

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

TRANSMITTAL SHEET

Release No. 169

March 23, 1990

SUBJECT: Administrative Series
Part 375 Information Resources Management
Program Management
Chapter 19 Automated Information Resources Security
Program

EXPLANATION OF MATERIAL TRANSMITTED:

This manual chapter prescribes policies, procedures, and responsibilities for the management and implementation of an Automated Information Resources Security Program within the Minerals Management Service.


Acting Director

3/23/90

FILING INSTRUCTIONS:

REMOVE:

INSERT:

<u>Part</u>	<u>Chapter</u>	<u>Pages</u>	<u>Release</u>	<u>Part</u>	<u>Chapter</u>	<u>Pages</u>	<u>Release</u>
306	7	1-11	75	375	19	1-17	169
	7-H-3		90				

PEN AND INK CHANGES: Release Number 113, delete 306.7-H-1 and insert 375.19-H-1 throughout handbook and Release Number 87, delete 306.7-H-2 and insert 375.19-H-2 throughout handbook.

OPR: Information Technology Branch
Information Resources Management Division
Office of Administration
Office of Management and Budget

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources

Administrative Series

Management Program

Automated Information

Chapter 19 Resources Security Program

375.19.1

1. Purpose. This chapter prescribes policies, procedures, and responsibilities for the implementation and management of an Automated Information Resources Security Program within the Minerals Management Service (MMS).

2. Objective. The MMS Automated Information Resources Security Program is established for the protection of all automated information resources owned by or operated on behalf of the MMS to accomplish a Federal function.

3. Authority.

A. Federal Information Resources Management Regulation, Part 201.7 Security of Information Resource Systems, Amendment 1, December 1984.

B. Office of Management and Budget (OMB) Circular Number A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems.

C. Public Law (P.L.) 100-235, The Computer Security Act of 1987.

D. Office of Personnel Management, 5 CFR Part 930, Training Requirements for the Computer Security Act.

E. P.L. 97-255, The Federal Managers' Financial Integrity Act.

F. OMB Circular Number A-123, Internal Control Systems.

4. References.

A. Departmental Manual (375 DM 19 and 441 DM).

B. MMS Manual (MMSM), 375.19-H-1 Automated Information Resources Security Program, Handbook Conducting an ADP Risk Analysis and MMSM, 375.19-H-2 Automated Information Resources Security Program, Handbook Preparing an ADP Continuity of Operations Plan.

C. MMSM 317, Privacy Act Requirements.

D. MMSM 386, Safeguarding of Records and Information.

OPR: Information Technology Branch
Office of Administration

Supersedes Release No. 75

Date: March 23, 1990 (Release No. 169)

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources
Management Program

Administrative Series

Automated Information

Chapter 19 Resources Security Program

375.19.4E

E. MMSM 400, Property Management Accountability and Responsibility.

F. OMB Bulletin Number 88-16, Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information, July 6, 1988.

G. MMSM 730, Internal Control Systems.

H. Information Technology Installation Security, Office of Technical Assistance, Federal Computer Performance Evaluation and Simulation Center (FEDSIM).

5. Definitions. See Glossary, Appendix 1.

6. Policy. It is the policy of the MMS to ensure the protection of its automated information resources. The MMS will have one Automated Information Resources Security Program and that program will be consistent from one location to another while making allowances in size, scope, physical facilities, environmental factors, and use of the various ADP installations of the Bureau.

7. Exceptions. This chapter does not apply to any resources classified for national security.

8. Oversight.

A. The MMS will have a Bureau Information Resources Security Administrator (BIRSA) and an alternate. The BIRSA will report to the Associate Director for Management and Budget for ADP security matters and shall be delegated sufficient authority to exercise this responsibility. An additional performance element pertaining to this function will be included in the BIRSA's performance standards and will state or carry the following intent: "Automated Information Resources Security Administration: Administers the MMS Automated Information Resources Security Program." The BIRSA and alternate positions will be designated critical-sensitive and the position descriptions of each will include reference to specific security responsibilities required of the incumbents.

B. The Bureau will be divided into organizational components, designated as ADP installations by the Associate Directors for the purposes of this policy. They will assign to each an Installation ADP Security Officer (IADPSO) and an alternate.

C. The IADPSO will report directly to the senior manager directly responsible for the installation for installation-related ADP security matters, and shall be delegated sufficient authority

Page 2

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources

Administrative Series

Management Program

Automated Information

Chapter 19 Resources Security Program

375.19.8C

to exercise this responsibility. Certain IADPSO responsibilities may be delegated, yet overseen, by the IADPSO at his/her discretion. The IADPSO and alternate positions will be designated critical-sensitive and the position descriptions of each will include reference to specific security responsibilities required of the incumbents.

D. Any manager, in conjunction with the IADPSO, may establish additional policy and guidance as deemed necessary, providing such policy/guidance does not countermand established MMS policy or procedures. A copy of all such additional policy and guidance will be sent to the BIRSA for review and reference.

