1.1 Purpose. This chapter describes the Assistant Secretary - Indian Affairs (AS-IA) Information Resources Management (IRM) program and its scope, goals, responsibilities, and structure. The program has been established to effect the administration, policy guidance, program direction, and authority of the Deputy Assistant Secretary for Information Resource Management/Chief Information Officer – Indian Affairs (DASIRM/CIO – IA) for information resources management activities throughout the AS-IA and Bureau of Indian Affairs (BIA). The IRM program provides the policy, authorities, and responsibilities of the DASIRM/CIO – IA and its relevance to the management and oversight of the Information Technology (IT) serving individual Indians, Indian tribes, and Indian Affairs business owners. The AS-IA IT organization applies innovative management and technologies to enhance service delivery to a complex, nationwide organization which interfaces with tribes and other governmental agencies, both internal and external.

1.2 Scope. The DASIRM/CIO – IA is responsible for the acquisition, utilization, architecture, security, operations and information resources management and IT; develops IT policy and procedures; and serves as system owner and system manager for all BIA systems. The Office of the Chief Information Officer – Indian Affairs (OCIO-IA) IRM program encompasses the information resources and information management and coordination processes of the AS-IA and all BIA offices. The policies, procedures and standards established within the OCIO – IA shall also apply to work or activities performed by consultants, contractors, universities and other government agencies for the AS-IA to the extent that these activities involve information resources management functions or processes. The OCIO – IA provides leadership to six information management directorates, which manage IT and IT investments; creates new computer applications; implements security technology policy, practices, and standards; develops new information technology policy; engineers modern information technology infrastructures, and operates Indian Affairs technology and major applications; and implements appropriate Privacy Act sensitivity and confidentiality requirements for Indian Affairs data for electronic and hardcopy formats.

1.3 Policy. It is the policy of the DASIRM/CIO – IA to plan, design, operate, and protect government information resources for conducting official government business in accordance with applicable federal and departmental directives and guidelines for Indian Affairs (IA).

1.4 Authority. The IRM program is based on the authorities assigned to the AS-IA and delegated to the DASIRM/CIO – IA, as delineated in 110 DM 8.5 and 130 DM 10. The IRM program is the focal point for the implementation of public laws, Federal regulations, and Executive Orders related or pertaining to information resources. The following is a list of the most significant of these authorities:

A. Statutes.

(1) Title 44, U.S.C. § 36, E-Government Act of 2002

(2) Title 5, U.S.C. § 552a, Privacy Act of 1974

(3) Title 5, U.S.C. § 552 Freedom of Information Act of 1966

(4) Federal Records Act of 1940, as amended 1950

(5) Computer Security Act of 1987

(6) Computer Matching and Privacy Act of 1988

(7) The Chief Financial Officer Act of 1990

(8) The Government Performance and Results Act of 1993

(9) The Federal Acquisition Streamlining Act of 1994

(10) The Paperwork Reduction Act of 1995

(11) Information Technology Management Reform Act of 1996 (Clinger-Cohen Act)

(12) The Government Paperwork Elimination Act of 1998

(13) The Government Information Security Reform Act of 2000.

(14) Federal Information Security Management Act of 2002

B. Regulations. (Reserved)

C. Court Rulings. (Reserved)

D. Presidential Directives.

(1) Presidential Decision Directive, NSC 63, Critical Infrastructure Protection and Continuity of Operations

(2) Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure/ Identification, Prioritization, and Protection

E. OMB Directives.

(3) OMB Memorandum M-03-18, Implementation Guidance for the E-Government Act of 2002

(4) OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security

(5) OMB Circular A-130: Management of Federal Information Resources

(6) OMB Memorandum M-96-20 Chief Information Officer

F. Departmental Directives.

(1) 109 DM 8, Assistant Secretary – Indian Affairs, Organization

(2) 130 DM 10, Assistant Secretary – Indian Affairs, Office of Information Resources Management

(3) 209 DM 8, Assistant Secretary – Indian Affairs, Delegation

(4) 375 DM 19, Information Technology Security Program

(5) 383 DM 15, Freedom of Information Act Handbook

(6) 383 DM 1-13, Privacy Act Program

(7) DOI Information Technology Security Plan

(8) DOI Certification and Accreditation Guide

G. Other Agency Directives.

(1) National Institute of Standards and Technology (NIST). Multiple NIST Special Publication 800 series guidelines related to IT Security

(2) National Institute of Standards and Technology (NIST). Multiple Federal Information Processing Standards (FIPS) related to IT security

H. Handbooks. (Reserved.)

1.5 Definitions. The following is a list of terms and definitions most frequently used when describing IRM functions or activities. Each program chapter for the core program disciplines contains additional terms and definitions, which are primarily related to that discipline.

