b) Education, which includes classes and seminars designed to provide managers, owners, users, and custodians of information and information technology resources with a general understanding of how to implement security measures and how to determine if security breaches have occurred.

c) Training, which includes more in-depth and formal classes designed to provide owners and users, especially information technology professionals, with the ability to perform risk analyses, design protection programs, and evaluate the effectiveness of existing security programs.

6) Acquisitions and Procurements. It is essential that appropriate safeguards be determined before procuring information technology resources, not only to ensure the wise expenditure of funds, but also to ensure that resources are protected from the time of installation or implementation. To accomplish this, all contract specifications for the acquisition of hardware, software, software development, equipment maintenance, facility management, and related services shall contain requirements for safeguards that encompass technical, administrative, personnel, and physical security.

7) Other Applicable Regulations. Personnel responsible for information resources security must be knowledgeable of, and all activities must conform with, the DOI Departmental Manual, including the parts listed below.

376 DM, Automated Data Processing
377 DM, Telecommunications
381 DM, Origination of Records and Information
382 DM, Records Operations
383 DM, Policies and Procedures for Implementing the Privacy Act of 1974
384 DM, Records Disposition
385 DM, Office Automation Technology
436 DM, Vital Records
441 DM, Clearances and Suitability Investigation Requirements
442 DM, National Security Information
443 DM, Industrial Security Program
444 DM, Physical Security

8) Security Incidents. Each employee must report to the OSM officials listed below at the time of discovery all suspected, actual, or threatened security incidents involving information resources. The type of incident encountered will determine to whom it should be reported. The responsible OSM official will report the incident promptly to the appropriate management authority and follow up with a written report containing the location, the resources involved, and any corrective actions taken. If warranted, investigative action will be taken by the proper enforcement authority.

a) Incidents involving physical, personnel, and national security complaints and violations shall be reported to the OSM Security Officer. This includes the destruction, physical abuse, or loss of technological resources.

b) Incidents involving records and their unlawful removal, defacing, alteration, or destruction shall be reported to the Records Management Office for subsequent notification of the OSM Director and the National Archives and Records Administration.

c) Incidents involving Privacy Act violations shall be reported to the OSM Privacy Act Officer for coordination of corrective action with the pertinent program/system manager.

d) Incidents involving technology resources resulting in the loss of data, fraud, or compromise or disclosure of sensitive material shall be reported at the time of discovery to the Bureau Information Resources Security Administrator (BIRSA).

c. Responsibilities. All personnel associated with the transmission, handling, and dissemination of information or data share responsibility for its protection.

1) The DOI Office of Information Resources Management is responsible for conducting periodic reviews and evaluations of OSM information resources security programs to ensure compliance with Federal and DOI directives.

2) The Director of the Office of Surface Mining is responsible for promoting an attitude of concern for security among OSM employees. The Director is responsible for establishing and implementing an effective information resources security program that conforms to Federal and DOI regulations.

3) The MIS Division Chief is responsible for:

a) Oversight of OSM's compliance with Federal and DOI policies, guidelines, and regulations pertaining to information resources security.

b) Appointing a BIRSA and alternate to coordinate the management of OSM's information resources security program. Both the BIRSA and alternate must be knowledgeable in information technology and security matters and be department employees unless a waiver is granted by the DOI Information Resources Security Administrator.

4) The Assistant Director for Budget and Administration is responsible for oversight of OSM's compliance with Federal and DOI policies, guidelines, and regulations pertaining to physical, personnel, and information security programs. The OSM Security Officer, Records Management Officer, and Privacy Act Officer have specific responsibilities for performing these functions.

5) All Assistant Directors and Field Office Directors are responsible for appointing an Installation Information Resources Security Officer (IIRSO) and alternate, and for designating resource managers and owners for facilities and systems under their jurisdiction. The IIRSO and alternate must be knowl-

edgeable in information technology and security matters and must be department employees unless a waiver is granted by the DOI Information Resources Security Administrator.

6) The BIRSA is responsible for administration of the information resources security program, coordinating all OSM activities designed to protect information resources, promoting security awareness, and reporting on the effectiveness of these activities to OSM and departmental management. The BIRSA will consult with all OSM officials that have security responsibility (for example, the OSM Security Officer, the Records Management Officer, and system owners) to ensure that information resources are adequately safeguarded throughout OSM. The responsibility assigned to the BIRSA does not supersede or replace security responsibilities previously assigned to any other OSM official.

7) The IIRSO is responsible for coordinating all activities related to the management of an installation's information resources security program and for providing technical assistance to installation management about security requirements.

8) The OSM Security Officer is responsible for implementing departmental policies related to physical, personnel, and information/document security for OSM. This involves conducting periodic reviews of sites to ensure the adequacy of their physical security, safeguarding national security information, investigating security incidents, ensuring appropriate sensitivity classifications for all positions using ADP, and initiating appropriate personnel background investigations. All plans affecting physical security require the approval of the Security Officer. All ADP enforcement issues will be processed through the Security Officer.

9) The Records Management Officer is responsible for ensuring OSM compliance with regulations issued by the National Archives and Records Administration and GSA governing the creation, maintenance, and disposal of records, regardless of their physical form. This responsibility includes automated as well as manual records.

10) The Privacy Act Officer is responsible for developing and implementing programs to manage OSM records covered by the Privacy Act (that is, records that contain information about individuals and which are retrieved by the individual's name or other personal identifier) and for conducting periodic inspections of areas where Privacy Act records are maintained.

11) Supervisors and Managers will ensure that employee performance standards contain appropriate references to their security responsibilities and that employees receive security clearances and ADP access certifications appropriate to respective positions. Supervisors and managers will ensure that

appropriate operational procedures and safeguards are implemented for acquiring, accessing, using, maintaining, or disposing of information and technological resources under their control, and that security policies and procedures are adhered to for those resources they control.

12) System Owners are responsible for implementing safeguards to ensure the protection and proper use of the information resources in their areas. This responsibility includes automated applications, manual applications, and associated hardware and software resources. They are responsible for labeling all information and data with appropriate sensitivity labels, must ensure that adequate security requirements are incorporated into internal or contract specifications before conducting risk analyses, and develop COOPs for systems in their areas.

13) Areas designated as information technology facilities (such as computer centers and word processing centers) require the appointment of a Resource Manager. The Resource Manager is responsible for the overall management of an information technology facility. Responsibilities include ensuring that adequate security exists at the facility in conformance with departmental and system owner requirements. The Resource Manager is responsible for conducting a risk analysis and for developing a COOP for the facility.

14) Each Data Base Administrator is responsible for implementing and controlling access to a data base.

15) Users of information and technological resources are responsible for complying with all security requirements pertaining to the resources they use and are accountable for all activity performed under User IDs and passwords which have been assigned to them for the use of automated systems.

4. Reporting Requirements

a. Each IIRSO will conduct an annual review of the installation's information resources security program to assess its effectiveness and to recertify the adequacy of the installed security safeguards. These reviews may utilize existing reports, such as risk analyses, application system certifications, Privacy Act inspections, records management evaluations, the Departmental Control Evaluation Program, and Inspector General audits. The output of this review should serve as the basis for ensuring the adequacy of the installation's automated information system security.

b. Each IIRSO will prepare an annual installation security report. This report will be incorporated in the BIRSA's annual security plan for transmittal to the DOI Information Resources Security Administrator. The annual reviews described above should serve as the basis for this report.

c. Other requirements as stated herein.

