U.S. DEPARTMENT OF THE INTERIOR
OFFICE OF SURFACE MINING
RECLAMATION AND ENFORCEMENT

# DIRECTIVES SYSTEM

Subject Number: INF-11

Transmittal Number: 663

Date: MAR 12 1991

**Subject:** Information Resources Management Policies and Procedures Manual

**Approval:** [signature]

**Title:** Director

1. Purpose. The purpose of this directive is to provide practical, consistent guidelines for implementation of the Office of Surface Mining Reclamation and Enforcement (OSM), Information Systems Management Program.

   **NOTICE: THIS DIRECTIVE REFERS TO THE OSM ADP SERVICES OFFICE AS THE MANAGEMENT INFORMATION SYSTEMS DIVISION. READERS NOTE THAT UNTIL FURTHER NOTICE, THIS OFFICE WILL BE REFERRED TO AS THE ASSISTANT DIRECTOR, INFORMATION SYSTEMS MANAGEMENT.**

2. Applicability. This directive applies to all persons and OSM organizational units involved in Automatic Data Processing (ADP) hardware and software, telecommunications equipment and systems, and other information handling mediums.

3. Summary. The attached Information Resources Management (IRM) Policies and Procedures Manual is a comprehensive, consolidated document which describes the Information Systems Management organization, defines the IRM program, and identifies and explains policies and procedures relative to ADP, telecommunications, and data administration.

4. Policies and Procedures. The five chapters in the IRM Policies and Procedures Manual prescribes the goals, responsibilities, policies, and procedures for managing information systems, capabilities, services, and associated resources.

5. Reporting Requirements. None.

6. Effect on other Documents. Supersedes the following:

   a. Directive ADP-2, Bureau Information Resources Security program, dated March 8, 1988.

   b. Directive ADP-3, System Implementation Standards, dated September 1, 1986.

   c. Directive ADP-4, Standardization of Microcomputer Software, dated January 31, 1989.

d. Directive INF-11, Information Systems Management Program, dated October 26, 1982.

7. References. Information Resources Management Policies and Procedures Manual, Appendix B.

8. Effective Date. Upon issuance.

9. Contact. Assistant Director, Information Systems Management (202) 208-2916 or FTS 268-2916.

10. Keywords. Information Systems, Policy, ADP, Telecommunications, Hardware, Software, Computer.

11. Appendix. Information Resources Management Policies and Procedures Manual.

# OFFICE OF SURFACE MINING

# INFORMATION RESOURCES MANAGEMENT (IRM) POLICIES AND PROCEDURES MANUAL

Division of Management Information Systems
Office of Surface Mining
U.S. Department of the Interior

January 1991

**OFFICE OF SURFACE MINING**
**INFORMATION RESOURCES MANAGEMENT POLICIES AND PROCEDURES**

**TABLE OF CONTENTS**


| | | Page | Date of Last Update |
|---|---|---|---|
| I. | **MIS ORGANIZATION** | I–1 | |
| II. | **IRM PROGRAM MANAGEMENT** | II–1 | |
| | A. Program Definition, Goals, and Responsibilities | II–1 | Jan. 1991 |
| | B. IRM Policy and Program Coordination | II–5 | Jan. 1991 |
| | C. IRM Planning | II–9 | Jan. 1991 |
| | D. IRM Assessment Program | II–15 | Jan. 1991 |
| | E. Economic Analysis in Support of IRM Decisionmaking | II–19 | Jan. 1991 |
| | F. Information Resources Standards Program | II–21 | Jan. 1991 |
| | G. Information Resources Security Program | II–25 | Jan. 1991 |
| IV. | **AUTOMATED DATA PROCESSING (ADP)** | III–1 | |
| | A. ADP Acquisition | III–1 | Jan. 1991 |
| | B. ADP Cost Accounting, Cost Recovery, and Sharing | III–15 | Jan. 1991 |
| | C. Life-Cycle Management of ADP Information Systems | III–17 | Jan. 1991 |
| | D. ADP Resource Inventories | III–35 | Jan. 1991 |
| | E. Automated Information Systems Management Accountability | III–39 | Jan. 1991 |
| IV. | **TELECOMMUNICATIONS** | IV–1 | Jan. 1991 |
| V. | **DATA ADMINISTRATION** | V–1 | |

**OFFICE OF SURFACE MINING**
**INFORMATION RESOURCES MANAGEMENT POLICIES AND PROCEDURES**

## LIST OF APPENDICES


| | | Page |
|---|---|---|
| Appendix A | Office of Surface Mining ADP Documentation Content Guidelines | A–1 |
| Appendix B | Cumulative List of References | B–1 |
| Appendix C | Office of Surface Mining Management Information Systems Division Contacts | C–1 |

**OFFICE OF SURFACE MINING**
**INFORMATION RESOURCES MANAGEMENT POLICIES AND PROCEDURES**

## LIST OF FIGURES


| Figure | Description | Page |
|---|---|---|
| II–1 | Information Resources Management (IRM) Strategic Plan and Budget Formulation: Major Milestones | II–10 |
| II–2 | Applications Portability Profile (APP) Components | II–23 |
| III–1 | OSM Core Software for Microcomputers and Networks | III–4 |
| III–2 | DOI/OSM ADP Acquisition Threshold Summary | III–6 |
| III–3 | Department of the Interior System Life Cycle | III–19 |
| III–4 | Comparison of OSM Minimum Documentation Requirements | III–24 |
| III–5 | Summary of Minimum Documentation Requirements and Reference Numbers for OSM Level 1 | III–27 |
| III–6 | Summary of Minimum Documentation Requirements and Reference Numbers for OSM Level 2 | III–28 |
| III–7 | Summary of Minimum Documentation Requirements and Reference Numbers for OSM Level 3 | III–29 |
| III–8 | Summary of Minimum Documentation Requirements and Reference Numbers for OSM Level 4 | III–31 |

This page intentionally blank

# Chapter I

# MIS ORGANIZATION

# MIS ORGANIZATION

## 1. Purpose

This section describes the organization of the U.S. Department of the Interior (DOI) Office of Surface Mining (OSM) Management Information Systems Division (MIS).

