

INDIAN AFFAIRS DIRECTIVES TRANSMITTAL SHEET

(modified DI-416)

DOCUMENT IDENTIFICATION NUMBER 65 IAM 7	SUBJECT Email Use Policy	RELEASE NUMBER 07-48
FOR FURTHER INFORMATION Office of Chief Information Officer		DATE

EXPLANATION OF MATERIAL TRANSMITTED:

This policy mandates the proper use of the BIA email system for all IA users and presents what IA deems as acceptable and unacceptable use of the email system. This policy establishes standards for acceptable use of BIA email by IA employees, volunteers, and contractors when using Government-owned or leased equipment.



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

FILING INSTRUCTIONS:

Remove: None

Insert: 65 IAM 7

- 1.1 Purpose.** This policy mandates the proper use of the Bureau of Indian Affairs (BIA) email system for all Indian Affairs (IA) users and conveys acceptable and unacceptable use of the email system. This policy establishes standards for acceptable use of BIA email by IA employees, volunteers, and contractors when using Government-owned or leased equipment.
- 1.2 Scope.** This policy applies to all IA users including all employees and contractors accessing the BIA email.
- 1.3 Policy.**
- A. Official Records -** The BIA email system is for official business-use only and shall only be used in accordance with the appropriate IA use policy of information resources.
- a. All messages sent or received on BIA systems are IA property.
 - b. Employees and contractors do not have the right to, nor should they have an expectation of privacy while using the email system; users consent to monitoring and recording of email usage with or without cause by using BIA email.
 - c. Email documents are official records
 - i. When they are created or received in the transaction of agency business and are appropriate for preservation as evidence of government functions and activities
 - ii. When they are valuable because of the information they contain
 - d. Email documents are not official records
 - i. When they provide no evidence of agency functions and activities
 - ii. When they provide no information of value
 - iii. When duplicate information is already documented in existing records
 - e. All official electronic records shall be printed in hardcopy and filed in the official paper record keeping system. Only when this has been completed can the electronic version of the email be deleted if no longer needed.
 - f. Special instructions apply for printing and deleting email messages related to the Cobell litigation. Included in electronic records that must be printed and filed are all email messages with all attachments that relate to:
 - i. Cobell litigation
 - ii. American Indian Trust reform activities
 - iii. Administration of Individual Indian Money (IIM) accounts
- B. Prohibitions**
- a. Users are prohibited from creating, copying, transmitting, or retransmitting any chain letters or unauthorized mass/group mailings regardless of subject matter.
 - b. Users shall not use the BIA email system for activities that are illegal and inappropriate. Such activities include but are not limited to hate speech or

INDIAN AFFAIRS MANUAL

Part 65
Chapter 7

Information Security
Email Use

Page 1

material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, age, or sexual orientation.

- c. Users shall not use the BIA email system for downloading, viewing, storing, copying, or transmitting sexually-explicit or sexually-oriented materials.
- d. Users shall not use the BIA email system for creating, downloading, viewing, storage, copying, or transmitting of materials related to illegal gambling, illegal weapons, terrorist activities, or any other illegal activities.
- e. Users shall not use the BIA email system to support a personal business including assisting relatives, friends, or other persons in such activities.
- f. Users shall not use the BIA email system for commercial purposes, in support of for-profit activities, or in support of other outside employment or business activity such as consulting for pay, sales or administration of business transactions, or sales of goods or services.
- g. Users shall not use the BIA email system for engaging in any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited political activity.
- h. Users shall not open any email message received from unknown or suspect sources with any unknown file attachments. All emails and attachments shall be scanned locally on the user's computer for viruses and other malicious code.
- i. Users shall not use the BIA email system for posting agency information to external news groups, bulletin boards, or other public forums without authorization. This includes any activity that could create the perception that the communication was made in an official capacity as a Federal Government employee unless appropriate IA approval has been obtained.
- j. Users are prohibited from exchanging copyright material as attachments to email messages.

C. Encryption

- a. An approved encryption process shall be employed if sensitive information must be sent by email. The employed encryption standard must enforce end-to-end encryption.

1.4 Authority.

A. The Department of the Interior (DOI)

- a. Memorandum by J.Steven Griles, Responsibility of Maintaining Electronic-Mail (Email) Records, July 9, 2004
- b. Departmental Manual 375 DM 19 Information Resource Management.

B. National Archives and Record Administrator regulation 36 CFR Part 1234.24, Standards for Managing Electronic Mail Records

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.