5. References

Department of the Interior Departmental Manual, Part 375 DM 19, IRM Program Management—Information Resources Security Program.

Department of the Interior Departmental Manual, ADP Standards Handbook, Part 306 DM 2).

Office of Management and Budget, Circular No. A-130, Management of Federal Information Resources.

General Services Administration, Federal Information Resources Management Regulations (FIRMR) on security, privacy, ADP management and acquisition, telecommunications management and acquisition, and records management.

National Bureau of Standards Federal Information Processing Standards Publications dealing with security.

Office of Personnel Management, Federal Personnel Manual.

National Archives and Records Administration regulations on records management.

National Security Decision Directive 145.

Department of Treasury Directive 81-80, Electronic Funds and Securities Transfer Policy—Message Authentication.

DOI Information Resources Security Handbook (available from Division of Printing and Publications, Office of Administrative Services, Department of the Interior, Washington, DC 20240).

Computer Security Act of 1987 (Public Law 100-235).

Department of Defense Authorization Act of 1982.

6. Effect on Other Documents

Incorporates ADP-2, Bureau Information Resources Security Program (8 March 1988)

7. Effective Date

Upon issuance

8. Contact

MIS Division Chief or BIRSA

Chapter III

AUTOMATED DATA PROCESSING

AUTOMATED DATA PROCESSING

A. ADP ACQUISITION

1. Purpose

This section contains Office of Surface Mining (OSM) policies and procedures for the acquisition of ADP hardware, software, ADP maintenance services, and ADP support services, including word-processing equipment and electronic mail/message systems.

2. Definitions

a. Terms

Contracting Officer. Individual with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

Contracting Officer's Technical Representative. Individual designated by the Contracting Officer as the representative authorized to perform specific administrative functions with respect to the contract.

Technical Project Officer. Individual assigned technical responsibility from the inception of a requirement through its completion. The same individual may serve as both COTR and TPO.

User. Individual (organization) requesting services through an ADP contract. In some instances, the TPO and/or the COTR is the user for a particular requirement.

b. Abbreviations

A&F	Accounting and Finance Assistant Directorate
ADP	Automated Data Processing
COTR	Contracting Officer's Technical Representative
DOI	Department of the Interior
EFO	Eastern Field Operations Assistant Directorate
FAR	Federal Acquisition Regulations
IRM	Information Resources Management
MIS	Management Information Systems Division
OSM	Office of Surface Mining
TPO	Technical Project Officer
WFO	Western Field Operations Assistant Directorate

3. Policy/Procedures

a. Policy

1) Procurement of ADP Equipment and Services — Authority

a) Assistant Directors are granted the authority to approve requisitions to procure equipment and ADP services as set forth in the OSM Directive OPM-1, Delegation of Authority. At present, Assistant Directors may approve purchases up to $10,000, except that new microcomputer purchases must be approved by the MIS Division Chief (see Figure III-2 on page III-6). Equipment must conform with OSM, DOI, and Federal standards. Any procurement exceeding this threshold must be approved by the MIS Division Chief. Requirements shall not be fragmented into individual procurements in order to circumvent acquisition thresholds. ADP requirements should be planned for and identified in the input to the annual IRM Strategic Plan and ADP and Telecommunications Acquisition Plan. These planned purchases also will be within budgetary requirements. Appropriate documentation that justifies selection and purchase of all ADP resources selected shall be developed and maintained by the originator.

b) Before acquisition, an evaluation of various alternatives for satisfying the need should be conducted. This evaluation should include the option of employing existing information resources which may be available outside of the organization (that is, sharing resources).

c) Services to be provided by contractors, as well as those performed by OSM employees, shall comply with life-cycle development standards (see section III.C, Life-Cycle Management of ADP Information Systems).

d) Maintenance for equipment in Headquarters will be provided by the MIS Division Chief. Otherwise, maintenance is the responsibility of each assistant directorate. Maintenance contracts, when deemed economically justifiable, may be made with local vendors. Consideration should be given to using blanket purchase agreements or other OSM or DOI maintenance agreements, when available.

2) ADP Contract Administration

All procedures and activities in the administration of ADP contracts will be consistent with the applicable contracts, Federal Acquisition Regulations (FAR), DOI Acquisition Regulations (DIAR), and Federal Information Resources Management Regulations (FIRMR). All ADP contracts are limited to ADP support and may not be used for non-ADP activities. The MIS Division Chief is responsible for providing management, policy oversight, and direction for all OSM ADP contracts. The Assistant Directors for EFO, WFO, and A&F are responsible for providing administrative and management oversight for ADP

contracts within their respective assistant directorates, including subordinate offices.

The following policies apply to all OSM ADP contracts:

a) All support requested through a contract will be within the organization and scope of work covered by that contract. Assistant directorate support is restricted to the specific assistant directorate and its subordinate offices. The MIS Division Chief will provide contractor support for Headquarters offices; these contracts may also be used to provide nationwide support.

b) ADP support requirements involving or affecting nationwide OSM programs or functions will be provided by the MIS Division Chief, unless otherwise agreed to by the MIS Division Chief. Support will be implemented in EFO, WFO, and A&F through the local assistant directorate's contractor.

c) All communications between contractors will be coordinated through the respective COTRs. Contractors may not communicate with each other without the coordination of designated OSM staff.

d) Support requirements involving applications developed for a specific assistant directorate may be transported and used within that assistant directorate without MIS coordination. Applications will be provided to offices outside of the assistant directorate only through the MIS Division Chief and through the coordination of the COTRs.

e) Support for the Solicitor's office and other departmental organizations will be provided, where necessary, by the MIS Division Chief. As needed, implementation for field office solicitors may be provided through field operations assistant directorate contractors.

f) Support for State regulatory authority programs with nationwide impact, such as the Technical Information Processing System (TIPS), will be provided through EFO and WFO.

g) ADP contracts will not be used to provide continuing data entry or related clerical support. Data entry is limited to support of specific applications and for a specific period of time.

3) Core Microcomputer Software

To facilitate procurement, training, and interoperability, OSM has identified categories of software for which "core" packages have been selected (see Figure III–1). For the software types included in the figure, only core packages may be purchased. OSM will provide applications assistance, training, and other support to those who use these software packages, which were selected after considering OSM-wide and industry-wide usage and standards.