## 2. Definitions

a. Terms

Information Resources Management. Coordination and direction of the planning, development, acquisition, and use of ADP hardware, software, telecommunications, and personnel/management functions for the purpose of managing the data and information required to fulfill the mission and goals of OSM.

b. Abbreviations

| | |
|---|---|
| ADP | Automated Data Processing |
| DOI | Department of the Interior |
| GSA | General Services Administration |
| IRM | Information Resources Management |
| MIS | Management Information Systems Division |
| OSM | Office of Surface Mining |

## 3. Policy/Procedures

a. Policy

Coordination and management of OSM information resources is provided by the MIS Division Chief, who reports to the Deputy Director for Administration and Finance. The MIS organization is described in OSM Directive OPM–11.

b. Procedures

Changes in the responsibilities of the MIS Division Chief will be effected through the OSM directives system and must be approved by the Director of the Office of Surface Mining.

c. Responsibilities

The MIS Division Chief is responsible for all IRM programs and activities at OSM, including establishing and maintaining policies and programs in the areas of IRM Planning, IRM Program Assessment, Economic Analysis and Life-Cycle

Management, Information Standards, and Information Resources Security. Specific program responsibilities are detailed in Chapter II of this manual.

**4. Reporting Requirements**

The DOI Departmental Manual specifies reporting requirements for various components of the OSM IRM program. The MIS Division Chief is the Agency IRM Coordinator and, as such, provides the IRM reports required of OSM by DOI, GSA, and others.

**5. References**

Department of the Interior Departmental Manual, Organization of Office of IRM, 110 DM 10.

OSM Directive OPM–11, Information Systems Management Directorate Organization and Functional Statements.

**6. Effect on Other Documents**

None

**7. Effective Date**

Upon issuance

**8. Contact**

MIS Division Chief

# Chapter II

# IRM PROGRAM MANAGEMENT

# IRM PROGRAM MANAGEMENT

## A. PROGRAM DEFINITION, GOALS, AND RESPONSIBILITIES

### 1. Purpose

This section defines the Office of Surface Mining (OSM) Information Resources Management (IRM) program and identifies associated goals and responsibilities.

### 2. Definitions

a. Terms

Information Resources Management. Coordination and direction of the planning, development, acquisition, and use of ADP hardware, software, telecommunications, and personnel/management functions for the purpose of managing the data and information required to fulfill the mission and goals of OSM.

b. Abbreviations

| | |
|---|---|
| ADP | Automated Data Processing |
| DOI | Department of the Interior |
| IRM | Information Resources Management |
| MIS | Management Information Systems Division |
| OSM | Office of Surface Mining |

### 3. Policy/Procedures

a. Policy

1) The goals of the OSM IRM program are as follows:

- Provide responsible analytical and systems support as required to assist program managers in meeting the various OSM missions.
- Coordinate systems within OSM to prevent or minimize duplication of data and functions and to provide compatibility where feasible.
- Conserve resources and meet identified support needs through the most economical and efficient means available.
- Ensure compliance with regulatory requirements.

- Assist the States in sharing technological advances in the field of information systems as related to the OSM mission in administering Public Law 95–87, the Surface Mining Control and Reclamation Act of 1977 (SMCRA).

2) Some IRM responsibilities may be delegated to other OSM assistant directorates. For example, in some instances ADP procurement authority has been delegated to the field. When IRM responsibilities are delegated, the assistant directorates receiving the IRM control and responsibility will be required to be aware of and comply with pertinent policies and regulations promulgated by OSM, DOI, and/or other Federal authorities. The MIS Division Chief will provide oversight and guidance as needed.

3) The MIS Division Chief is responsible for maintaining a staff with a level of technical and management IRM skills commensurate with IRM requirements.

b. Procedures

None

c. Responsibilities

1) The MIS Division Chief is responsible for the following:

a) Establishing OSM policies for ADP and program informational activities consistent with DOI and Federal requirements.

b) Collecting, maintaining, analyzing, and disseminating data, statistics, and program information in support of the OSM mission.

c) Developing, in a cost-effective manner, new or enhanced management information systems and computer technologies to support new or continuing OSM missions.

d) Identifying and evaluating emerging ADP technologies to support OSM administrative, technical, and programmatic needs.

e) Ensuring that existing management information systems and computer technologies are operated and maintained in an efficient manner in support of the OSM mission.

f) Where required by OSM mission needs, providing support for the management information systems and computer technology requirements of the State regulatory authorities.

2) When delegated IRM authority, Assistant Directors are responsible for:

a) Within the assistant directorate, ensuring compliance with OSM, DOI, and Federal IRM policies and regulations.

b) Maintaining a level of technical and management skills commensurate with mission requirements. To this end, Assistant Directors must maintain an environment that fosters staff development. An essential part of this development is training. Depending upon individual skill levels and professional requirements, training in the following areas may be beneficial:

- Use of commercial software packages
- Application development using a specific package or language
- Hardware
- Telecommunications
- System development life-cycle activities, including training in system development and project management.

A number of options are available for training: vendor-supplied training courses; training developed in-house; or classroom, self-study, hands-on, and computer-based training.

## 4. Reporting Requirements

None

## 5. References

Department of the Interior Departmental Manual, Part 375 DM 1, IRM Program Management—Program Definition, Goals, Responsibilities.

OSM Directive OPM–11, Information Systems Management Directorate Organization and Functional Statements.

Office of Management and Budget, OMB Circular A–130, Management of Federal Information Resources.

General Services Administration, Federal Information Resources Management Regulations.

## 6. Effect on Other Documents

Supersedes OSM Directive INF–11, Information Systems Management Program, 26 October 1982.

## 7. Effective Date

Upon issuance

**8. Contact**

MIS Division Chief

## B. IRM POLICY AND PROGRAM COORDINATION

### 1. Purpose

This section describes the development and implementation of Office of Surface Mining (OSM) Information Resources Management (IRM) policies and procedures. It also describes the program coordination organizations available to facilitate this development and implementation.

