embedded software capabilities of SanDisk Cruzer Enterprise and 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 secure USB flash drives – locally and remotely, within and outside the corporate environment.

CMC provides many functions such as provisioning, centralized deployment, constant monitoring, auditing and tracking. Depending on an organization's particular needs, these functions can incorporate various parameters set for various levels of restrictions. IT departments can also deploy centralized updates and configurations of all drive parameters, administer passwords and remotely deactivate lost or stolen drives.

¹ "UK's Families put on Fraud Alert", BBC, 20 November 2007

² "UK Government's lost data 'worth billions to criminals'", CNET, 29 November 2007

³ "2007 Annual Study: U.K. Cost of a Data Breach", Ponemon Institute, 25 February 2008

⁴ "Whitehall looks to encryption", Computing 22 Jan, 2008

Encryption that Ensures the Ultimate Protection

SanDisk® Cruzer® Enterprise Secure USB flash drives meet the requirements of government agencies by:

- Limiting the use of government-issued flash drives to government-owned PCs
- Using powerful, hardware-based 256-bit AES encryption, the most secure block cipher encryption standard adopted to date, complex password protection and a lock-down mechanism when a set number of incorrect password attempts is exceeded to ensure that data on lost or stolen drives cannot be hacked
- Enabling authorized employees to transfer data securely, even when sensitive information needs to be used on different computers or stations
- Offering FIPS 140-2 level 2 certification for encryption, a standard set by the National Institute of Standards and Technologies
- Increasing productivity of government employees with customized group-based policies that provide authorized parties with access to sensitive information
- Circumventing reliance on the user through mandatory 100 percent data encryption of all files
- Enabling the drive to be constantly monitored, audited and tracked using central management
- Maintaining a full content audit trail of files read, written or deleted from the drives
- Centralizing deployment and provisioning through centralized updates and configuration of all device parameters, remote password administration, and remote deactivation of lost or stolen drives through implementation of optional SanDisk Central Management & Control (CMC) software
- Supporting usage policies that allow for a restricted operating environment to prevent drives from operating on unauthorized PCs
- Ensuring business continuity through seamless backup of drive content and the ability to restore or recreate data on lost or stolen drives

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, can 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 percent 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

Key Mandates to Protect Government Data

European Union Data Protection Directive requires member countries to develop rigorous policies regarding collection, storage, usage and disclosure of personal information. Varying implementations within member countries recommend or require encryption.

UK Cabinet Secretary Rules issued by the cabinet secretary in January 2008 prohibit the removable of mobile computers and data devices containing unencrypted sensitive data.

US Federal Government OMB Memorandum M-06 16 requires that agencies encrypt all data on mobile devices unless the agency has determined that data to be nonsensitive.

Payment Card Industry / Data Security Standards (PCI/DSS) requires encryption of cardholder data. (Ver 1.1, Section 3 addresses data at rest), which applies to several governmental ministries.

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