Figure III-1
OSM CORE SOFTWARE FOR MICROCOMPUTERS AND NETWORKS

Software Type	Core Package	Version
Operating System	PC-DOS	3.3
	MS-DOS	3.3
Word Processing	WordPerfect	5.0
Data Base Management	FoxBase	2.0
	dBase III+	1.1
Electronic Spreadsheet	Lotus 1–2–3	2.01/2.2
Telecommunications	Crosstalk XVI	3.61A
	Novell Netware	2.15

4) ADP Coordination and Review

The MIS Division Chief acts as the OSM IRM Coordinator and as such, is responsible for all OSM IRM and ADP activities.

b. Procedures

1) Procurement of ADP Equipment and Services

a) Within Threshold

Assistant Directors may approve acquisitions of ADP resources without prior written approval from the MIS Division Chief when the costs will not exceed the threshold identified in the policy stated above. Appropriate documentation that justifies selection and purchase of all IRM resources selected shall be developed and maintained and shall be submitted to the MIS Division Chief. All requests for procurement of microcomputers, minicomputers, or mainframe processors must be approved by the MIS Division Chief.

b) In Excess of Threshold

All ADP resource acquisitions expected to exceed the OSM threshold must have written approval from the MIS Division Chief before procurement documents are issued. ADP resource acquisition requests shall:

- Be included in input to the IRM Strategic Plan and ADP and Telecommunications Acquisition Plan. The request shall include the information specified in section II.C, IRM Planning.

- Be approved by the MIS Division Chief.

All ADP resource acquisitions expected to exceed DOI thresholds (see Figure III–2) will be handled in accordance with procedures set forth in the DOI Departmental Manual, Part 376 DM 4. The MIS Division Chief is responsible for obtaining DOI approval.

2) ADP Contract Administration

Assistant Directors may contract for ADP service above the authorized threshold only with the approval of the MIS Division Chief.

All ADP contracts will follow the technical and administrative procedures stated in respective statements of work.

Each ADP contract must include the following contract administration elements. Additional assistant directorate-specific administrative requirements should be included when necessary.

Figure III–2
DOI/OSM ADP ACQUISITION THRESHOLD SUMMARY

<u>OSM AD Threshold</u> $10,000 per total procurement

<u>Departmental Thresholds</u>

    Full and Open Competition

        ADP Hardware — Purchase $1,000,000 total value
        ADP Hardware — Lease $25,000/month
          (including maintenance costs)
        Proprietary Software $300,000 total value
        Maintenance Service $1,000,000/annum
        ADP Contract Service $500,000/annum

    Other Than Full and Open Competition

        ADP Hardware — Purchase $100,000 total value
        ADP Hardware — Lease $3,000/month
          (including maintenance costs)
        Proprietary Software $100,000 total value
        Maintenance Service $100,000/annum
        ADP Contract Service $100,000/annum

    8(a) Firm

        ADP Hardware/Software $100,000/total value
        ADP Contractor Service $500,000/annum

    ADP Software/Contractor Services from
    Other Government Source $500,000/annum

    Hardware Through Reutilization Process

        CPU Cost $50,000 total value
        Lease (including maintenance costs) $3,000/month

a) Monitoring Contract Performance. The contractor's technical performance is monitored through a technical progress or status report submitted at intervals designated by the specific contract. The Contracting Officer, COTR, and TPO (as applicable) review and evaluate contractor progress during a specific period of performance. This may also include briefings or other reporting as included in specific contracts.

b) Inspection and Acceptance. Inspection is the examination and testing of services to determine whether they conform to contract requirements. Acceptance is the action of an authorized representative of OSM by which the Government approves specific deliverables or services rendered as partial or complete performance of the contractor. The COTR and TPO must inspect and then accept or reject all deliverables submitted by contractors.

c) Invoice Review and Approval. The contractor will submit invoices as required by the specific contract. The COTR is responsible for reviewing and coordinating invoice reviews with TPOs (as applicable) to ensure that all costs the Government pays are appropriate, reasonable for the work performed and comply with contract requirements and schedules.

d) Government Property Held by Contractor. If it becomes necessary to provide the contractor with Government property (software, hardware, or other materials), the COTR, in coordination with the Contracting Officer, must ensure that all contractor-held Government property is properly documented and meets all property management requirements. Before providing Government-furnished equipment or property to a contractor, specific FAR clauses must be added to the contract and the contractor has very specific guidelines that he must follow to properly follow to properly maintain and inventory such property.

e) Contractor Purchase. If it is necessary for the contractor to purchase equipment or other goods, the purchased item(s) becomes the property of the Government. The COTR, in coordination with the Contracting Officer, is responsible for ensuring that all contractual requirements are met and followed.

3) Core Software

The following procedures should be followed when purchasing microcomputer or network software.

a) Obtaining a Copy of Core Software

Request a copy of the software from the MIS Software Inventory Coordinator. If the software is not available from inventory or other OSM or DOI sources, the MIS Software Inventory Coordinator will recommend the most effective and efficient way to satisfy the requestor's requirements.

Activities may *not* use other software as a substitute for core software.

b) Obtaining a Copy of Other Software

Software for which no core software is designated should be purchased through the requesting office's Procurement Agent or Contracting Officer. The requestor will prepare a requisition in accordance with established OSM procurement procedures and authorities. In addition, if the non-core software has a purchase price of $250 or greater, approval of the MIS Division Chief must be obtained prior to purchase.

c) Obtaining an Update to Core Software

Newly released versions of core software must not be purchased for routine use until the MIS Division Chief has approved an OSM-wide upgrade. However, such packages may be purchased for special projects or analysis upon approval of the MIS Division Chief.

d) Requesting Changes to the OSM Core Software

Requests for changes to, additions to, or deletions from the OSM core software list should be sent to the MIS Division Chief. The requesting letter should include an explanation of the requested change and the reasons a change/addition is needed.

c. Responsibilities

1) The MIS Division Chief is responsible for:

a) Ensuring that major systems comply with life-cycle development standards and economic analysis standards.

b) Developing a Five-Year ADP and Telecommunications Acquisition Plan and ensuring that acquisition requests conform with the plan.

c) Ensuring that OSM systems are managed in accordance with the authorities cited in the references listed below.

d) Conducting periodic reviews to ensure the efficiency, effectiveness, and proper implementation of contract management controls.

e) Coordinating OSM ADP contracting policy and procedures with the Branch of Contracting.

f) Administering and overseeing all ADP delegations of authority from DOI to OSM.

g) Providing liaison with and accountability to the DOI Office of Information Resources Management for ADP procurement activities.

h) Oversight of all ADP contracts supporting information resources.

i) Delegating administrative authority to Assistant Directors for ADP contracts supporting the information resources of the particular assistant directorate.

j) Conducting reviews of assistant directorate ADP contractor efforts to evaluate compliance with DOI and OSM ADP policies and procedures.

k) Approving all requests for contractor support.

l) Providing ADP contractor support for the Office of the Solicitor and other departmental organizations.

m) Providing ADP contractor support to OSM field offices and State regulatory authority programs where there is nationwide impact.

n) Providing lead coordination for efforts requiring MIS and/or assistant directorate contractors to work with each other.

2) For the ADP contracts for which they are accountable, Assistant Directors are responsible for:

a) Ensuring that any system development project is approved by the MIS Division Chief.

b) Ensuring that projects conform to OSM standards and follow the OSM and DOI life-cycle development requirements, and maintaining and forwarding to the MIS Division Chief for review and approval all required life-cycle documentation, especially documentation relating to ADP acquisition and project approval decisions.

c) Conducting site/security readiness reviews before system installation.

d) Administering ADP delegations of authority from the MIS Division Chief.

e) Ensuring compliance with all OSM, DOI, and Federal policies and procedures, including ensuring that the systems are managed in compliance with authorities listed in the references below.

f) Establishing and administering supplemental assistant directorate contracting policy and procedures.

g) Administering and overseeing approved assistant directorate contracts supporting information resources.

h) Ensuring that all ADP contract support represents the best interests of the Government.

i) Approving all requests for contractor support within the respective assistant directorate.

j) Implementing support of nationwide efforts through assistant directorate contracts as requested by the MIS Division Chief.

k) Ensuring that assistant directorate coordination is provided for efforts involving contractors in other assistant directorates.

l) Approving all requests for the expenditure of assistant directorate ADP contract funds.

