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

DIRECTIVES SYSTEM

Subject Number: AOP-2

Transmittal Number:

Date:

Subject: Bureau Information Resources Security Program

Approval:

Title:

1. Purpose.

This directive defines policies, assigns responsibilities, and prescribes procedures for the management of the Office of Surface Mining Reclamation and Enforcement (OSMRE) Information Resources Security Program. The purpose of the program is to protect the Bureau'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. The program assures that adequate measures are established to ensure an appropriate level of protection for the information resources under OSMRE's authority. The program complies with all Federal policies, procedures, and standards governing information resources security. The provisions of this directive:

a. Combine all the requirements and responsibilities for manual and automated information resources security into one directive; and establish responsibilities and procedures for the development, administration and maintenance of an information resources security program for OSMRE.

b. Apply to all Bureau divisions and offices, and their employees; and to the personnel and facilities of contractors providing information resources support to the Bureau.

c. Concern non-national security information.

d. Pertain but are not limited to the following:

(1) Information created, transmitted, stored, processed or disseminated in any media form (e.g., magnetic tape, microfilm, paper documents).

(2) Information in any form when used as input to or retrieval from an information system.

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

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

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

2. Definitions.

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

b. Information Resources. Information and the personnel, monetary and technological elements involved in its creation, collection, storage, use, and dissemination.

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

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

e. 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 (e.g., word processors, copiers); telecommunications equipment (i.e., switches, networks); and the associated software for these types of equipment.

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

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

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

i. Data Base Administrator. An individual whose prime responsibility is to design and manage data base applications.

j. Sensitive Information/Data. Information or data that require protection due to the risk and magnitude of loss or harm which 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 requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.

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

l. Records. All written, machine readable, audiovisual and other documentary materials, regardless of physical form or characteristics, made or received by the Bureau 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, functions, policies, decisions, procedures, operations, or other activities, or because of the informational value of the recorded data.

m. 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".

n. Vital Records. Those records or information deemed necessary to ensure continuity of essential governmental activities during and following national emergency conditions, and also those records essential to the protection of the rights and interests of the Bureau and of the individuals for whose rights and interests it has responsibility.

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

p. 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.

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

3. Policy/Procedures.

a. Responsibilities. All personnel associated with the transmission, handling, and dissemination of information or data share responsibility in its protection. The specific

responsibilities assigned Bureau employees and custodians are listed below.

(1) The Director, OSMRE is responsible for promoting an attitude of concern for security among Bureau employees. The Director is responsible for establishing and implementing an effective information resources security program that conforms to Federal and Departmental regulations.

(2) The Assistant Director Information Systems Management is responsible for overseeing OSMRE's compliance with Federal and Departmental policies, guidelines and regulations pertaining to information resources security. He/she is responsible for appointing a Bureau Information Resources Security Administrator (BIRSA) and alternate to coordinate the management of OSMRE's information resources security program. The BIRSA position must be at an organizational level commensurate with the responsibility assigned and must be delegated sufficient authority to exercise this responsibility. Both the BIRSA and alternate must be knowledgeable in information technology and security matters and be Departmental employees unless a waiver is granted by the Departmental Information Resources Security Administrator.

(3) The Assistant Director Budget and Administration is responsible for overseeing OSMRE's compliance with Federal and Departmental policies, guidelines and regulations pertaining to physical, personnel, and information/document security programs. The Bureau Security Officer, Records Management Officer, and Privacy Act Officer have specific responsibilities for the performance of these functions.

(4) All Headquarters and Field Assistant Directors, are responsible for appointing an Installation Information Security Officer (IIRSO) and alternate, and for designating resource managers and system owners for facilities and systems under their jurisdiction. The IIRSO and alternate must be knowledgeable in information technology and security matters and be Departmental employees, unless a waiver is granted by the Departmental Information Resources Security Administrator.

(5) The Bureau Information Resources Security Administrator (BIRSA) is responsible for administering the information resources security program, coordinating all Bureau activities designed to protect information resources, promoting security awareness, and reporting on the effectiveness of these activities to Bureau and Departmental management. The BIRSA will consult with all Bureau officials having security responsibility (e.g., the Bureau Security Officer, the Records Management Officer, system owners) to ensure that information resources are adequately safeguarded throughout the Bureau. The responsibility assigned the BIRSA does not supersede or replace the security responsibilities previously assigned any other Bureau official.