E. Additional oversight activities may be conducted on the Program or any component to assess compliance with regulations and to review the quality of the Program. Security reviews and evaluations typically may be conducted by any of the following:

- (1) The OMB;
- (2) the General Accounting Office;
- (3) the Department's Office of Information Resources Management (OIRM);
- (4) the Department's Office of Inspector General (OIG);
- (5) the MMS Internal Control Coordinator (ICC);
- (6) the MMS Security Officer;
- (7) the MMS Records Manager; and
- (8) the MMS Privacy Act Officer.

The BIRSA will generally be notified by the oversight authority in the event a review is to be conducted at any ADP installation. The IADPSO will notify the BIRSA should the BIRSA be circumvented by any authority scheduling a review at the installation (including unannounced visits.) In addition, the IADPSO will forward to the BIRSA a copy of any review documentation or final report issued to the installation directly by an oversight authority.

9. Responsibilities.

A. All Associate and Regional Directors, the Chiefs of the Office of Congressional and Legislative Affairs, Public Affairs,

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources
Management Program

Administrative Series

Automated Information

Chapter 19 Resources Security Program

375.19.9A

and Equal Employment Opportunity, and the Administrative Service Center Managers are responsible for the implementation of the MMS Automated Information Resources Security Program within their respective organizations.

B. The Associate Director for Management and Budget is responsible for the formulation, establishment, coordination, compliance, and interpretation of automated information resources security policies and instructions; appointment of the BIRSA and alternate; development of the MMS Automated Information Resources Security Program to include appropriate policies and procedures; and, review of MMS implementation.

C. The BIRSA is the individual within the MMS who has responsibility for overall administration of the MMS Automated Information Resources Security Program and fulfills the role of the BIRSA, as prescribed by 375 DM 19. The BIRSA must be knowledgeable in ADP and ADP security matters. Additionally, the BIRSA must be an MMS employee. The BIRSA will act as the Bureau focal point for all ADP security matters. Specifically, the BIRSA is responsible for:

(1) Ensuring that the following oversight reviews are conducted:

(a) Annual ADP Installation Reviews. Each ADP installation will undergo a thorough evaluation every year to certify that the installation meets the minimum requirements of this policy. The review should be a coordinated effort between the ADP Managers, the BIRSA, and the respective IADPSO's. The results will be documented and will identify weaknesses and recommend corrective actions. The report will be approved by the appropriate Associate or Regional Director and will serve as the basis for the Annual Bureau Security Plan.

(b) Internal Control Evaluations. ADP internal control evaluations are coordinated by the MMS ICC and management officials and are conducted according to very specific guidelines. Generally, these evaluations are scheduled every three years. Because such evaluations include inspection of related security activities and safeguards, they should be conducted concurrently with annual ADP installation reviews, thereby eliminating any redundancy in the two studies. ADP internal control evaluations are briefly described below:

(i) Computer Center Control Evaluations are conducted for each mainframe and minicomputer center designated

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources

Administrative Series

Management Program

Automated Information

Chapter 19 Resources Security Program

375.19.9C(1)(b)(i)

as a separate internal control component in the Management Control Plan.

(ii) Automated Application System Control Evaluations. Each application system within the MMS has been identified and associated with internal control components. These evaluations are conducted concurrently with the specific internal control component with which they have been identified. As a result, it may not be practical to conduct these evaluations concurrently with the required annual ADP installation review. However, the information collected while conducting these reviews should be used to avoid any duplication of effort.

(iii) Other ADP-related internal control evaluations may be also scheduled as they are identified.

(c) Other Evaluations. Security reviews of ADP installations or systems will be conducted upon request at any time by the Director, Associate Directors, Regional Directors, ADP Managers, or other authority.

(2) Maintaining copies of each review or evaluation conducted.

(3) Informing appropriate managers of any security deficiencies and/or noncompliance with regulations and conducting a followup review to assure actions are completed.

(4) Attending a minimum of one security training seminar or course each year. The training should relate to items of particular interest to the BIRSA or to specific Bureau ADP security problems.

(5) Submitting formal written reports for all security incidences in any circumstance warranting departmental notification.

(6) Updating this policy as deemed necessary to accommodate departmental and technological changes.

(7) Preparation of the Annual Bureau Security Plan and submission to the OIRM, as requested.

(8) Ensuring that security aspects of critical systems and a summary of the Computer Security Plans are included in the IRM Strategic Plan to ensure continued funding for ADP resources and activities in accordance with P.L. 100-235.

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources

Administrative Series

Management Program

Automated Information

Chapter 19 Resources Security Program

375.19.9C(9)

(9) Oversight of mandatory, periodic security training requirements of P.L. 100-235 with training personnel, IADPSO's, supervisors, and managers.