### 2. Definitions

a. Terms

IRM Coordinator. Individual appointed by an Assistant Director to serve as the focal point for IRM communication within and across assistant directorates. This includes planning, developing, implementing, and monitoring IRM activities within the assistant directorate.

b. Abbreviations

| | |
|---|---|
| ADP | Automated Data Processing |
| DOI | Department of the Interior |
| GSA | General Services Administration |
| IRM | Information Resources Management |
| MIS | Management Information Systems Division |
| OMB | Office of Management and Budget |
| OSM | Office of Surface Mining |

### 3. Policy/Procedures

a. Policy

This OSM IRM Policies and Procedures Manual is the authority by which IRM program policy at OSM is established. The OSM IRM program is coordinated and managed by the MIS Division Chief, and all other assistant directorates actively participate in the program. OSM IRM program policy is issued through the OSM directives system. In accordance with the directives system, changes to IRM policy will be initially issued in draft form, will be available for review by interested OSM employees, and will be issued in final form after incorporation of comments. Through the directives system, copies of the directive will be furnished to the DOI Office of Information Resources Management within 30 days of issuance.

To facilitate effective management of information resources, IRM policy development and implementation will be coordinated throughout OSM and with other agencies. To this end, participation in Federal and industry information systems organizations is encouraged.

Primary OSM IRM coordination organizations include:

1) Management Information Systems Field Liaison Program

To facilitate communication throughout OSM, the MIS Field Liaison Program has been established. Each Field Office Director and each Assistant Director is responsible for appointing one or more IRM Coordinators to participate in this program. IRM Coordinators will meet at least twice each year to discuss activities pertinent to ADP and IRM issues across OSM. The MIS Division Chief oversees the MIS Field Liaison Program.

2) MIS Field Liaison Subcommittees

Informal ADP-issue-specific subcommittees have been formed to provide input and comments from a user and field perspective on issues of interest to IRM Coordinators throughout OSM. These groups work with the MIS Field Liaison Program to provide assistance to the MIS Division Chief on ADP issues.

3) OSM ADP System User Groups

A user group is an organization established to communicate application-specific information between the user community and the application developers and/or maintenance personnel. The information communicated relates to the development, use, and planned or potential enhancements of an application system. Official points of contact for OSM user groups formed for major information systems developed for OSM will be established through the MIS Division Chief.

4) Other Government and Industry Organizations and Associations

The MIS Division Chief will ensure that OSM obtains important information regarding current trends in information management and will disseminate this information to affected OSM organizations. The MIS Division Chief will also ensure appropriate OSM participation in departmental and other Government and industry organizations and councils. Examples of these groups are:

Federal and Interdepartmental—
- Departmental-Level Working Group on IRM (Policy), chaired by OMB
- Interagency Telecommunications Committee (advisory committee to GSA)
- Interagency Committee on Automated Data Processing
- Subcommittee: Federal ADP Users Group
- Information Resources Council, established by DOI
- Integrated Software Federal User Group (ISFUG)

Department-Wide/Inter-Bureau—
- Interior Digital Cartographic Coordinating Committee
- Earth Science Data Standards Council

- Information Resources Management Forum (principal internal DOI assembly for program review and advice)

Industry—
- Product-specific user groups (for example, WordPerfect User Support Group).

b. Procedures

1) Any OSM employee may suggest changes to, or comment on, current and/or potential policies and procedures. In commenting on IRM policy and procedures changes:

a) If the comments relate to a draft OSM directive, provide comments in accordance with the memorandum transmitting the draft.

b) If comments relate to an IRM policy/procedure currently in effect or a suggested (new) policy/procedure, send them to the MIS Division Chief.

2) To attend meetings or join IRM organizations and attend meetings/workshops, contact your local IRM Coordinator or the MIS Division Chief.

c. Responsibilities

1) The MIS Division Chief is responsible for overall IRM policy and program coordination, including:

a) Keeping Deputy Directors, Assistant Directors, and Field Office Directors informed of relevant MIS activities through personal contact, periodic newsletters, on-site visits, and chairing ADP user group meetings.

b) Providing a single point of contact and direct hands-on assistance for expeditious handling of user problems.

c) Meeting with IRM Coordinators periodically to help plan and review system development activities.

d) Coordinating field development efforts to share development activities among the field offices.

e) Evaluating proposed systems to determine if they have value at other field locations or throughout OSM and assuming responsibility for further systems development.

f) Working closely with IRM Coordinators to ensure compliance with configuration management processes, documentation standards, security issues, etc.

g) Helping to ensure that all personnel receive training on new software packages, upgrades to core software, etc.

2) Assistant Directors are responsible for appointing and supporting IRM Coordinators.

3) IRM Coordinators are responsible for:

a) Attending IRM Coordinator meetings.

b) Coordinating, assisting, and informing user organizations with respect to information resources management.

## 4. Reporting Requirements

The MIS Division Chief must be informed when IRM Coordinator appointments are made or are changed. The coordinator's name, organization, position title, address, and FTS number should be supplied upon appointment.

## 5. References

Department of the Interior Departmental Manual, Part 375 DM 2, Information Systems Management—IRM Policy and Program Coordination.

Paperwork Reduction Act (44 USC 3506(c)(8)).

## 6. Effect on Other Documents

None

## 7. Effective Date

Upon issuance

## 8. Contact

MIS Division Chief

## C. IRM PLANNING

### 1. Purpose

This section describes the Information Resources Management (IRM) planning process and provides policy and procedural guidance for planning the acquisition and use of information resources. It identifies the Office of Surface Mining (OSM) organizational elements involved in planning and sets forth their respective responsibilities.