(A) Business Owner. Business owners of systems are the functional owners responsible for the Indian mission program business requirements, business processes, data content, and records. Business owners are responsible for creating Privacy Act system notices for systems which collect personal information and designating routine users of the system.

(B) Data. A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by machines.

(C) Data Administration. A function including development and coordination of the policies, procedures, practices, and plans for the capture, correction, storage, and use of data.

(D) Data Base. A collection of interrelated data logically stored to serve one or more uses or applications.

(E) Data Base Administration. The process of controlling the content, design, and use of one or more data bases to avoid uncontrolled redundancies and to enhance development.

(F) Data Resource Management. The process of planning and controlling the activities and functions of an organization which relate to collecting, cataloging, processing, storing, communicating, and disposing of data.

(G) Federal Information Processing Standards (FIPS) Program. FIPS is an ongoing process designed to provide leadership, technical guidance, and coordination of government efforts in the development of guidelines and standards for the information sciences and related disciplines.

(H) Automated Service Center. A collective team that provides technical help and other assistance including specific or generalized IT information services, and IT application assistance as requested.

(I) Information Communications. The procedures and means by which data and information are communicated and disseminated throughout an organization.

(J) Information Cost. The aggregate cost an organization requires or expends to do the job of creating, processing, and disseminating information and paperwork.

(K) Information Disposition. The steps taken to determine data disposition.

(L) Information Dissemination. The active process of communicating recorded ideas, facts, and data by any medium.

(M) Information Inventory. A collection of descriptive data regarding the scope, quantity, content, or location of an organization's information holdings. This data may be contained within an information catalog.

(N) Information Management. The application of general management principles including planning, directing, and controlling the processing, handling, and uses of an organization's information.

(O) Information Processing. To copy, exchange, read, combine mathematically logically, record, store, transmit, transport, or write information from one medium or format to another.

(P) Information Security. The IT management controls designed to protect information, equipment, facilities, and other assets from loss, destruction, or unauthorized access.

(Q) Information Services. A helpful activity provided to users to assist them in meeting their information needs and requirements.

(R) Information Source. The origin of data acquired or generated by an organization.

(S) Information Standards. Standards pertaining to the manner in which data and information are defined, cataloged, represented, transmitted, stored, processed, and accessed; also the manner in which associated information technology is designed, configured, interconnected, and operated in the process of handling data.

(T) Information System. The combination of human resources, technology, and established methods and procedures to collect, process, and communicate data in the form or format needed.

(U) Information Technology. The collection of electronic devices including optical equipment together with their control programs, operating systems, application systems, and instructions which are applied to the collection, organization, processing, storage, retrieval, and communication of data.

(V) Library. A collection of information pertaining to specialized or diverse subject areas stored in one or more media forms, accessible to those of a designated user community who require the information, and under the management of a librarian.

(W) Management Analysis. Analyzing, evaluating, and improving the effectiveness of IT work methods and procedures including project management, manpower utilization, distribution of work assignments, delegations of authority, management controls, information and documentation systems, and other functions of management.

(X) System Owner. The CIO is the System Owner and certifier for IT systems. The CIO is responsible for IT capital planning, IT architecture and development, IT security, and IT operations including software coding/testing, backup and recovery, hardware/servers, workstations, and networks for business application platforms, incident handling and continuity of operations and privacy act requirements.

1.6 Responsibilities.

A. The DASIRM/CIO-IA is responsible for:

(1) Leading IA strategic planning to improve the use of information and information processing resources.

(2) Developing and improving policies promoting the use of information technology and IRM throughout IA in consultation with Central Office and Program Directors.

(3) Developing effective working relationships with IRM Offices in the Department of the Interior.

(4) Supervising Field IT and IRM staff and managing all IA information resources and technology.

(5) Providing direction and oversight for IA IT security activities.

(6) Leading the planning and implementation of E-Government activities developed for IA mission programs.

(7) Developing and implementing IA policies on the creation, maintenance and disposition of records and information.