3) The Contracting Officer, and only the Contracting Officer, is authorized to:

a) Award, agree to, or execute any contract, contract modification, or notice of intent.

b) Execute or agree to any changes in the specifications, delivery schedule, or other terms and conditions of the contract.

c) Order work inside or outside the scope of the contract.

4) The COTR is responsible for:

a) Ensuring that all users and TPOs adhere to the contractual requirements for requesting support from the contractor.

b) Assisting the contractor in interpreting technical requirements of the contract's scope of work.

c) Coordinating written technical directions, specifications, and procedures relating to contractual work requirements with the contractor.

d) Issuing technical direction in accordance with the contract's technical direction contract clause.

e) Coordinating with the MIS COTR and other assistant directorate COTRs, as needed.

f) Reviewing and commenting on the contractor's request for Government-furnished facilities, supplies, materials, and equipment and forwarding the request to the Contracting Officer for disposition.

g) Reviewing and commenting on the contractor's request for consent to purchase supplies, materials, and equipment and forwarding the request to the Contracting Officer for disposition.

h) Maintaining a complete and open line of communication with the Contracting Officer regarding the contractor's technical performance and progress and, when requested, providing written assessment of the contractor's performance for inclusion in the contractor performance file.

i) Ensuring that Government inspection and acceptance for all deliverable items under the contract is accomplished.

j) Reviewing payment vouchers and concurring with respect to the percent of technical completion for items or services delivered and accepted under the contract.

k) Upon expiration of the contract, providing a written statement attesting to the contractor's completion of technical performance under the contract and of the delivery and acceptance of all goods and services for which inspection and acceptance are designated.

5) The TPO is responsible for:

a) Providing the contractor with written technical requirements in coordination with the contracting officer and user.

b) Ensuring that written requirements are submitted to the COTR (where applicable) for issuance to the contractor.

c) Scheduling and organizing meetings with the user and contractor to initiate work.

d) Ensuring that copies of written requests are submitted to the COTR (as applicable) and included in COTR files.

e) Reviewing and recommending COTR approval/disapproval (as applicable) of contractor proposals, management plans, and resumes.

f) Identifying and resolving all technical discrepancies and issues.

g) Ensuring that all dates and deadlines are monitored effectively.

h) Communicating effectively with the user and the contractor.

i) Anticipating and resolving problems as expeditiously as possible.

j) Reviewing, evaluating, and recommending acceptance of deliverables.

k) Ensuring that all documents requiring the user's review and signature are forwarded to the user.

l) Documenting all user and technical comments on contractor performance, deliverables, and the status of work.

m) Communicating with and keeping the COTR informed (as applicable) of contractor performance, the status of deliverables, and other matters involving the terms and conditions of respective contracts.

6) The user is responsible for:

a) Identifying and submitting needs and requirements to the TPO or COTR.

b) Working with the TPO or COTR to develop written requirements.

c) Reviewing and evaluating deliverables and providing comments to the TPO or COTR and recommending acceptance or nonacceptance of deliverables.

d) Monitoring management plan dates and deadlines with the TPO or COTR.

e) Communicating with the TPO or COTR on contractor performance.

f) Ensuring that documents requiring the user's signature are signed promptly and forwarded to the TPO or COTR.

7) The MIS Software Inventory Coordinator is responsible for:

a) Maintaining the OSM core software list.

b) Coordinating acquisition of core software throughout OSM.

c) Keeping abreast of high-level OSM requirements and technological changes to ensure that the core software continues to support OSM needs.

4. Reporting Requirements

As required by the references below and other chapters of this OSM IRM Policy and Procedures Manual.

5. References

OSM Directive OPM–1, Delegations of Authority

Department of the Interior Departmental Manual, Part 376 DM 4, Information Resources Management—ADP Acquisition.

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)).

Federal Information Resources Management Regulations (FIRMR), including:
FIRMR 201-33.003 (Reuse of ADPE)
FIRMR 201-31 (Sharing ADP resources)
FIRMR 201-32.104 (Computer security)
FIRMR 201-23.103 (Thresholds)
FIRMR 201-6 (Required contractual clauses for contracted operations)
FIRMR 201-30.007 (Requirements analysis)
FIRMR 201-30.009 (Analysis of alternatives)
FIRMR 201-30.007(d)(9) and 201-34.002
    (Performance evaluation for current ADP system)
FIRMR 201-30.009-3
    (Findings to support the use of compatibility-limited requirements)
FIRMR 201-30.012-1 (Software conversion study)
FIRMR 201-11.002(b) (Certified data to support sole source)
FIRMR 201-11.002-1 (Certified data to support sole make/model)
FIRMR 201-30.012 (Planned actions to foster competition)

Federal Acquisition Regulations (FAR), including:
FAR 2.1
FAR 24.104 (Required contractual clauses for contracted operations)

Federal Information Processing Standards (FIPS).

Interior Property Management Regulations (IPMR).

Department of the Interior Acquisition Regulations (DIAR), including:
DIAR 1424.104 (Required contractual clauses for contracted operations).

Privacy Act of 1974, as amended (5 USC 522a).

6. Effect on Other Documents

Supersedes OSM Directive ADP-4

7. Effective Date

Upon issuance

8. Contact

MIS Division Chief

B. ADP COST ACCOUNTING, COST RECOVERY, AND SHARING

1. Purpose

This section establishes Office of Surface Mining (OSM) policies and procedures for sharing ADP equipment. As OSM does not provide reimbursable ADP services to external organizations, no policies have been established for the cost accounting and cost recovery required when dealing with chargeback systems.

2. Definitions

a. Terms

None

b. Abbreviations

ADP	Automated Data Processing
MIS	Management Information Systems Division
OSM	Office of Surface Mining

3. Policy/Procedures

a. Policy

OSM will share information technology facilities with users from other agencies to the maximum extent feasible.

In selecting information technology facilities to support new applications, OSM will ensure that:

- In the interest of efficiency and economy, alternative facilities are considered, including other Federal agencies and non-Federal facilities and services.

- Policy does not require that priority be given to the use of in-house facilities.

- Selection decisions are documented in official records.

b. Procedures

When evaluating information resource requirements for new applications (or modifications to existing systems), consider the cost and availability of facilities and services of other Federal agencies and non-Federal organizations.

c. Responsibilities

    1) The MIS Division Chief is responsible for promoting OSM-wide ADP resource sharing and for ensuring that alternative sharing of ADP resources is evaluated before new procurements are made.

    2) Assistant Directors are responsible for promoting ADP resource sharing within the assistant directorate and for ensuring that alternative sharing of ADP resources is evaluated before new procurements are made.

