

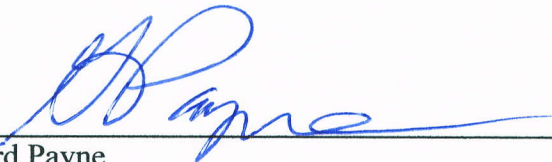
# INDIAN AFFAIRS DIRECTIVES TRANSMITTAL SHEET

(modified DI-416)

DOCUMENT IDENTIFICATION NUMBER 65 IAM 9	SUBJECT Remote Access Policy	RELEASE NUMBER #09-29
FOR FURTHER INFORMATION Office of the Chief Information Officer—Indian Affairs		DATE 3/8/2010

**EXPLANATION OF MATERIAL TRANSMITTED:**

This policy establishes mandates, authorities, responsibilities, and compliance requirements for users who remotely access the Indian Affairs (IA) network and systems in accordance with the Department of the Interior (DOI) regulations cited in Section 1.4.A of the policy. This policy applies to all users under the authority of the Assistant Secretary—Indian Affairs (AS-IA), to include contractors, consultants, temporary employees, interns, volunteers; and tribal users who access the IA network and systems remotely with government-furnished equipment.



\_\_\_\_\_  
Grayford Payne  
Acting Deputy Assistant Secretary—Indian Affairs (Management)

---

**FILING INSTRUCTIONS:**

Remove: None

Insert: 65 IAM 9 (New)

# INDIAN AFFAIRS MANUAL

- 1.1 Purpose.** This chapter establishes mandates, authorities, responsibilities, and compliance requirements for users who remotely access the Indian Affairs (IA) network and systems in accordance with the Department of the Interior (DOI) regulations.
- 1.2 Scope.** This policy applies to all users including but not limited to all functions under the authority of the Assistant Secretary—Indian Affairs (AS-IA), including AS-IA, Bureau of Indian Affairs (BIA), and Bureau of Indian Education (BIE); IA employees, contractors, consultants, temporary employees, interns, volunteers; and tribal users who access the IA network and systems remotely with government-furnished equipment.
- 1.3 Policy.**
- A. General**
- All users including but not limited to IA employees, contractors, consultants, temporary employees, interns, volunteers, and tribal users shall adhere to the following remote access and two-factor authentication requirements.
- a. Remote access control shall be enforced to include password authentication and encryption standards in compliance with Federal Information Processing Standards (FIPS) 140-2 requirements.
  - b. All users including but not limited to IA employees, contractors, consultants, temporary employees, interns, volunteers, and tribal users with remote access privileges to the IA network shall comply with all IA IT policies.
  - c. Remote Access and Two-Factor Authentication
    - i. Authorized users are allowed to access IA resources remotely from government-furnished equipment from their personal home networks, hotels, airports, and other places where an Internet connection wired/wireless is available.
    - ii. If a user has an activated HSPD -12 (Homeland Security Presidential Directive - 12) compliant Personal Identification Verification (PIV) card, hereafter referred to as a PIV card, they shall use two-factor authentication when accessing VPN (Virtual Private Network) to remotely connect to the IA network.
    - iii. Only government-furnished hardware and software shall be used to employ remote access and two-factor authentication
      - a. Government-furnished hardware constitutes a PIV card reader and computers.
      - b. Government-furnished software constitutes ActivIdentity software installed by the IA Office of Information Operations (OIO).

**B. Scanning**

- a. All applicable government-furnished equipment shall be scanned for vulnerabilities prior to receiving final approval for remote access.
- b. Any identified Critical, High, or Moderate vulnerabilities must be corrected prior to receiving final approval for remote access.
- c. All applicable government-furnished equipment shall be scanned for vulnerabilities every 30 days via an automated function of the established network security scanning tools. **Remote users agree to have all equipment scanned by the IA Computer Security Incident Response Team (CSIRT) prior to connecting to the IA network if the equipment has not been connected to the IA network for a period of more than 30 days in order to get the latest anti-virus updates and necessary software and operating system patches per OISP and OIO procedures documented in *Remote Access Approval Procedures, December 2009*.**
- d. All applicable government-furnished equipment that has been identified as having Critical, High, or Moderate vulnerabilities during a 30 day scan shall be corrected by IA OIO within 3 days.

**C. Prohibitions**

- a. All personal and non-government-furnished portable or mobile computing devices are prohibited from connecting to any IA system, subsystem, or network.
- b. Users who remotely access the IA network and systems
  - i. Shall not provide their log-on or email password to anyone, not even family members, for any reason.
  - ii. Shall not perform illicit activities as defined in chapter 65 IAM 5, Personal Use of Government Resources.
  - iii. Shall not use remote access for outside business interests.
  - iv. Shall not use non-IA email accounts such as Hotmail, Yahoo, and AOL or other external resources to conduct IA business.

**1.4 Authority.**

**A. Department of the Interior (DOI)**

- a. Department of the Interior (DOI) Information Technology Security Policy Handbook, v3.2.
- b. OCIO Directive 2005-012, *Wireless Network Security*, July 29, 2005.

**B. Indian Affairs Manual (IAM)**

- a. 65 IAM 5, Personal Use of Government Resources
- b. 65 IAM 4, Portable Device Use Policy

- C. **Office of the Chief Information Officer—Indian Affairs**
  - a. Remote Access Policy, IT-2007-037, December 17, 2007.
- D. **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.
- E. **Federal Information Security Management Act of 2002 (FISMA)**
- F. **National Institute of Standards and Technology (NIST) Special Publications (SP)**
  - a. SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, July 2008.
  - b. SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009.
  - c. SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, February 2007.
  - d. SP 800-121, *Guide to Bluetooth Security*, September 2008.
- G. **Office of Management and Budget (OMB)**
  - a. Circular A-130, Management of Federal Information Resources, Appendix III, *Security of Federal Information Resources*, November 2000.
  - b. M06-16, *Protection of Sensitive Agency Information*, June 23, 2006.
- H. **Office of the Chief Information Officer—Indian Affairs (OCIO-IA) Office of Information Security and Privacy (OISP) and Office of Information Operations (OIO)**
  - a. *Remote Access Approval Procedures*, December 2009

### 1.5 Definitions.

- A. **Remote access** - the capability to access the IA network from a location external to the network.
- B. **Two-Factor Authentication** is a combination of two elements:
  - i. ‘Something you know,’ defined as a Personal Identification Number (PIN), and
  - ii. ‘Something you have,’ defined as an HSPD-12 compliant Personal Identity Verification (PIV) card.
- C. **Virtual Private Network (VPN)**—a connection over a shared network that is encrypted and secure from other network users and, therefore, virtually appears to be a private network connection.

- D. Wireless** - a radio frequency connection, including wireless Ethernet and cellular connections.

### 1.6 Responsibilities.

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

**B. Bureau Chief Information Security Officer (BCISO)** shall ensure that the policy and processes in 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.

### 1.7 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.