INDIAN AFFAIRS
DIRECTIVES TRANSMITTAL SHEET

(modified DI-416)

DOCUMENT IDENTIFICATION NUMBER	SUBJECT	RELEASE NUMBER
65 IAM 3	Media Protection Policy	07-44
FOR FURTHER INFORMATION Office of Chief Information Officer		DATE

EXPLANATION OF MATERIAL TRANSMITTED:

This policy establishes compliance standards for media protection in Indian Affairs (IA) in accordance with NIST SP 800-53, and provides guidelines for IA employees, volunteers, and contractors on protecting Government owned or leased media equipment registered to IA.

Debbie L. Clark
Deputy Assistant Secretary – Indian Affairs (Management)

FILING INSTRUCTIONS:

Remove: None

Insert: 65 IAM 3

1.1 Purpose. This policy establishes compliance standards for media protection in Indian Affairs (IA) in accordance with National Institute of Standards and Technology Special Publication (NIST SP) 800-53, and provides guidelines for IA employees, volunteers, and contractors on protecting Government owned or leased media equipment registered to the Bureau of Indian Affairs (BIA).

1.2 Scope. This policy applies to all IA information systems and media including, but not limited to: paper and digital information system media, limited access to authorized users, and sanitization of information system media before disposal or release for reuse.

Senior IA management shall ensure that information systems operated by or on behalf of the Bureau receive adequate security equivalent to the safeguards required of BIA systems. Systems under development shall meet the security planning requirements commensurate with the sensitivity of the information they house and the current life cycle phase.

1.3 Policy.

A. Only Authorized users shall have access to media containing information system data. The media may be in printed form or on digital media removed from the information system.
B. External labels shall be affixed to removable information storage media and information system output.
C. Information system personnel shall mark human-readable output appropriately in accordance with applicable policies and procedures.
D. Information system personnel shall affix printed output with cover sheets if the printed output is not otherwise appropriately marked.
E. Information system personnel shall label digital media and cover sheets with
   a. Distribution limitation
   b. Handling caveats for the information, e.g., “Do Not Scan, Magnetic Media Enclosed”
   c. Applicable security markings such as For Official Use Only (FOUO), Sensitive But Unclassified (SBU)
F. Information system personnel shall physically control and securely store paper and digital information system media based on the highest FIPS 199 security category of the information recorded on the media.
G. Information system personnel shall control paper and digital information system media and restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.
H. Information system media shall be hand-delivered from authorized personnel to authorized personnel or transported via secure means with and acknowledgement of a sent-receipt.
I. Information system personnel shall sanitize information system digital media using approved equipment, techniques, and procedures in compliance with NIST SP 800–36.
J. Information system personnel shall track, document, and verify media sanitization actions and periodically test sanitization equipment/procedures to ensure correct performance.

K. Sanitization techniques including degaussing and overwriting memory locations shall ensure that the information system information is not disclosed to unauthorized individuals when such media is reused or disposed.

L. The product selected for degaussing shall be appropriate for the type of media being degaussed and part of the National Security Agency's approved list found at: http://www.nsa.gov/ia/government/MDG/NSA_CSS-EPL-9-12A.PDF.

1.4 Authority.

A. Department of the Interior (DOI) Computer Security Handbook, Version 1.0

B. Federal Financial Management Improvement Act of 1996 (FFMIA)

C. Federal Information Processing Standards (FIPS)

a. 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003

b. 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006

D. Federal Information Security Management Act of 2002 (FISMA)

E. National Institute of Standards and Technology (NIST) Special Publication (SP)

a. **SP 800-36**, Guide to Selecting Information Technology Security Products

b. **SP 800–53**, Recommended Security Controls for Federal Information Systems

c. **SP 800–88**, Guidelines for Media Sanitization Draft

F. Office of Management and Budget (OMB) Circular A-130, **Management of Federal Information Resources**, Appendix III, Security of Federal Information Resources, November 2000

1.5 Responsibilities.

A. Chief Information Officer and OCIO Staff are responsible for creating and/or revising information technology policies and ensuring that the information in the IAM for the programs and functions within their authority, including references and citations, is accurate and up-to-date.

B. Bureau Information Technology Security Manager (BITSM) shall ensure that the policy and processes in the IAM conform to applicable statutes, regulations, Federal standards, and policies.

C. Authorized IA Users, defined as IA employees, contractors, and other individuals who have been granted explicit authorization to access, modify, delete, or utilize IA information, shall adhere to this policy.

1.6 Sanction of Misuse. In accordance with 370 DM 752, personnel are individually responsible for protecting the confidentiality, availability, and integrity of data and information accessed, stored, processed, and transmitted. Individuals are accountable for actions taken on and with IA and BIA IT information resources. Failure to comply with this policy may lead to disciplinary action. Unauthorized disclosure of sensitive information may result in criminal or civil penalties.