


INDIAN AFFAIRS DIRECTIVES TRANSMITTAL SHEET

(modified DI-416)

DOCUMENT IDENTIFICATION NUMBER 65 IAM 6	SUBJECT Help Desk Use Policy	RELEASE NUMBER 07-47
FOR FURTHER INFORMATION Office of Information Operations (OIO) Eastern Zone Manager		DATE

EXPLANATION OF MATERIAL TRANSMITTED:

This policy establishes mandates, authorities, responsibilities, and compliance requirements for the Indian Affairs (IA) Help Desk, formally identified as the Support Center and also known as Support Desk, Information Technology (IT) Support, and Customer Support.



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

FILING INSTRUCTIONS:

Remove: None

Insert: 65 IAM 6

INDIAN AFFAIRS MANUAL

1.1 Purpose. This policy establishes mandates, authorities, responsibilities, and compliance requirements for the Indian Affairs (IA) Help Desk, formally identified as the Support Center and also known as Support Desk, Information Technology (IT) Support, and Customer Support.

1.2 Scope. This policy applies to all Users, employees and contractors accessing BIA systems, who need services and support regarding Indian Affairs internally developed software and systems; standard commercial-off-the-shelf (COTS) office automation software; enterprise Government-off-the-shelf (GOTS) software; user accounts and passwords; telecommunications; IA and Education networks; hardware repair; desk-side personal computer (PC) support; telephone-based PC support; and common PC peripherals support.

1.3 Policy.

- A. The Indian Affairs Help Desk shall be used only for official Government use.
- B. Users shall contact the Indian Affairs Help Desk for all IT service requests.
- C. The Indian Affairs Help Desk shall not be used for personal purposes.

1.4 Authority.

A. Department of the Interior (DOI)

- a. Security Policy Handbook and Standard
- b. Personnel Handbook
- c. IRM Bulletin 1997-001, DOI home page <http://www.doi.gov/orim/bulletins>

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.
- D. **Help Desk Call Technicians** shall receive support requests, open service tickets for all issues, resolve issues as quickly as possible, and escalate issues when appropriate.
- E. **Division of Information Operations (DIO) Support Managers** to include Field Support Managers, Zone Managers, and Branch Chiefs, shall ensure all IT support

INDIAN AFFAIRS MANUAL

work is documented, all service tickets are assigned to support technicians, service tickets are referred back to the Indian Affairs Help Desk as appropriate, service tickets are updated, and issues are resolved as quickly as possible.

- F. DIO Support Technicians**, to include Field support, Telecom, Systems, Disaster Recovery, and Special IT, shall review their Indian Affairs Help Desk queues regularly, resolve issues as quickly as possible, escalate service tickets to their supervisor when appropriate, notify customers directly of this policy, and create a service ticket immediately when the situation is critical.

- 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.