4. Reporting Requirements

None

5. References

Department of the Interior Departmental Manual, Part 376 DM 6, ADP—ADP Cost Accounting, Cost Recovery, and Sharing.

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

6. Effect on Other Documents

None

7. Effective Date

Upon issuance

8. Contact

MIS Division Chief

C. LIFE-CYCLE MANAGEMENT OF ADP INFORMATION SYSTEMS

1. Purpose

This section provides Office of Surface Mining (OSM) policy and procedural guidance to ensure that system development and implementation is efficient and effective. It does not dictate a specific development methodology to be used. Instead, it concentrates on documentation requirements over the life cycle to:

- Ensure that all OSM ADP systems and applications are consistently documented in clear, high-quality documents throughout their life cycles.

- Ensure that the proper level of documentation is developed for a proposed ADP system or application.

Appendix A clearly states format and content for the most common documents required during the life cycle of a proposed or operating ADP system or application used or planned for use within OSM.

2. Definitions

a. Terms

Life-Cycle Management (LCM). A management approach that provides a structured process for planning and controlling an information resource from inception to replacement or termination. LCM provides a common framework that facilitates control of the process, specifies the contents of deliverables, improves communications among diverse interest groups, and manages the development and acquisition of information resources. The effort and level of detail of the activities conducted by using the LCM management approach are to be commensurate with the size, complexity, and importance of the resource.

Documentation.[1] All information that describes the development, operation, use, and maintenance of computer software. This information is in a form that can be reproduced, distributed, updated, and referred to when it is needed.

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
TPO	Technical Project Officer

---

[1] Source: Federal Information Processing Standards, Publication 105, 6 June 1984.

3. Policy/Procedure

a. Policy

In general, software documentation fulfills the following important functions throughout the life cycle of a system or application:

- Assistance in defining mission needs and requirements.

- Communication to keep management apprised of requirements, progress, problems, and expectations while the system or application is under development.

- Communication to keep those who are performing various development, operation, and maintenance tasks aware of what other groups are doing or have done while the system or application is under development.

- Instruction and reference for those using the system or application.

- Information for maintenance, quality assurance, and auditing personnel.

- Historical reference for future development efforts and to assist in transferring the system or application to new environments.

A system's life cycle consists of well-defined activities that begin when a need is identified and continue until the resulting system or application is no longer of use. Figure III-3 shows the three phases and nine stages of this life cycle as defined by DOI. The three phases of the application system life cycle are initiation, development, and operation and maintenance. These phases are divided into eight stages, and the documentation required over the life cycle falls into those stages.

Initiation Phase. The documentation prepared during the initiation phase organizes and justifies the subsequent development effort. Mission analysis stage documentation concentrates on the general need for a system and preliminary organizational activities. Concept development stage documentation:

- Identifies alternatives and the costs and benefits of those alternatives.

- Delineates responsibilities for the production team.

- Defines schedules and milestones for the development project.

- Records the history of the development effort so that the rationale for the system's structure is available for later use.

Development Phase. Documentation prepared during the system analysis and system design stages of the development phase records details of discussions about system requirements.

Figure III-3
DEPATMENT OF THE INTERIOR SYSTEM LIFE CYCLE
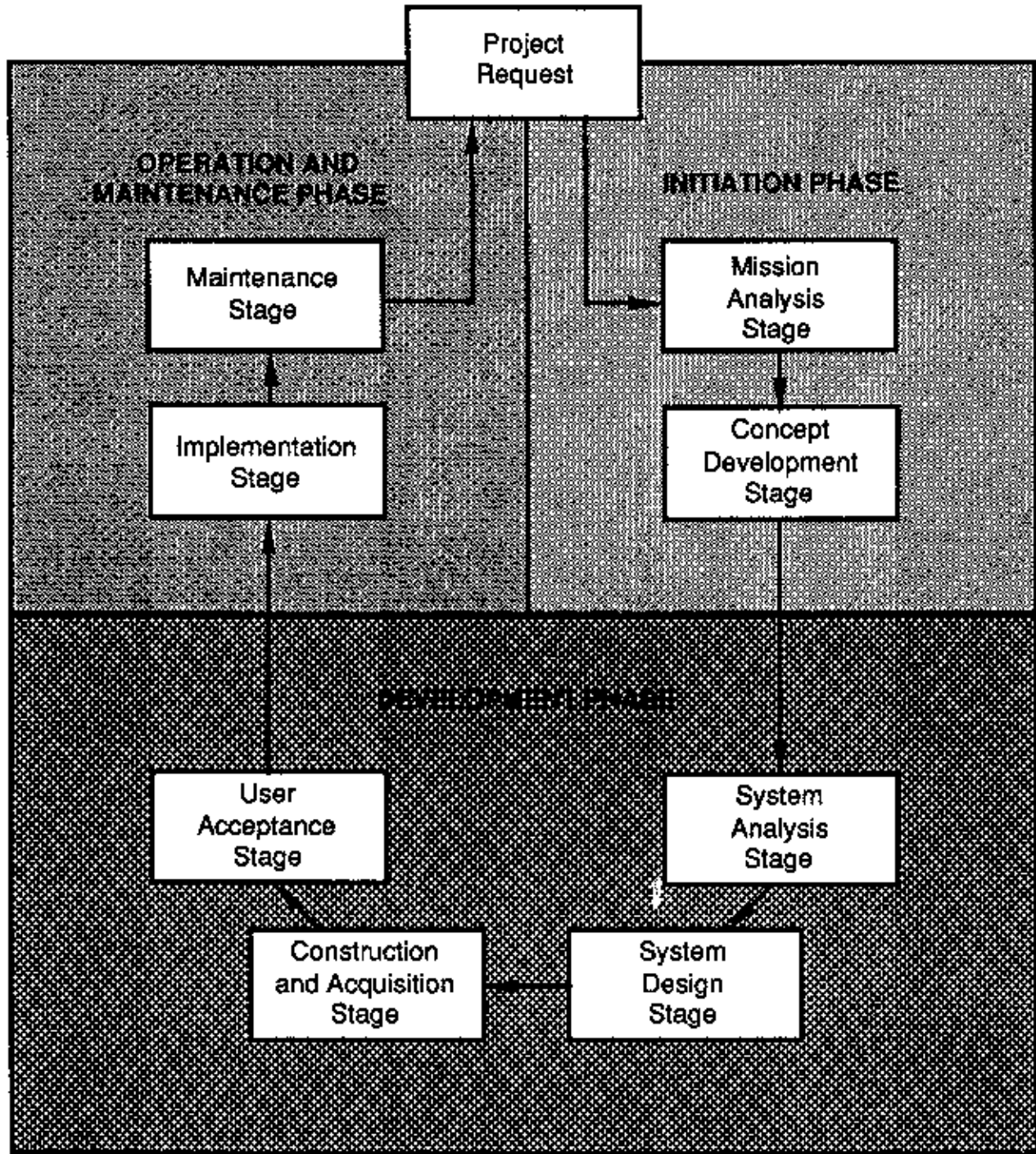
Documentation prepared during the system construction and acquisition and user acceptance stages of the development phase describes the results of the analysis and design effort. It provides the information needed for effective system design and testing as well as the use, operation, maintenance, and conversion and/or transfer of the resulting system or application. If the product is to be used by people other than the developers, this documentation will prevent any number of problems that may cause the product to fail. For example:

- System developers and programmers use information that describes what a system or application is supposed to do, when it should do it, and how it should be tested.

