Computer Security Policy for Encryption of Data at Rest When Outside of Agency Facilities

Effective December 31, 2008

The Office of Management and Budget released memorandum M-06-16, "Protection of Sensitive Agency Information," on June 23, 2006. This memorandum requested agencies to encrypt data on all devices (such as computer hard drives and thumb drives) that contain sensitive information and are removed from agency facilities. Data at rest is information that is electronically stored on media. Encryption involves conversion of data into a secret code. Encryption is considered effective when the altered text cannot be read by anyone except the intended recipient. The recipient uses a conversion tool along with cryptographic keys and a cryptographic algorithm to decrypt the text. Implementation of NRC's data encryption policy is being divided into two parts: encryption of data at rest and encryption of transmitted data. This policy addresses encryption of data at rest. A separate policy to address encryption of transmitted data will be issued in the near future. The next revision of Management Directive 12.5, "NRC Automated Information Security Program," will include this policy. NUREG/BR-168, revision 4 is also being issued to clarify safeguards information (SGI) processing guidance.

The following U.S. Nuclear Regulatory Commission (NRC) policy reflects the needs expressed above. This policy applies to all NRC employees, contractors, vendors, and agents (users) having access to any system that resides at any NRC facility or contractor facility having access to the NRC network or storing any public or non-public NRC information. This policy also applies to all information technology (IT) systems operated by the NRC or operated by a contractor or outside entity on behalf of the NRC. System owners are office directors, regional administrators, and Office of Information Services (OIS) division directors. This policy does not apply to licensees.

All new contracts and modifications to contracts that include IT must contain requirements to encrypt data at rest as required by this policy. All existing contracts must be modified by January 1, 2010 to include these requirements.

Policy

When using a computer outside of a facility that has been approved by the NRC designated approving authorities (DAAs) for NRC information processing, it is the user's responsibility to ensure that full-disk encryption technology has been used to encrypt the entire disk(s).

For all media containing electronic sensitive information, the user must ensure that the information stored on the media is encrypted when the media is outside of a facility that has been approved by the NRC DAAs for NRC information processing. Examples of media include, but are not limited to, compact disks (CDs), digital video disks (DVDs), thumb drives, backups, and external hard drives. All media must be appropriately labeled and controlled according to the sensitivity of information stored on the media.

Thumb drives used for SGI must be color coded purple to enable the user to readily identify the thumb drive as an SGI thumb drive.

Thumb drives used for SGI storage must automatically encrypt (occurs regardless of user configuration or intervention) all information stored on the device using Federal Information Processing Standard (FIPS) 140-2 validated encryption or encryption approved by the National Security Agency (NSA) for protection of classified information (see NUREG/BR-168, revision 4).

When encryption of classified information is required, classified information must be encrypted using encryption approved by NSA for protection of classified information.

When encryption of unclassified sensitive information is required, unclassified, sensitive information, including SGI, must be encrypted using FIPS 140-2 validated encryption or encryption approved by the NSA for protection of classified information.

Guidance

The OIS is continuing to research products for the encryption of data at rest to identify the best products for NRC-wide implementation. Until product selection is finalized, the Computer Security Office, in coordination with OIS, has recommended use of the SecureDoc product to enable full-disk encryption of laptop computers containing unclassified, sensitive information that are removed from NRC facilities. WinMagic's SecureDoc Client Version 4.3 full-disk encryption is available from: http://www.winmagic.com/corporate_info/contact_us.html. Steps for installing the software can be found in the "General Laptop Configuration Guidance" located at
http://www.internal.nrc.gov/CSO/documents/NRC_General_Laptop_Configuration_Std_Guidance_20081204.doc

OIS is acquiring Stealth MXI USB drives using a GSA blanket purchase agreement. These USB drives automatically perform FIPS 140-2 validated encryption on all data files moved to the private data storage area of the device. Devices used for SGI information must be color-coded purple to enable the user to identify them as SGI devices. OIS can provide information regarding management and use of these drives. Please contact Evan Jones to obtain needed devices.

CD and DVD files containing unclassified, sensitive information can be encrypted using the Secure Zip software available on all NRC desktops. OIS can provide information regarding use of SecureZip. However, for USB memory devices, SecureZip is not to be used to encrypt files due to the nature of the devices. Devices that automatically encrypt the information are required, currently the Stealth MXI USB devices described above.

Backups of information need to be encrypted using a technology consistent with the policy provided herein and compatible with the product that performs the backup.

For use of standard desktop tools to perform encryption, please consult with the OIS.

Please refer all questions regarding this policy to Kathy Lyons-Burke, Senior Information Technology Security Officer for Policy, Standards, and Training.