### 2. Definitions

a. Terms

IRM Strategic Plan. Document identifying the long-term direction to be followed by OSM for cost-effective use of information resources in support of the OSM mission and programs.

b. Abbreviations

| | |
|---|---|
| ADP | Automated Data Processing |
| DOI | Department of the Interior |
| IRM | Information Resources Management |
| MIS | Management Information Systems Division |
| OSM | Office of Surface Mining |

### 3. Policy/Procedures

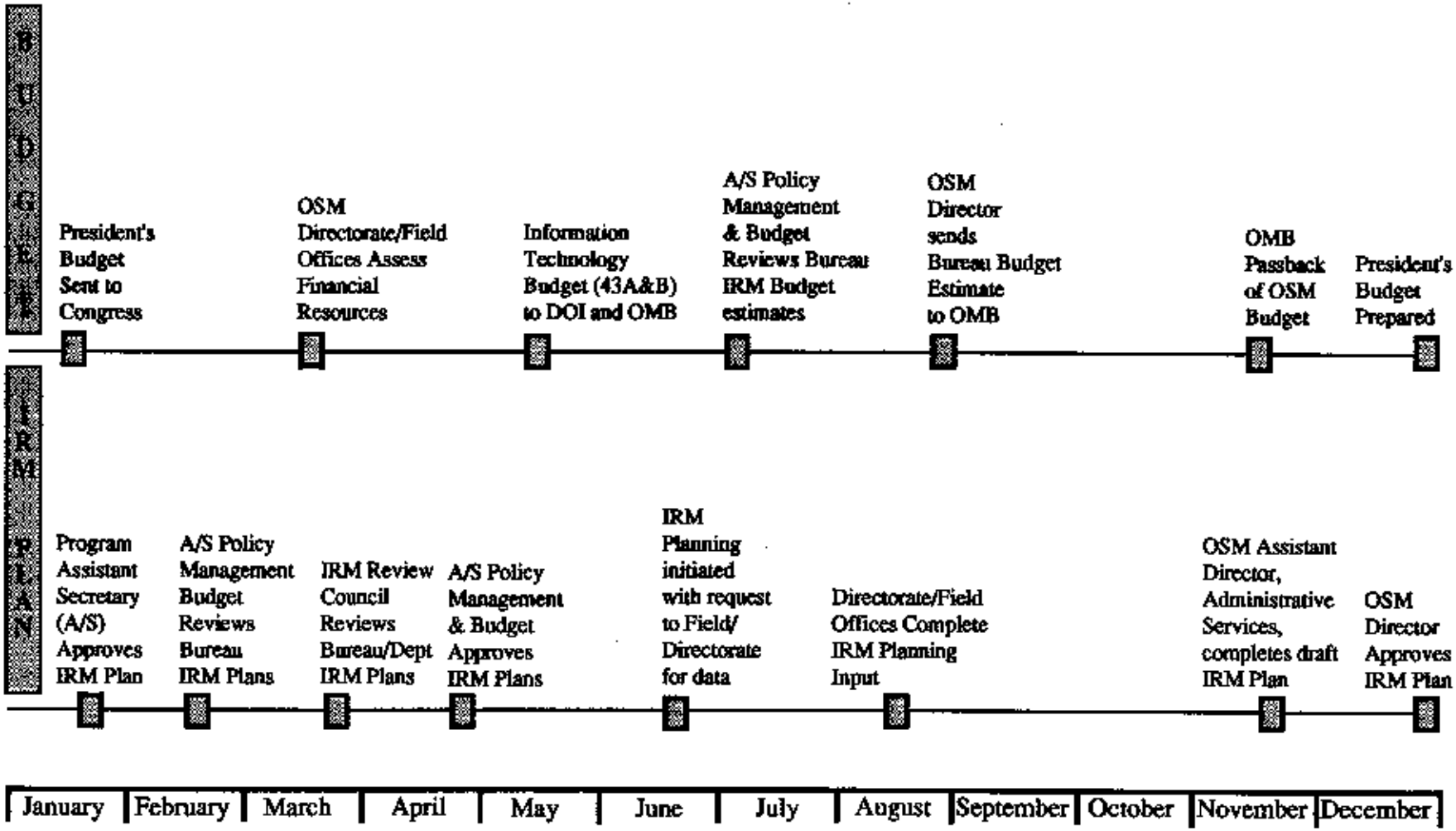
a. Policy

1) The MIS Division Chief will develop, maintain, and annually update an OSM IRM Strategic Plan. This plan will be integrated with mission plans and budget strategies and will serve as the basis for developing or acquiring information resources. The annual plan will be developed in accordance with the schedule established by the DOI Office of Information Resources Management (see Figure II–1).

2) The IRM Strategic Plan will identify the OSM IRM goals for the next 5 years, identify progress against the objectives of the previous annual submission, and identify initiatives and projects with budget requirements and timelines for accomplishing the new or revised strategic IRM objectives.

3) The MIS Division Chief will also develop an annual ADP and Telecommunications Acquisition Plan in accordance with OSM Directive PRC–4, Advance Procurement Planning. The annual ADP and Telecommunications Acquisition Plan will be incorporated into the IRM Strategic Plan. OSM will use the

**Figure II–1**
**INFORMATION RESOURCES MANAGEMENT (IRM) STRATEGIC PLAN AND BUDGET FORMULATION: MAJOR MILESTONES**



combined plans as the basis for developing statements of work, specifications, and requisitions for procurement action to acquire information resources.

b. Procedures

1) Field offices and assistant directorates will prepare the following planning input and provide it to the MIS Division Chief by 31 December of each year:

- Description of deficiencies and problems related to IRM.
- Identification and description of opportunities for using information resources to improve productivity.
- A Five-Year ADP and Telecommunications Acquisition Plan
- Plans within the activity to acquire or develop information resources through (at a minimum) the *next* fiscal year. This should cover all plans for information collection, application systems modernization and maintenance, data bases, ADP technology, ADP facilities, telecommunications, office automation, records management, support services, and information dissemination.