(8) Ensuring standardized information technology and information resource management functions within IA to achieve continuity of operations and accountability throughout the organization.

(9) Managing and coordinating information and data replies that cross organizational or functional lines.

(10) Managing certification and delegated approving authority for all IA information systems.

(11) Serving as Information Technology manager for IA information technology centers.

(12) Serving as system owner of all AS-IA and BIA information systems.

(13) Approving information technology investments for all IA IRM and IT equipment, software and services.

(14) Managing and implementing policy and oversight for the IA Freedom of Information Act (FOIA) program.

(15) Managing and implementing policy and oversight for the IA Privacy Act (PA) program.

(16) Interacting with other governmental agencies – Office of Management and Budget, General Accountability Office, General Services Administration, Federal Cyber Security organizations, National Infrastructure Protection Center, GSA Federal Computer Incident Response Center, and Congressional Committees as they relate to information management and technology.

(17) Interacting with other Department of the Interior bureaus to coordinate and implement IT initiatives.

(18) Managing the AS-IA and BIA information systems, defining the system functional requirements, providing functional oversight, and providing for periodic review of the system requirements in order to determine whether the requirements continue to exist and that the system continues to meet the purposes for which it was developed in an efficient and cost effective manner.

B. Records Management Officer. The IA Records Management Officer is responsible for ensuring that information resource management and IA records, regardless of their physical form, are created, maintained, and disposed of in compliance with applicable laws and regulations and computer system management standards.

C. Freedom of Information Act (FOIA) and Privacy Act (PA) Officer. The IA FOIA/PA Officer is responsible for ensuring that information resource management policy and oversight for records, and the accessing and safeguarding of records covered by the FOIA/PA Act, is in compliance with applicable laws and regulations and computer system management standards.

D. IA Directors, including AS-IA, BIA and OIEP, are responsible for:

(1) Ensuring that IA policies and procedures for IRM are implemented.

(2) Identifying IRM requirements in program and budget plan formulation.

(3) Conducting annual reviews and analysis of the Central Office and Regional Offices for use of IT and needed improvements in information-handling.

(4) Serving as active members on the Information Resource Management Committee (IRMC) as designated in the IRMC Charter.

(5) Ensuring that FOIA and PA roles and responsibilities are implemented.

(6) Implementing Records Management requirements.

1.7 Information Resource Management Program and Policy Structure. The IRM program is developed and maintained according to the following structure.

(A) Program Management Elements:

(1) IRM Policy Development and Dissemination

(2) IRM Program Coordination

(3) IRM Strategic Planning

(4) IRM Assessment

(5) IRM Organizations

(B) Resources and Technology Management Elements:

(1) IRM Budgeting and Financial Management

(2) Information Technology and Services Management

(3) Information Technology and Services Procurement

(4) Information Resources Managers and Technologists

(5) Information Resources Standards Program

(C) Information Life Cycle Management Elements:

(1) Information Acquisition

(2) Information Cataloging and Inventorying

(3) Information Use Management

(4) Information Processing Management

(5) Information Communication

(6) Information Dissemination or Sharing

(6) Information Disposition

(7) Information Management, Disclosure, and Withholding

1.8 Reports and Forms. (Reserved)

1.9 Description of DASIRM/CIO-IA Core Program.

A. General Description. IRM is concerned with the management and operational interrelationships that include data processing, telecommunications, libraries and information centers, records management, data administration, IT project management and management analysis in regulating or utilizing information resources. The span of the IRM program activities covers information technology life cycles including the acquisition, management, cataloging, communication, processing, usage, access, restrictions, and disposition of information technology. The program is also concerned with the personnel and fiscal resources associated with information-related activities within the AS-IA and BIA.

B. OCIO – IA IRM Core Programs.

(1) Office of Information Policy (See 110 DM 8.5**)** develops policies and guidance on information resources and technology management; manages the Freedom of Information Act policy, oversight and communications; manages Privacy Act policy, oversight, and communications; performs records management oversight and guidance; acts as liaison to Indian Affairs program offices and DOI for the OMB Information Collection process for Federal Register notices. The Office of Information Policy coordinates with IA programs, tribes, and other governmental agencies on records management, Indian records assessments. The office is responsible for IA compliance with the Paperwork Reduction Act of 1995, the Computer Security Act of 1987, the Competition in Contracting Act of 1984, the Federal Records Act of 1950, OMB Circular A-130: Management of Federal Information Resources, the Government Paperwork Elimination Act (GPEA), and the Freedom of Information Act of 1966 and Privacy Act of 1974

