INDIAN AFFAIRS
DIRECTIVES TRANSMITTAL SHEET

(modified DI-416)

DOCUMENT IDENTIFICATION NUMBER	SUBJECT	RELEASE NUMBER
65 IAM 8	Internet Use Policy	07-49
FOR FURTHER INFORMATION Office of Chief Information Officer		DATE

EXPLANATION OF MATERIAL TRANSMITTED:

The Internet provides a source of information that can benefit every professional discipline represented in Indian Affairs (IA). This policy establishes standards for acceptable use of the Internet by IA employees, volunteers, and contractors when using Government-owned or leased equipment, facilities, Internet addresses, or domain names registered to the BIA.

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

FILING INSTRUCTIONS:

Remove: None

Insert: 65 IAM 8

1.1 Purpose. The Internet provides a source of information that can benefit every professional discipline represented in Indian Affairs (IA). This policy establishes standards for acceptable use of the Internet by IA employees, volunteers, and contractors when using Government-owned or leased equipment, facilities, Internet addresses, or domain names registered to the Bureau of Indian Affairs (BIA).

1.2 Scope. This policy applies to all IA users including all employees, volunteers, and contractors accessing the Internet using BIA equipment.

1.3 Policy.

A. Users have no inherent right to employ BIA Internet resources for personal use.

B. Users may use the Internet during off-duty hours, such as before or after a workday, subject to local office hours, lunch periods, or during short infrequent breaks.

C. Any use of BIA Information Technology (IT) resources is made with the understanding that such use may not be secure, is not private, is not anonymous, and may be subject to disclosure under the Freedom of Information Act (FOIA). IA employees, volunteers, and contractors do not have a right to, nor shall they have an expectation of, privacy while using BIA IT resources at any time including accessing the Internet through BIA gateways and using email, which may be subject to release pursuant to the Freedom of Information Act. To the extent that employees wish that their private activities remain private, they shall avoid making personal use of BIA IT resources.

D. Users shall conduct themselves professionally in the workplace and shall refrain from using government office equipment for activities that are inappropriate.

E. Electronic data information about the Internet usage of a specific user may be disclosed to appropriate Department of the Interior (DOI) employees on a need-to-know basis for the performance of their duties. As an example, with manager approval, technical staff may employ monitoring tools to maximize utilization of resources that may include the detection of inappropriate use.

F. Users shall not use the Internet for the intentional creation, downloading, viewing, storage, copying, or transmission of sexually-explicit or sexually-oriented materials.

G. Any personal use of the Internet that could cause congestion, delay, or disruption of service to any BIA IT resource is prohibited. Greeting cards, video, and sound files are prohibited. Large file attachments can degrade the performance of the entire network as do some uses of “push” technology such as audio and video streaming from the Internet.

H. Users shall not use the Internet for the intentional creation, downloading, viewing, storage, copying or transmission of materials related to gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited.

I. Users shall not use the Internet for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include but are not limited to hate speech or material that ridicules others on the basis of race, creed, religion, color, age, sex, disability, national origin, or sexual orientation.

J. Users shall not use the Internet for commercial purposes or 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, sale of goods or services.

K. Users shall not use the Internet for establishing personal, commercial and/or nonprofit organizational web pages on government-owned machines.

L. Users shall not use the Internet for engaging in any outside fundraising activity including nonprofit activities endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

M. Users shall not use the Internet for posting agency or personal information including information which is at odds with Departmental missions or positions to external newsgroups, bulletin boards or other public forums without authority. This includes any use that could create the perception the communication was made in an official capacity as a Federal Government employee unless appropriate Agency approval has been obtained.

N. Users shall not use the Internet for the use of BIA systems as a staging-ground or platform to gain unauthorized access to other systems.

O. Users shall not use the Internet for the intentional unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data that includes information subject to the Privacy Act, copyrighted, trademarked, or material with other intellectual-property rights beyond fair use, proprietary data, or export-controlled software or data.

P. Users shall not use the Internet for the use or creation of unauthorized list servers or the distribution of unauthorized newsletters.

Q. Users shall not use the Internet for using Peer-to-peer (P2P) and other file-sharing software on the Internet such as Kazaa, BitTorrent, and Emule.

R. Use of Instant Messaging (IM) technology such as AIM, MSN, Yahoo, and so forth is prohibited on BIA IT resources.

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. Department of the Interior (DOI) Internet Acceptable Use Policy, May 23, 1997

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

E. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems

F. 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. Memorandum 04-04, E-Authentication Guidance for Federal Agencies, December 2003

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 BIA IT resources and IA information. Failure to comply with this policy may lead to disciplinary action. Unauthorized or inappropriate use of the Internet could result in loss of use or limitations on use of equipment, disciplinary or adverse actions, criminal penalties and/or employees or other users being held financially liable for the cost of inappropriate use. Unauthorized disclosure of sensitive information may result in criminal or civil penalties.