  The plans should be consistent with anticipated budgets and should include the following:

  Application/Project Name
  Functional Description
  Anticipated Software Environment
  (for example, operating system required, programming language)
  Anticipated Hardware Requirements
  (for example, CPU required, memory and storage requirements)
  Planned Installation Date
  Estimated Level of Effort/Cost
  - One-Time/Installation Costs:
    - OSM Employee Effort/Cost
    - Contractor Effort/Cost
    - Equipment/Software Cost
    - Other Cost
  - Recurring/Monthly Costs:
    - OSM Employee Effort/Cost
    - Contractor Effort/Cost
    - Equipment/Software Cost
    - Other Cost

  Anticipated Documentation Level
  (see Section III.C, Life-Cycle Management of ADP Information Systems)
  Developer(s)
  OSM Technical Project Officer (Name, Position, FTS Number)
  OSM IRM Project Coordinator (Name, Position, FTS Number)

2) Each year, the MIS Division Chief will revise the OSM IRM Strategic Plan and develop an ADP and Telecommunications Acquisition Plan in accordance with guidance set forth in the Departmental Manual (375 DM 4) and OSM Directive PRC–4. This process will include evaluating the prior year's performance with respect to attainment of goals; reviewing and updating the summary of current problems and deficiencies; and refining short- and long-term objectives and goals based upon OSM-specific information needs, available resources, and industry-wide information management and technology trends. The draft IRM Strategic Plan will be prepared by the ISM Assistant Directorate in accordance with the schedule set forth in 375 DM 4. Upon DOI approval, the OSM IRM Strategic Plan will be available for dissemination throughout OSM.

c. Responsibilities

1) The MIS Division Chief is responsible for:

a) Coordinating the development, maintenance, and updating of the annual OSM IRM Strategic Plan.

b) Providing input as required for the DOI IRM Strategic Plan.

c) Preparing an Advance Procurement Plan, as required.

2) Field Office Directors are responsible for:

a) Obtaining the Assistant Director's approval for the acquisition and use of information resources within the field office.

b) Providing field office input to the IRM strategic planning process in accordance with the procedures set forth in section II.C.3.b above.

3) Assistant Directors are responsible for:

a) Mission-related program planning for programs that may involve ADP technology.

b) Providing assistant directorate input to the IRM strategic planning process in accordance with the procedures set forth in section II.C.3.b above.

**4. Reporting Requirements**

As described in section II.C.3 above:

1) Field Office Directors and Assistant Directors will provide input to the IRM strategic planning process by 31 December of each year. The input will be provided to the MIS Division Chief.

2) The MIS Division Chief will prepare and maintain an IRM Strategic Plan in accordance with the requirements of 375 DM 4.

## 5. References

Department of the Interior Departmental Manual, Part 375 DM 4, IRM Program Management—IRM Strategic Planning.

Federal Manager's Financial Integrity Act.

Federal Information Resources Management Regulation Subpart 201–19, Triennial Review of Agency Administration and Operation of Information Resources Management Activities.

Office of Management and Budget, OMB Circular A–130, Management of Federal Information Resources, 24 Dec 1985.

Paperwork Reduction Act (44 USC 3506(c)(8)).

OSM Directive PRC–4, Advance Procurement Planning.

## 6. Effect on Other Documents

None

## 7. Effective Date

Upon issuance

## 8. Contact

MIS Division Chief

This page intentionally blank

## D. IRM ASSESSMENT PROGRAM

### 1. Purpose

This section describes the Office of Surface Mining (OSM) Information Resources Management (IRM) assessment program, which is required by Federal policies and procedures.

### 2. Definitions

a. Terms

Internal Controls. The steps taken to provide reasonable assurance that obligations and costs are in compliance with applicable law; funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.

IRM Review. Agency review of IRM activities to ensure that these are carried out in an efficient, effective, and economical manner. Selective reviews of agency IRM activities are also performed by OMB, together with GSA, at least once every 3 years to assess their adequacy and efficiency.

b. Abbreviations

| | |
|---|---|
| ADP | Automated Data Processing |
| DOI | Department of the Interior |
| GSA | General Services Administration |
| IRM | Information Resources Management |
| MIS | Management Information Systems Division |
| OMB | Office of Management and Budget |
| OSM | Office of Surface Mining |

### 3. Policy/Procedures

a. Policy

1) OSM will prepare an Annual Review Assessment Plan for conducting periodic reviews of IRM activities such as telecommunications, end-user computing, software management, information management, and electronic filing.

2) OSM will periodically assess IRM activities to ensure their adequacy and efficiency. This assessment will include an evaluation of the ability of systems to meet internal control objectives for the following:[1]

Information Collection
- Information collected is meaningful and useful.
- Information collected is reliable.
- Information is arranged in an orderly fashion.
- Information is maintained on a current basis.

Correspondence Handling
- Correspondence is channeled to the appropriate parties.
- Replies are made promptly, accurately, and responsively.

Records Maintenance
- Records are readily available.
- Records are adequately protected.
- Only necessary records are maintained.

ADP
- Proper authorization of transaction inputs, adequate edit checks, and necessary safeguards of sensitive input forms ensure accurate, proper, complete, and timely entry of information.
- Adequate security measures prevent unauthorized system access or improper changes to or loss of data.
- Appropriate controls can detect unauthorized use of the system.
- Outputs are produced accurately, completely, and on time.

b. Procedures

1) The IRM Reviews will be conducted by the operations staff in accordance with established guidelines on IRM.

2) The internal control objectives will be evaluated during Federal Manager's Financial Integrity Act (FMFIA) reviews.

c. Responsibilities

The MIS Division Chief is responsible for:

1) Establishing and maintaining an internal IRM assessment program.

2) Establishing and providing reporting mechanisms as required by the DOI implementation of the Federal IRM Review Program.

---

[1] Source: Executive Office of the President, Office of Management and Budget, Internal Control Guidelines, December 1982.

3) Participating in and providing required information for compliance assessments conducted by the DOI Office of Information Resources Management.

4) Providing plans to the Director of the DOI Office of Information Resources Management for assessments to be conducted during a fiscal year as required by the DOI Office of Information Resources Management as part of the review process mandated by the Paperwork Reduction Act.

5) Responding to and initiating follow-up actions relating to the findings and recommendations included in internal and DOI assessment reports.

## 4. Reporting Requirements

Annual schedule of assessments is submitted to GSA as part of the Federal IRM Review Program and the triennial IRM review process required by the Paperwork Reduction Act.