(6) The Installation Information Resources Security Officer (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.

(7) The Bureau Security Officer is responsible for implementing the Departmental policies regarding physical, personnel and information/document security for OSMRE. 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 Bureau Security Officer. All ADP enforcement issues will be processed through the Bureau Security Officer.

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

(9) The Privacy Act Officer is responsible for the development and implementation of programs to manage agency records covered by the Privacy Act (i.e., 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.

(10) Supervisors/Managers will ensure that employees' performance standards contain appropriate referances to their security responsibilities, that employees receive security clearances and ADP access certifications appropriate to the job they will perform, and that employees receive an adequate level of security training. Supervisors/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.

(11) System Owners are responsible for implementing safegaurds to ensure the protection and proper use of the information resources under their domain. 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, and ensuring that adequate security requirements are incorporated into

internal or contract specifications prior to the acquisition or design of these systems. They are responsible for conducting risk analyses, and developing continuity of operations plans for systems under their domain.

(12) The Resource Manager is responsible for the overall management of an information technology facility. 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 ensuring that adequate security exists at the facility in conformance with Departmental and system owner requirements. He/she is responsible for conducting a risk analysis and for developing a continuity of operations plan for the facility.

(13) The Data Base Administrator is responsible for implementing and controlling access to a data base.

(14) Users of information and technological resources are responsible for complying with all security requirements pertaining to the resources they utilize and are accountable for all activity performed under User ID's/passwords which have been assigned to them for the use of automated systems.

b. Procedures. Successful implementation of an information resources security program is dependent upon accurately determining potential risks and instituting safeguards to minimize them. Every Bureau information system and every information technology facility operated by or on behalf of the Bureau must be protected. It is the responsibility of the system owners and resource managers to ensure the protection of information systems and facilities under their control. The basic methodology for ensuring that this occurs is outlined below.

(1) Risk Analysis. Performance of a risk analysis is the first step in establishing a security plan. Risk analyses must be performed 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 National Bureau of Standards (NBS) Federal Information Processing Standards Publications (FIPS PUBs) 31 and 65.

(a) Information Technology Facilities and Automated Application Systems. A risk analysis shall be performed at least every five years if one has not been performed 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 (i.e., either hardware or software) of the computer on which the system is operated changes so as to create the potential for either greater or easier access.

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

(2) Protection. Specific safeguards should be employed to provide a reasonable means of counteracting each threat described in the risk analysis and for detecting actual or potential security violations. At a minimum, the following procedures should be considered:

(a) Physical Security. Appropriate practices and safeguards must be utilized 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 position sensitivity for positions under their domain. System owners are responsible for ensuring that Federal personnel and contractors managing or using systems under their domain have appropriate sensitivity clearances. The criteria for determining sensitivity levels and the procedures for initiating sensitivity clearances are contained in OSMRE directive entitled "Personnel Security Program", PER-13. It is the supervisor's responsibility to ensure that employees using 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 password usage, encryption, security software) shall be utilized to prevent the unauthorized access and use of information, data and software resident on peripheral devices or storage media or in the process of being communicated via technological means.

(d) Administrative Security. Procedures shall be established and disseminated 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.

(3) Automated Application Safeguards. Specific procedures must be followed to ensure that appropriate safeguards are incorporated into automated application systems. They include:

(a) Determining appropriate security safeguards prior to system development or acquisition;

(b) Conducting design reviews and system tests prior to system implementation to ensure that the system satisfies the approved security requirements;

(c) Certifying prior to implementation that a new system satisfies applicable policies, regulations and standards and that its security safeguards are adequate; and

(d) Evaluating at least every three years the sufficiency of security safeguards for existing sensitive systems.

(4) Continuity of Operations Planning.

