

OMB Guidance to Federal Agencies on Data Availability and Encryption

OMB has asked that the following information be provided to Federal agencies:

"The National Institute of Standards and Technology has recently announced the Secretary of Commerce's approval of the Advanced Encryption Standard (AES), which will provide agencies with a new encryption method designed to be secure for at least 20-30 years. Encryption (whether AES or another approved means such as Triple DES) is an important tool for protecting the confidentiality of disclosure-sensitive information entrusted to an agency's care.

When suitably strong encryption algorithms are employed and implemented with appropriate assurance, encryption can prevent the disclosure of communicated or stored data to unauthorized parties. However, encryption of agency data also presents risks to the availability of information needed by the agency to reliably meet its mission. Specifically, without access to cryptographic key(s) needed to decrypt information, the agency risks losing access to its valuable information.

Therefore, when implementing encryption, agencies are reminded of the need to protect the continuity of their IT operations and agency services. In particular, agencies must address information availability and assurance requirements through appropriate data recovery mechanisms such as cryptographic key recovery. Consequently, NIST will issue appropriate guidance to agencies by April 2002. In the interim, agency IT purchasing and operating decisions should be made with a view toward an Agency's ability to implement data recovery processes that ensure availability of essential data when necessary."