## 5. References

Department of the Interior Departmental Manual, Part 375 DM 5, IRM Program Management—IRM Assessment Program.

General Services Administration, Federal Information Resources Management Regulations (FIRMR) Supplement, Federal IRM Review Handbook, 1985. See also Appendix B, Regulatory References.

Paperwork Reduction Act of 1980 (44 USC 3501 et. seq.)

Office of Management and Budget, OMB Circular A–130, Management of Federal Information Resources, 24 Dec 1985.

Internal Control Guidelines 1982.

## 6. Effect on Other Documents

None

## 7. Effective Date

Upon issuance

8. **Contact**

MIS Division Chief

## E. ECONOMIC ANALYSIS IN SUPPORT OF IRM DECISIONMAKING

### 1. Purpose

This section provides guidance for use in conducting economic analyses in support of Office of Surface Mining (OSM) Information Resources Management (IRM) decisions.

### 2. Definitions

a. Terms

Economic analysis. An assessment of the economic considerations, both costs and benefits, for an ADP project; provides information for rational decisionmaking and establishes a common base for making comparisons of alternative methods for achieving the goal of the project.

b. Abbreviations

| | |
|---|---|
| ADP | Automated Data Processing |
| DOI | Department of the Interior |
| IRM | Information Resources Management |
| MIS | Management Information Systems Division |
| OSM | Office of Surface Mining |

### 3. Policy/Procedures

a. Policy

All ADP development projects and procurements for hardware, software, and/or services will be analyzed to ensure that they are economically feasible and justifiable.

b. Procedures

Cost/benefit analyses will be conducted in accordance with Federal, DOI, and OSM guidance (see references and also Appendix A, OSM ADP Documentation Requirements, outline for Cost/Benefit Analysis).

c. Responsibilities

1) The MIS Division Chief is responsible for ensuring that OSM ADP investments are economically feasible and justifiable.

2) Subject to delegation of ADP procurement authority from the MIS Division Chief, Assistant Directors and Field Office Directors are responsible for ensuring that cost/benefit analyses for ADP development/acquisition projects

under their purview are conducted in accordance with applicable guidance (see references and Appendix A).

## 4. Reporting Requirements

Assistant Directors shall ensure that appropriate cost/benefit analyses are forwarded to the MIS Division Chief along with other documentation supporting the request for approval.

## 5. References

Department of the Interior Departmental Manual, Part 375 DM 7, IRM Program Management—Economic Analysis in Support of IRM Decision Making.

Department of the Interior, A Project Manager's Guide to Benefit/Cost Analysis of Information Technology Investments, January 1989.

Department of the Navy, Naval Data Automation Command, Publication 15, Economic Analysis Procedures for ADP.

Office of Management and Budget, OMB Circular A–11, Preparation and Submission of Budget Estimates, Section 43.2.

Federal Information Processing Standard Publication 64, Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase, August 1979.

## 6. Effect on Other Documents

None

## 7. Effective Date

Upon issuance

## 8. Contact

MIS Division Chief

## F. INFORMATION RESOURCES STANDARDS PROGRAM

### 1. Purpose

This directive describes the development, application, and maintenance of technical standards for Office of Surface Mining (OSM) Information Resources Management (IRM).

### 2. Definitions

a. Terms

American National Standards Institute (ANSI). The principal organization forming standards in the United States. Formed in 1918, it is a nonprofit, nongovernmental organization.

Federal Information Processing Standards (FIPS). Standards developed under the Federal Government's standardization program and concerned with computer sciences, telecommunications, and information management.

International Standards Organization (ISO). A non-treaty organization founded in 1947 and currently comprised of nearly 90 member nations. Each nation assigns its principal standardization body to the ISO. ANSI represents the United States.

Voluntary standards. Standards that are established generally by private sector bodies and are available for use by any person or organization, private or governmental. They are commonly referred to as "industry standards" or "consensus standards" and do not include standards of professional conduct, institutional codes of ethics, private standards of individual firms, or standards mandated by law.

b. Abbreviations

| | |
|---|---|
| ADP | Automated Data Processing |
| DOI | Department of the Interior |
| IRM | Information Resources Management |
| MIS | Management Information Systems Division |
| OSM | Office of Surface Mining |

### 3. Policy/Procedures

a. Policy

If cost-effective and consistent with applicable laws and regulations, standards used in OSM will be based on existing Federal, DOI, and OSM standards—in that order. Where these standards are not cost-effective or are nonexistent, the use of

voluntary (industry) standards is preferred in lieu of developing in-house standards.

b. Procedures

1) OSM organizations will consider Federal, DOI, and OSM standards when evaluating and selecting information resources for use at OSM (see also section III.A, ADP Acquisition). Specific Federal or adopted standards important to improving applications portability are detailed in Figure II–2. Should an organization find that a particular standard is not cost-effective or is inconsistent with applicable laws or regulations, a request to disregard the standard will be submitted to the MIS Division Chief. This request shall include specific references, cost justifications, and other explanations as appropriate.

2) OSM employees with advice regarding proposed standards, the introduction of new standards, revisions to existing standards, or requests for waivers should contact the MIS Division Chief.

3) At least once every 3 years, OSM standards will be reviewed to determine their continued applicability and economic benefit.

c. Responsibilities

1) The MIS Division Chief is responsible for:

a) Implementing and maintaining Federal and DOI IRM standards.

b) Providing advice on proposed standards, the necessity of new standards, needed revisions, and requests for waivers.

c) Developing and implementing an OSM IRM standards program and standards to supplement Federal and DOI standards.

d) Ensuring that OSM IRM standards are reviewed at least once every 3 years.

e) Establishing liaison between DOI and OSM on matters related to the development and implementation of IRM standards.

f) Maintaining an inventory of IRM standards and standards groups in which OSM participates.

2) Assistant Directors are responsible for ensuring that information resources leased or acquired conform with applicable Federal, DOI, and OSM standards.