(a) Information Technology Facilities and Automated Application Systems. It is the responsibility of facility managers and system owners to develop a Continuity of Operations Plan (COOP) 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 appropriateness of the established procedures. It shall be revised when indicated by changes in software, equipment or other related factors. At a minimum, the COOP shall address the following:

1 Procedures for backup storage and recovery of data and software;

2 Establishment of processing capabilities and procedures for transferring operations to an alternate site;

3 Consistency between application system COOP's and the COOP of the information technology facility where the application is processed; and

4 Annual testing of the COOP at large ADP mainframe installations and other installations that provide essential bureau ADP support.

5 NBS FIPS PUB 31 contains guidance for developing contingency plans.

(b) Manual Application Systems. Continuity of operations plans must be developed for all manual application systems containing vital records to ensure their continued protection and so that essential Bureau activities can 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 Bureau employees must be adequately trained so that they may fulfill their security responsibilities. All contractor personnel must be advised of OSMRE security requirements and regulations. The level of security awareness activities in which employees participate shall be dependent 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; briefings, guides and/or films designed to acquaint employees with the nature of risks associated with information resources and the use of security measures to counteract them;

(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; and

(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) Acquisition Planning. It is essential that appropriate safeguards be determined before the acquisition of information technology resources not only to ensure the wise expenditure of funds but also so that resources may be 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 conform to, the regulations 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. It is the responsibility of every employee to report at the time of discovery all suspected, actual, or threatened security incidents involving information resources to the Bureau officials indicated below. The type of incident encountered will determine to whom it should be reported. The responsible Bureau 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 warrented, 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 Bureau 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 Bureau Head and the National Archives and Records Administration.

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

(d) Incidents involving technology resources resulting in the loss of technology, fraud, or compromise/disclosure of sensitive material shall be reported at the time of discovery. All computer hacker incidents shall be reported to the OIG via the OIG hotline and to the BIRSA via conventional communication lines. All other types of technological security incidents should be reported only to the BIRSA using conventional communication lines. The OIG hotline can be reached as folows: Washington, D. C. area (202) 343-2424; Toll free long distance (800) 424-5081

TAKE PRIDE IN AMERICA

OFFICIAL FILE COPY

OFFICE	IRM
SURNAME	
DATE	2/9/88
OFFICE	IRM
SURNAME	RTA
DATE	2-9-88
OFFICE	DRM
SURNAME	Atkins
DATE	02/3
OFFICE	
SURNAME	2-25-88
DATE	
OFFICE	DD-OTS
SURNAME	
DATE	2-25-88
OFFICE	BOLDT
SURNAME	2-25-88
DATE	
OFFICE	
SURNAME	
DATE	
OFFICE	
SURNAME	
DATE	

Review and Evaluations.

(1) The Department of Interior, Office of Information Resources Management, will conduct periodic reviews and evaluations of Bureau information resources security programs to ensure compliance with Federal and Departmental directives.

(2) Each IIRSO will conduct an annual review of the installation's information resource security program to assess its effectiveness and to recertify the adequacy of the installed security safeguards. These reviews may utilize existing reports, such as those for 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 forassuring the adequacy of the installation's automated information system security.

(3) Each IIRSO will prepare an annual installation security report. This report will be incorporated in the BIRSA's annual Bureau security plan for transmittal to the Departmental Information Resources Security Administrator. The output of the annual reviews described in paragraph c.(2) above should serve as the basis for this report.

4. Reporting Requirements. As stated in the directive.

5. References.

This directive implements guidance published in the Departmental Manual (375 DM 19); Departmental Manual, ADP Standards Handbook, (306 DM Chapter 2); (Office of Management and Budget Circular No. A-130 on the Management of Federal Information Resources; the General Services Administration's Federal Information Resources Management Regulations on security, privacy, Automated Data Processing (ADP) and acquisition, telecommunications management and acquisition, and records management; National Bureau of Standards Federal Information Processing Standards Publications dealing with security; the Office of Personnel Management's Federal Personnel Manual; the National Archives and Records Administration's regulations on records management; National Security Decision Directive 145; and Department of Treasury Directive 81-80 on Electronic Funds and Securities Transfer Policy - Message Authentication.

6. Effect on Other Documents. This directive replaces OSMRE Directive ADP-2, "Automated Data Processing (ADP) Security Program".

7. Contact. Information Systems Management Directorate, Division of Resource Management, Bureau Information Resources Security Administrator (or alternate) (202) 343-5909.