- System administrators, operators, and maintenance programmers use information that tells how to operate, support, and maintain the system or application.

- Users employ training and reference materials that enable them to quickly learn how to use the system or application and find answers to specific questions.

- Management uses information in the documentation to inform other managers and potential system users about the system's existence and capabilities.

All ADP development projects, whether the development of a new system or the modernization or modification of an existing system, involve all phases of the life cycle: initiation, development, and operation and maintenance. The development or enhancement process will follow a systematic, structured approach that will be documented as set forth herein. The specific development methodology used may vary from project to project. When cost effective, state-of-the-art development approaches such as prototyping, computer-assisted software engineering (CASE), and reverse engineering (prototyped systems) for mandatory documentation should be used; however, the fundamental considerations will not change. These considerations are established in the procedures described below.

The degree of documentation required is determined by comparing the scope of the ADP development project to the five levels of documentation as described in the procedures below. This decision should be made in the early planning stages and should be reported in field office and assistant directorate input to the IRM Strategic Plan.

To reiterate, all ADP development efforts involve all stages of the system life cycle, even if formal documentation is not required. For example, even a system developed by one individual for his or her own use will involve the following system life-cycle activities:

- Determining a need, conceptualizing the system, and determining if benefits outweigh the costs of development (project initiation).

- Analyzing specific functional and data requirements (system analysis).

- Designing the software and data base (system design).

- Coding the programs, establishing the data base structure, converting or keying the data, testing the system, and determining acceptance (system construction and acquisition, user acceptance).

- Using and maintaining the system (operation and maintenance).

Adhering to a structured approach of development and maintenance reduces the potential for overlooked requirements and inefficient or ineffective designs. The larger and more complex the system, the more expensive changes become in the later stages of the life cycle. For this reason, more stringent documentation requirements are established and must be followed for these systems.

b. Procedure

As the scope of projects varies, so do the requirements for documentation. The following paragraphs define five levels of documentation and provide guidance on how to choose the appropriate level for an ADP development effort.

Level 0   No documentation is required for microcomputer programs developed by an OSM staff member for individual use. However, if the programs are found to be useful to other individuals within the office—or would be used by a successor in the position—Level 1 documentation is required at a minimum.

Level 1   Required for systems used within a single office (that is, one Headquarters division or one field office division).

Level 2   Required for systems used throughout one OSM location (that is, in all Headquarters divisions or in all divisions of a field office).

Level 3   Required for systems used by more than one OSM organizational level or more than one field office (for example, systems that communicate information from a field office to a Headquarters office or among field offices).

Level 4   The maximum level of documentation will be prepared for major, service-wide systems that require oversight by the DOI Office of Information Resources Management.

c. Responsibilities

1) The MIS Division Chief is responsible for:

a) Maintaining up-to-date documentation standards and policies and communicating those standards and policies to the responsible organizational units.

b) Ensuring that MIS TPOs follow the appropriate policy and procedures in developing plans for application life-cycle documentation requirements.

2) Assistant Directors are responsible for:

a) Maintaining up-to-date documentation standards in their files.

b) Ensuring that TPOs on their staffs follow the policies and procedures with regard to preparing documentation plans for application systems developed by their offices.

3) TPOs are responsible for:

a) Managing projects in accordance with DOI and OSM guidance to ensure efficient development and implementation of an effective system.

b) Preparing project management plans for ADP development and maintenance projects. Documentation plans, which will indicate the level of and schedule for planned documentation, will be included therein. These plans will be included in each system proposal.

4) Documentation Specialists (contractors and OSM) are responsible for following the detailed requirements for content and format found either in Appendix A to this directive or in the DOI Project Manager's Guide to Application Systems Life-Cycle Management (see references), as determined by the level of documentation required.

4. Reporting Requirements

At the onset of any ADP development effort, OSM project officers are responsible for using this guide to prepare a list of required documentation. All phases of the system life cycle (initiation, development, and operation and maintenance) should be considered when preparing this list. The decision as to the documentation required should be made early in system planning efforts and should be reported in field office and assistant directorate input to the IRM Strategic Plan.

Figure III–4 is a matrix that shows documentation requirements for all phases and stages of the four levels of required documentation as defined in the policy above. Figures III–5 through III–8 provide detailed listings for each documentation level and each life-cycle phase and stage. Content summaries and annotated outlines for documentation required in phases 1 through 3 can be found in Appendix A to this directive. Details on phase 4 documentation can be found in the DOI Project Manager's Guide to Application Systems Life-Cycle Management (see references).

The requirements discussed in this section should serve as a general guide to determining the extent of documentation required, and they are intended to be flexible. Developers may feel that more documentation is required, less documentation is

required, or that some documents can be combined. Factors such as the size of the application system, the development methodology used, the projected number of users, and the size of the development team will influence the documentation desired. For example, while all systems require analysis and design before they are implemented, the level of detail and formality of development documentation will vary according to factors such as those listed above.

While the policy for documentation to be prepared is flexible, the detailed requirements for content and format found in Appendix A and in the DOI Project Manager's Guide to Life-Cycle Management must be followed where they apply.

Copies of documentation for systems which may have applicability throughout OSM should be forwarded to the MIS Division Chief for review and consideration for further promulgation. Requirements and final products should also be discussed at the semi-annual IRM Coordinator meetings.

Figure III–4
COMPARISON OF MINIMUM DOCUMENTATION REQUIREMENTS

Life-Cycle Phase/Stage/Document		Level 4	Level 3	Level 2	Level 1
1	**INITIATION PHASE**				
1.1	**Mission Analysis Stage**				
1.1.1	Project Request	Required			
1.1.2	Mission Analysis Methodology	Required			
1.1.3	Cost/Benefit Analysis	Required			
1.1.4	Project Charter	Required			
1.1.5	Organizational Model	Required			
1.1.6	Mission Processes Model	Required			
1.1.7	Information Model	Required			
1.1.8	Mission Need Statement	Required			
1.2	**Concept Development Stage**				
1.2.1	System Objectives	Optional			
1.2.2	Application System Architecture	Optional			
1.2.3	Data Architecture	Optional			
1.2.4	Data Communications Architecture	Optional			
1.2.5	Feasibility Study		Required	Required	
1.2.6	System Life-Cycle Strategy	Required			
1.2.7	System Life-Cycle Dates	Required			
1.2.8	System Life-Cycle Resources Estimate	Required			
1.2.9	Project Management Plan		Required	Required	
1.2.10	Quality Assurance Plan		Required	Required[1]	
1.2.11	Cost/Benefit Analysis	Required	Required	Required	
1.2.12	Revised Mission Need Statement	Required			
1.2.13	System Decision Paper 1	Required			

[1]Incorporated in Project Management Plan.