**Figure II–2. APPLICATIONS PORTABILITY PROFILE (APP) COMPONENTS**

| Function | ADP Element | Standard |
|---|---|---|
| Operating System | POSIX | FIPS 151–1 |
| | xl | IEEE P1003.2 |
| Data Base Management | SQL | FIPS 127 |
| | IRDS | X3.138 (Proposed FIPS) |
| Data Interchange: | | |
| Business Graphics | GKS and CGM | FIPS 120, 128 |
| Product Data | IGES | NBSIR 86–3359 |
| Document Processing | SGML | ISO 8879–1986 |
| | ODA/ODIF | ISO/DIS 8613 |
| Network Services: | | |
| Data Communications | OSI | FIPS 146 (GOSIP) |
| File Management | NFS | IEEE P1003.X |
| User Interface | X Window System | X3H3.6 (Proposed FIPS) |
| Languages | | CX3J11 draft X3.159 |
| | COBOL | FIPS 021–2 |
| | FORTRAN | FIPS 069–1 |
| | Ada | FIPS 119 |
| | Pascal | FIPS 109 |

**ACRONYM DEFINITIONS**

| | |
|---|---|
| CGM | Computer Graphics Metafile |
| FIPS | Federal Information Processing Standard |
| GKS | Graphics Kernel System |
| GOSIP | Government Open Systems Interconnection Profile |
| IEEE | Institute of Electrical and Electronics Engineers |
| IGES | Initial Graphics Exchange Specification |
| IRDS | Information Resource Dictionary System |
| ISO | International Standards Organization |
| NFS | Network File System |
| ODA/ODIF | Office Document Architecture/Office Document Interchange Format |
| OSI | Open Systems Interface |
| POSIX | Portable Operating System Interface for Computer Environments |
| SGML | Standard Generalized Markup Language |
| SQL | Structured Query Language |

## 4. Reporting Requirements

None

## 5. References

Department of the Interior Departmental Manual, Part 375 DM 12, IRM Program Management—Information Resources Standards Program.

DOI Strategic Framework, July 1988.

Federal Information Processing Standards (FIPS).

American National Standards Institute (ANSI).

Institute of Electrical and Electronics Engineers (IEEE).

International Organization for Standardization (IOS).

Electronic Industries Association (EIA).

National Institute of Standards and Technology (NIST) (develops FIPS).

Federal Telecommunications Standards Committee.

International Telegraphic and Telephone Consultative Committee (CCITT).

## 6. Effect on Other Documents

None

## 7. Effective Date

Upon issuance

## 8. Contact

MIS Division Chief

## G. INFORMATION RESOURCES SECURITY PROGRAM

### 1. Purpose

This section defines policies, assigns responsibilities, and prescribes procedures for management of the Office of Surface Mining (OSM) Information Resources Security Program. The purpose of the program is to protect OSM's information resources against loss, theft, natural disasters such as fire or flood, improper use, unauthorized access or disclosure, alteration, manipulation, violations of confidentiality, physical abuse, or unlawful destruction.

### 2. Definitions

a. Terms

Information. Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained on paper or in media such as computerized data bases, microform, or magnetic tape.

Information Resources. The personnel, technology (hardware and software), and monetary allowance used to create, collect, store, use, and disseminate information.

Information Resources Security. The management controls and safeguards designed to protect information resources and ensure the continued performance of governmental activities during emergency situations.

Information System. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

Information Technology Facility. An area containing the technological resources used to collect, process, store, transmit, disseminate, and/or retrieve information in the form or format needed. Technological resources consist of large, medium, and small data processing systems (including mainframe, mini-, and micro- computers); peripheral and storage units; office automation equipment such as word processors and copiers; telecommunications equipment (for example, switches and networks); and the associated software for these types of equipment.

Information Technology Installation. One or more information technology facilities within close physical proximity which, from a management viewpoint, are logically considered a single entity.

Data. A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.

Data Base. A collection of data fundamental to a system or an enterprise.

Data Base Administrator. The individual responsible for managing the design and implementation of data base structures to maximize efficiency and effectiveness with regard to processing time and storage requirements.

Sensitive Information/Data. Information or data that requires protection due to the risk and magnitude of loss or harm that would result from inadvertent or deliberate disclosure, alteration, or destruction. The term includes information or data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission; proprietary data; records about individuals that require protection under the Privacy Act; and data not releasable under the Freedom of Information Act.

Sensitive Computer Application. A computer system that processes sensitive data or requires a degree of protection due to the magnitude of loss, risk, or harm that could result from inadvertent or malicious manipulation of the application.

Records. All written, machine-readable, audio-visual, and other documentary materials, regardless of physical form or characteristics, made or received by OSM in pursuance of Federal laws or in connection with the transaction of public business and preserved or appropriate for preservation as evidence of the organization and its functions, policies, decisions, procedures, operations, or other activities, or because of the informational value of the recorded data.

System of Records. As defined by the Privacy Act of 1974: "A group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

Vital Records. Records or information deemed necessary to ensure continuity of essential governmental activities during national emergency conditions. Records essential to the protection of the rights and interests of OSM and of the individuals for whose rights and interests it has responsibility.

System Owners. Individuals responsible for acquisition or development and/or the primary user of microcomputer systems, office automation systems, application systems, data bases, and/or manual information systems.

Risk Analysis. The process used to establish the value of assets, review potential threats to those assets, and determine the cost of reasonable safeguards to protect them from damage or loss.

Continuity of Operations Plan. A plan to ensure support to users of information systems during interruptions, emergencies, and disasters.

b. Abbreviations

| | |
|---|---|
| ADP | Automated Data Processing |
| BIRSA | Bureau Information Resources Security Administrator |
| COOP | Continuity of Operations Plan |
| DOI | Department of the Interior |
| GSA | General Services Administration |
| IIRSO | Installation Information Resources Security Officer |
| MIS | Management Information Systems Division |
| OSM | Office of Surface Mining |

## 3. Policy/Procedures

a. Policy

The OSM Information Security Program will ensure that adequate measures are established to provide an appropriate level of protection for the information resources under OSM's authority. The program complies with all Federal policies, procedures, and standards governing information resources security. The provisions of this policy shall:

1) Combine all the requirements and responsibilities for manual and automated information resources security into one policy and establish responsibilities and procedures for the development, administration, and maintenance of an information resources security program for OSM.