(2) Office of Information Planning (See 110 DM 8.5) coordinates the Indian Affairs strategic planning, portfolio management, and budgeting processes for information technology; provides capital planning and investment support to assure that IA plans support IA business planning and mission accomplishments; coordinates the activities of the Information Technology Investment Council (ITIC); provides leadership for special priority initiatives; and develops the IT five-year plan. The office is also responsible for administrative support and planning within IT and manages IT funds for cross-functional and infrastructure projects. It also ensures Indian Affairs compliance with the Information Technology Management Reform Act of 1996 (the Clinger Cohen Act), and OMB Circular A-130: Management of Federal Information Resources.

(3) Office of Information Architecture and Engineering (See 110 DM 8.5) develops policies and guidelines addressing Internet technologies, enterprise information, and IT architecture;

coordinates with agencies through working groups and seminars to promote a partnership with business partners; and provides oversight and control of data, software, and hardware assets. The office oversees IA business data applications, technical and security architecture from baseline through transition, and is responsible for establishing database standards, technical references, and engineering assistance for projects. The office is also responsible for implementing IA architectural and engineering compliance with the Information Technology Management Reform Act of 1996 (the Clinger Cohen Act), the Computer Security Act of 1987, Federal Records Act of 1940, as amended 1950, OMB Circular A-130: Management of Federal Information Resources, and the Government Information Security Reform Act of 2000.

(4) Office of Information Security and Privacy (See 110 DM 8.5**)** implements and administers a program to protect the information resources of IA in compliance with Federal legislation; monitors cyber security policies and guidance for IA; monitors all IA systems development and operations for security and privacy compliance; monitors program office information system security activities; develops, implements, and evaluates employee cyber security awareness and training programs; establishes and leads the IA Computer Security Incident Response Capability team; monitors IT certification and accreditation; and establishes guidance and training requirements for managers of information systems designated as sensitive. The office is also responsible for implementing IA security and privacy compliance with the Information Technology Management Reform Act of 1996 (the Clinger Cohen Act), the Computer Matching and Privacy Act of 1988, the Computer Security Act of 1987, OMB Circular A-130: Management of Federal Information Resources, the Government Information Security Reform Act of 2000, Presidential Decision Directive NSC 63 Critical Infrastructure Protection, and Continuity of Operations (COOP).

(5) Office of Information Development (See 110 DM 8.5) recommends and implements the development of web-based applications for the Internet and Intranet, palm device attachment applications, and other applications for databases, communications, wireless solutions, and emerging and enabling technologies. The office also assists in developing business process reengineering solutions and supports IA IT business.

(6) Office of Information Operations (See 130 DM 10) includes the following divisions:

(a) The Division of Telecommunications supports all IA wireless, radio, voice, data, video, wide-area and local-area networks. This includes Internet, Intranet, wireless and radio communications, virtual satellite communications, narrow band radio, radio frequency communications, remote access and Voice over Internet Protocol (VoIP). The Division also assists in developing and implementing IA-wide telecommunications policy and future enhancements.

(b) The Division of Systems is responsible for maintenance and operation of all IA mainframe, midrange, and mini server hardware and software operations including, but not limited to OS/390, Unisys, Unix, Linux, Windows operating system, and Novell. The Division maintains and operates IA electronic messaging capabilities (e-mail and voice mail), database administration, Notes administration, Internet hosting and maintenance, Intranet hosting and maintenance, software distribution, and virus detection.

(c) The Division of Special IT Services provides specialized Information Technology services for wireless, law enforcement services, education, and land mobile radio programs.

(d) The Division of Disaster Recovery, located in Albuquerque, New Mexico, provides backup and recovery of selected IA mainframe and midrange servers, applications and Internet/Intranet access. The Division also provides technology refurbishment and replacement for Information Technology to include workstations and printers.

(e) The Division of User Services provides Level 1, Level 2, and Level 3 operations problem management resolution support and training for IA user workstations, network printers, and applications and web browsers. The Division also maintains and operates automated hardware and software inventory of IT connected to the BIA network. The Division provides resolution of IT incidents and requests for technology support including equipment refreshment. Field Information Technology staff at regional offices and agency offices report to the Chief, Division of User Services.