Figure III–4 (Continued)
COMPARISON OF MINIMUM DOCUMENTATION REQUIREMENTS

	Life-Cycle Phase/Stage/Document	Level 4	Level 3	Level 2	Level 1
2	**DEVELOPMENT PHASE**				
2.1	**System Analysis Stage**				
2.1.1	Current System Description	Optional	Required[2]	Required[2]	Optional[2]
2.1.2	Detailed Functional Requirements	Optional	Required	Required	Optional
2.1.3	Data Requirements	Required	Required	Required	Optional
2.2	**System Design Stage**				
2.2.1	Design Proposal	Required			
2.2.2	Detailed Cost/Benefit Analysis	Required			
2.2.3	Revised Life-Cycle Strategy	Required			
2.2.4	System Decision Paper 2	Required			
2.3	**System Construction and Acquisition Stage**				
2.3.1	Test Plans:				
2.3.1.1	Unit Test Plan		Required		
2.3.1.2	Integration Test Plan		Required		
2.3.1.3	System Test Plan	Required	Required		
2.3.1.4	Acceptance Test Plan		Required		
2.3.2	ADPE Specifications	Optional	Required[3]		
2.3.3	Application Software Documentation:				
2.3.3.1	System/Subsystem Specification	Optional	Required		
2.3.3.2	Data Base Specification	Optional	Required	Required	Optional
2.3.3.3	Detailed Process Design	Optional			
2.3.3.4	Program Specification	Optional	Required		
2.3.3.5	Test Data Design	Optional			
2.3.3.6	Data Dictionary	Optional	Required	Required	Optional
2.3.4	Control, Backup, and Security Study	Required	Required[4]	Required[4]	Required[4]
2.3.5	Contingency Plan		Required	Required	

[2]Incorporated in Detailed Functional Requirements.
[3]Incorporated in System/Subsystem Specification.
[4]Incorporated in User's Manual, Operations Manual, and Data Base Administration Procedures Manual.

Figure III–4 (Continued)
COMPARISON OF MINIMUM DOCUMENTATION REQUIREMENTS

Life-Cycle Phase/Stage/Document		Level 4	Level 3	Level 2	Level 1
2.4	**User Acceptance Stage**				
2.4.1	Current System Description	Required			
2.4.2	Mission Analysis Methodology	Required	Required[5]		
2.4.3	Cost/Benefit Analysis	Optional	Required		
2.4.4	User Training Plan	Optional	Required	Required	
2.4.5	Post-Implementation Review Plan	Required			
2.4.6	Program Maintenance Manual	Required	Required	Required	Optional
2.4.7	Data Processing Manual	Optional			
2.4.8	User's Manual	Optional	Required	Required	Required
2.4.9	Operations Manual	Optional	Required	Required	Required
2.4.10	Data Base Administration Procedures Manual		Required	Required	Required
2.4.11	System Decision Paper 3	Required			
3	**OPERATION AND MAINTENANCE PHASE**				
3.1	**Implementation Stage**				
3.1.1	Application Stewardship Document	Required			
3.2	**Maintenance Stage**				
3.2.1	Post-Implementation Review Report	Required			
3.2.2	System Decision Paper 4	Required			

[5]Incorporated in Conversion Plan.

Figure III-5
SUMMARY OF MINIMUM DOCUMENTATION REQUIREMENTS
AND REFERENCE NUMBERS FOR OSM LEVEL 1

INITIATION PHASE

Mission Analysis Stage   None Required

Concept Development Stage   None Required

DEVELOPMENT PHASE

System Analysis Stage
Current System Description[1] 2.1.1
Detailed Functional Requirements* 2.1.2
Data Requirements* 2.1.3

System Design Stage   None Required

System Construction and
Data Base Specification* 2.3.3.2
Data Dictionary* 2.3.3.6
Control, Backup, and Security Plan[2] 2.3.4

User Acceptance Stage
Program Maintenance Manual* 2.4.6
User's Manual 2.4.8
Operations Manual 2.4.9
Data Base Administration Procedures Manual 2.4.10

OPERATION AND MAINTENANCE PHASE

Implementation Stage   None Required

Maintenance Stage   None Required

*Optional

---

[1]Incorporated in Detailed Functional Requirements.

[2]Incorporated in User's Manual, Operations Manual, and Data Base Administration Procedures Manual.

Figure III-6
SUMMARY OF MINIMUM DOCUMENTATION REQUIREMENTS
AND REFERENCE NUMBERS FOR OSM LEVEL 2

INITIATION PHASE

Mission Analysis Stage

None Required

Concept Development Stage

Feasibility Study 1.2.5
Project Management Plan 1.2.9
Quality Assurance Plan[1] 1.2.10
Cost/Benefit Analysis 1.2.11

DEVELOPMENT PHASE

System Analysis Stage

Current System Description[2] 2.1.1
Detailed Functional Requirements 2.1.2
Data Requirements 2.1.3

System Design Stage

None Required

System Construction and

Data Base Specification 2.3.3.2
Data Dictionary 2.3.3.6
Control, Backup, and Security Plan[3] 2.3.4
Contingency Plan 2.3.5

User Acceptance Stage

User Training Plan 2.4.4
Program Maintenance Manual 2.4.6
User's Manual 2.4.8
Operations Manual 2.4.9
Data Base Administration Procedures Manual 2.4.10

OPERATION AND MAINTENANCE PHASE

Implementation Stage

None Required

Maintenance Stage

None Required

---

[1]Incorporated in Project Management Plan.

[2]Incorporated in Detailed Functional Requirements.

[3]Incorporated in User's Manual, Operations Manual, and Data Base Administration Procedures Manual.

Figure III-7
SUMMARY OF MINIMUM DOCUMENTATION REQUIREMENTS
AND REFERENCE NUMBERS FOR OSM LEVEL 3

INITIATION PHASE

Mission Analysis Stage	None Required	
Concept Development Stage	Feasibility Study	1.2.5
	Project Management Plan	1.2.9
	Quality Assurance Plan	1.2.10
	Cost/Benefit Analysis	1.2.11

DEVELOPMENT PHASE

System Analysis Stage	Current System Description[1]	2.1.1
	Detailed Functional Requirements	2.1.2
	Data Requirements	2.1.3
System Design Stage	None Required	
System Construction and Acquisition Stage	Unit Test Plan	2.3.1.1
	Integration Test Plan	2.3.1.2
	System Test Plan	2.3.1.3
	Acceptance Test Plan	2.3.1.4
	ADPE Specification[2]	2.3.2
	System/Subsystem Specification*	2.3.3.1
	Data Base Specification	2.3.3.2
	Program Specification	2.3.3.4
	Data Dictionary	2.3.3.6
	Control, Backup, and Security Plan[3]	2.3.4
	Contingency Plan	2.3.5
User Acceptance Stage	Implementation Plan[4]	2.4.2
	Conversion Plan	2.4.3
	User Training Plan	2.4.4
	Program Maintenance Manual	2.4.6
	User's Manual	2.4.8
	Operations Manual	2.4.9
	Data Base Administration Procedures Manual	2.4.10

[1]Incorporated in Detailed Functional Requirements.

[2]Incorporated in System/Subsystem Specification.

[3]Incorporated in User's Manual, Operations Manual, and Data Base Administration Procedures Manual.

[4]Incorporated in Conversion Plan.