2) Apply to all OSM divisions and offices and their employees and to the personnel and facilities of contractors providing information resources support to OSM.

3) Concern information that is not related to national security. (National security issues are subject to more stringent security policies and procedures.)

4) Pertain to, but are not limited to, the following:

   a) Information created, transmitted, stored, processed, or disseminated in any media or form (for example, magnetic tape, microfilm, paper documents).

   b) Information in any form when used as input to or retrieved from an information system.

   c) Information technology facilities used in the collection, processing, storage, communication, and retrieval of information.

   d) Other technical systems, such as supervisory process control systems (except those identified in the Department of Defense Authorization Act of 1982).

e) The processes, procedures, and software involved in any of the above activities.

b. Procedures

Successful implementation of an information resources security program is dependent upon accurately determining potential risks and instituting safeguards to minimize them. Every OSM information system and every information technology facility operated by or on behalf of OSM must be protected. System owners and resource managers are responsible for the protection of information systems and facilities under their control. The following activities will be performed to ensure that all systems are protected.

1) Risk Analysis. Conducting a risk analysis is the first step in establishing a security plan. Risk analyses must be conducted for all information technology facilities, all automated application systems, and all manual application systems covered by the Privacy Act. The extent of the risk analysis performed should be commensurate with the magnitude and use of the resources to be protected. Guidance for performing a risk analysis can be found in the National Bureau of Standards (NBS) Federal Information Processing Standards (FIPS), Publications 31 and 65.

a) Information Technology Facilities and Automated Application Systems. A risk analysis shall be conducted at least every 5 years if one has not been conducted within that timeframe under the following special circumstances: when planning the development of a new system or facility, when significant changes are made to the nature or relative sensitivity of data being processed or to the system or facility, and when environmental factors change in such a manner as to alter the threats presented. For automated systems processing sensitive data (such as information covered by the Privacy Act), a risk analysis should be conducted when the configuration on which the information is operated changes so as to create the potential for either greater or easier access.

b) Manual System of Records. A risk analysis shall be performed when a new system of records is proposed under the Privacy Act or when a proposed change to an existing system significantly alters the character of the system by increasing or changing the number or types of individuals on whom records are maintained; expands the types or categories of information maintained; alters the purposes for which the information is used; or exempts records maintained on individuals from any provision of the Privacy Act.

2) Protection. Specific safeguards should be employed to provide a reasonable way to counteract each threat described in the risk analysis and to detect actual or potential security violations. At a minimum, the following procedures must be considered:

a) Physical Security. Appropriate practices and safeguards must be used to minimize the following threats to those places where information and technological resources are located: theft, unauthorized or illegal access, accidental or intentional damage or destruction, improper use, and improper disclosure of information.

b) Personnel Security. Appropriate Federal and contractor employees shall receive security clearances commensurate with the sensitivity of the information or ADP facilities they manage or use. Supervisors are responsible for determining the sensitivity of positions in their areas. System owners are responsible for ensuring that Federal personnel and contractors managing or using systems in their areas have appropriate sensitivity clearances. The criteria for determining sensitivity levels and the procedures for initiating sensitivity clearances are contained in OSM Directive PER–13, Personnel Security Program. Supervisors are responsible for ensuring that employees who use information and technological resources sign statements acknowledging their responsibility for the security of these resources. These statements shall be retained in the employee's official personnel folder.

c) Technical Security. Appropriate safeguards (such as passwords, encryption, and security software) shall be used to prevent unauthorized access to and use of information, data, and software resident on peripheral devices or storage media or in the process of communication via technological means.

d) Administrative Security. Procedures to ensure that all information resources are properly protected and that information technology resources are used only by authorized personnel and for official use only shall be established and disseminated.

3) Automated Application Safeguards. The following specific procedures must be followed to ensure that appropriate safeguards are incorporated into automated application systems.

a) Determine appropriate security safeguards prior to system development or acquisition.

b) Conduct design reviews and system tests prior to system implementation to ensure that the system satisfies the approved security requirements.

c) Certify before implementation that a new system satisfies applicable policies, regulations, and standards and that its security safeguards are adequate.

d) Evaluate the adequacy of security safeguards for existing sensitive systems at least every 3 years.

4) Continuity of Operations Planning

a) Information Technology Facilities and Automated Application Systems. Facility managers and system owners are responsible for developing a Continuity of Operations Plan for each information technology facility and each automated application system under their control to ensure that interruptions of service of whatever type or duration are kept to a minimum. The COOP shall be evaluated periodically to determine the continued adequacy of the established procedures. The COOP shall be revised when indicated by changes in software, equipment, or other related factors. At a minimum, the COOP shall address the following:[2]

- Procedures for backup storage and recovery of data and software
- Processing capabilities and procedures for transferring operations to an alternate site
- Consistency between application system COOPs and the COOP of the information technology facility where the application is processed
- Annual testing of the COOP at large ADP mainframe installations and other installations that provide essential ADP support.

b) Manual Application Systems. A Continuity of Operations Plan must be developed for each manual application system that contains vital records to ensure its continued protection and to ensure that essential OSM activities continue during periods of national emergency. These plans shall be reviewed annually and periodically tested under emergency conditions to ensure their adequacy.

5) Security Awareness Activities. All OSM employees must be adequately trained to fulfill their security responsibilities. All contractor personnel must be advised of OSM security requirements and regulations. The level of security awareness activities in which employees participate shall depend upon their specific involvement with information resources. Supervisors are responsible for ensuring that employees participate in one or more of the following levels of security awareness activities and that a record of this participation is retained in official personnel folders:

a) Orientation, which includes an understanding of Federal regulations and standards and briefings, guides, and/or films designed to acquaint employees with the nature of risks information resources are subject to and the use of security measures to counteract them.

---

[2]Federal Information Processing Standards (FIPS) Publication 31 contains guidance for developing contingency plans.