OPERATION AND MAINTENANCE PHASE

Implementation Stage   None Required

Maintenance Stage   None Required

Figure III–8
SUMMARY OF MINIMUM DOCUMENTATION REQUIREMENTS
AND REFERENCE NUMBERS FOR OSM LEVEL 4

INITIATION PHASE

Mission Analysis Stage

Project Request 1.1.1
Mission Analysis Methodology 1.1.2
Cost/Benefit Analysis 1.1.3
Project Charter 1.1.4
Organizational Model 1.1.5
Mission Process Model 1.1.6
Information Model 1.1.7
Mission Need Statement 1.1.8

Concept Development Stage

System Objectives* 1.2.1
Application System Architecture* 1.2.2
Data Architecture* 1.2.3
Data Communications Architecture* 1.2.4
System Life-Cycle Strategy 1.2.6
System Life-Cycle Dates 1.2.7
System Life-Cycle Resources Estimate 1.2.8
Cost/Benefit Analysis 1.2.11
Revised Mission Need Statement 1.2.12
System Decision Paper 1 .... 1.2.13

DEVELOPMENT PHASE

System Analysis Stage

Current System Description* 2.1.1
Detailed Functional Requirements* 2.1.2
Data Requirements 2.1.3

System Design Stage

Design Proposal 2.2.1
Detailed Cost/Benefit Analysis 2.2.2
Revised Life-Cycle Strategy 2.2.3
System Decision Paper 2 .... 2.2.4

System Construction and
Acquisition Stage

System Test Plan 2.3.1.3
ADPE Specifications* 2.3.2
System/Subsystem Specification* 2.3.3.1
Data Base Specification* 2.3.3.2
Detailed Process Design* 2.3.3.3
Program Specification* 2.3.3.4
Test Data Design* 2.3.3.5
Data Dictionary* 2.3.3.6
Control, Backup, and Security Plan 2.3.4

*Optional

User Acceptance Stage	System Acceptance Report	2.4.1
	Implementation Plan	2.4.2
	Conversion Plan*	2.4.3
	User Training Plan*	2.4.4
	Post-Implementation Review Plan	2.4.5
	Program Maintenance Manual	2.4.6
	Data Processing Manual*	2.4.7
	User's Manual*	2.4.8
	Operations Manual*	2.4.9
	System Decision Paper 3	2.4.11

OPERATION AND MAINTENANCE PHASE

Implementation Stage	Application Stewardship Document	3.1.1
Maintenance Stage	Post-Implementation Review Report	3.2.1
	System Decision Paper 4	3.2.2

5. References

U.S. Department of the Interior, A Project Manager's Guide to Application Systems Life-Cycle Management (376 DM 10), August 1985.

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

Guidelines for Software Documentation Management, 6 June 1984, Federal Information Processing Standards Publication 105, National Bureau of Standards.

Guidelines for Documentation of Computer Programs and Automated Data Systems, 30 June 1974, Federal Information Processing Standard Publication 38, National Bureau of Standards.

Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase, 1 August 1979, Federal Information Processing Standard Publication 64, National Bureau of Standards.

6. Effect on Other Documents

This documentation standard supersedes OSM Directive ADP-3, Systems Implementation Standards.

7. Effective Date

Upon issuance

8. Contact

MIS Division Chief

This page intentionally blank

b. Procedures

1) When commercial ADP equipment or software is purchased, the hardware/
    software package inventory will be updated. The inventory will be maintained
    by each field office and assistant directorate and will include, at a minimum:

    Item Purchased (including Version or Release Number)
    Description of Item Purchased
    Type of Purchase (indicate one of the following: Computer, Add-in Board,
        Peripheral, Software, Accessory, Other)
    Manufacturer
    Vendor
    Serial Number
    Purchase Order Number
    Purchase Date
    Receipt Date
    Quantity
    Price
    Person(s) who approved purchase
    Distribution Information:
        To whom equipment/software is assigned
            (including Name, Title, Telephone Number)
        Location of equipment/software

    The hardware and software inventory will be supplied to the MIS Division
    Chief.

2) Each organization will maintain an inventory of custom-developed software
    applications. When a software development effort is approved, completed, or
    terminated, the application inventory will be updated. This inventory will
    include:

    Application Name
    Functional Description
    Software Environment
        (for example, operating system required, programming language)
    Hardware Requirements
        (for example, CPU required, memory requirements, storage requirements)
    Development Start Date
    Installation Date
    Installation Date Projected/Actual Indicator
    Use Termination Date
    System Developer(s)
    System Owner(s) (Name, Position, Telephone Number)
    System Manager(s) (Name, Position, Telephone Number)

c. Responsibilities

    1) The MIS Division Chief is responsible for compiling and maintaining an ADP resource inventory and providing necessary inventory data to the DOI Office of Information Resources Management. The necessary data will be accurate and provided on a timely basis.

    2) Assistant Directors and Field Office Directors are responsible for ensuring that ADP resource inventories are maintained.

4. Reporting Requirements

Updates to the hardware, software, and application inventories will be provided to the MIS Division Chief semiannually (at the end of the second and fourth quarters) in the electronic format specified by the MIS Division Chief.

5. References

Department of the Interior Departmental Manual, Part 376 DM 11, Information Resources Management—ADP Resource Inventories.

Paperwork Reduction Act of 1980 (44 USC 3501).

General Services Administration, Federal Information Resources Management Regulations (FIRMR).

6. Effect on Other Documents

None

7. Effective Date

Upon issuance

8. Contact

MIS Division Chief

This page intentionally blank

E. AUTOMATED INFORMATION SYSTEMS MANAGEMENT ACCOUNTABILITY

1. Purpose

This section provides Office of Surface Mining (OSM) policies and responsibilities concerning management accountability for automated information systems.

2. Definitions

a. Terms

Automated Information System (AIS). An organized combination of human resources, ADP equipment, software, and established methods and procedures designed to collect, process, and/or communicate data or information for the purposes of supporting specific administrative, mission, or program requirements.

Major AIS. An AIS that requires special, continuing management attention because of its importance to the support of a mission; its high development, operation, or maintenance costs; or its significant impact on the administration of programs, finances, property, or other resources. An AIS is determined to be major when it meets any one of the following criteria:

- The system directly affects the ability of DOI or OSM to perform a mission designated by the President, the Congress, the Office of Management and Budget, or the Secretary as being of importance.

- The system involves a significant investment, including personnel costs, relating to development, operation, and/or maintenance. In this context, significant investment has occurred if (a) the cost of initial development from conception to implementation exceeds $1 million, (b) the cost of operating and maintaining the system in any one year exceeds $0.5 million, or (c) the total life-cycle cost exceeds $5 million.

- The system affects national security or the security and safety of people, substantial financial resources, or other valuable assets.

- The system is used throughout DOI.

- The system supports a function that is multi-bureau in scope.

- The system directly affects DOI's ability to meet a critical departmental, national, or international mission.

System Owner/Steward. The program official whose program is supported by the AIS and is the primary user of the AIS, who initiated development of the AIS, or who exercises functional oversight of the AIS. The system owner is responsible and accountable for the products of the system. In some cases, system ownership may be shared.