(10) Maintaining an inventory of all sensitive and critical systems in compliance with P.L. 100-235.

(11) Collection of Computer Security Plans from the ADP Managers and submission of the plans to OIRM upon request for National Institute of Standards and Technology and National Security Agency advice and comment. The BIRSA must also ensure that the plans are updated and improved as directed by the Department.

(12) Submission of the Annual Statement on Bureau Automated Information System Security to the MMS ICC, upon request. This statement satisfies departmental requirements and describes whether adequate security exists in MMS automated information systems. It also provides for the description of material security weaknesses identified during audits or reviews of ADP installations or sensitive applications.

(13) Issuing ADP security bulletins as necessary on security awareness issues.

D. The IADPSO is the individual who serves as the focal point for all ADP security matters associated with the respective designated ADP installation. The IADPSO's must be knowledgeable of ADP and ADP security matters. Specifically, each IADPSO is responsible for:

(1) ADP Security Plans. The BIRSA will formally solicit input to the Annual Bureau Security and Computer Security Plans from the ADP Managers. However, the IADPSO will need to maintain the following information for their respective installations and provide it to the ADP Managers as requested:

(a) A descriptive list of all ADP installation-specific applications and software;

(b) Updated risk analyses or continuity of operations plans. Do not include those unchanged from the previous submission;

(c) Written results of contingency plan tests;

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources

Administrative Series

Management Program

Automated Information

Chapter 19 Resources Security Program

375.19.9D(1)(d)

(d) A description of major security accomplishments or activities conducted during the previous fiscal year. Do not include those activities conducted by the BIRSA;

(e) ADP installation-specific security documentation produced/issued by the IADPSO or management;

(f) A descriptive, summarized list of major ADP equipment, including telecommunications equipment;

(g) A description of any actual or perceived security problems facing the installation;

(h) A milestone schedule of any security activities planned for the current fiscal year; and,

(i) Other items as the OIRM updates its requirements.

(2) Ensuring that a risk analysis is conducted for the installation and obtaining management concurrence that indicates whether the risks are accepted or proposed safeguards will be adopted.

(3) Ensuring that continuity of operations plans are developed, maintained current, and tested annually.

(4) Ensuring that all users of the installation-specific systems are aware of their security responsibilities. This can be accomplished through briefings, memoranda, or other means.

(5) Attending a minimum of one security training seminar or course each year. The training should relate to areas of special interest or to installation-specific security problems.

(6) Reporting any major security incidents immediately to the BIRSA. Major incidents include those which cannot be handled in-house or those which may receive Bureauwide or national attention. They also include those incidents which occurred in the general vicinity of the installation, yet had no impact on the installation such as earthquakes, air disasters, tsunamis; anything in which the BIRSA should be kept knowledgeable to ensure credibility in the program.

(7) Identifying security needs for new or replacement equipment, software, and services and ensuring their inclusion in the procurement process.

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources
Management Program

Administrative Series

Automated Information

Chapter 19 Resources Security Program

375.19.9D(8)

(8) Ensuring that reasonable technical, physical, and administrative controls are present to protect the installation's automated information resources.

(9) Coordinating security awareness training, required by The Computer Security Act of 1987, with the ADP Managers and the servicing training offices for all individuals associated with the installation.

(10) Becoming knowledgeable of the various planning activities related to computer security (budget submissions, Strategic Plan, computer security plans, etc.).

E. All MMS supervisors are responsible for:

(1) Ensuring that each subordinate is aware of his or her security responsibilities.

(2) Providing appropriate technical, physical, and administrative security safeguards for the automated information resources for which they are responsible.

(3) Ensuring compliance with this policy.

(4) Contacting the IADPSO to identify security requirements in the procurement of new or replacement equipment, software, and services.

(5) Ensuring that departing employees do not access any automated information resources after initiating the Form MMS-1090, Employee Exit Clearance Report, if the departing employee poses any risk to those resources. Supervisors may be held responsible for any damage to these resources by departing employees.

F. Users are responsible for ensuring that all work performed through their user identification codes and passwords is for official Government use only. Any user who suspects unauthorized use should immediately:

(1) Change his/her password or request that it be changed; and,

(2) Notify the BIRSA or IADPSO and immediate supervisor of his/her suspicions.

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources

Administrative Series

Management Program

Automated Information

Chapter 19 Resources Security Program

375.19.9G

G. ADP Managers are responsible for:

(1) Annual Bureau Security Plan. The BIRSA will require specific input from each ADP Manager concerning all ADP environments within the Bureau. Installation-specific input should be obtained from the IADPSO's. As the departmental due date may vary, the BIRSA will make every attempt to allow ample time to gather the specific information. This input may be submitted informally and must include the following:

(a) A descriptive list of all ADP systems, to include applications and software;

(b) a descriptive list of all contingency plans prepared;

(c) written results of contingency plan tests for mainframe and minicomputer centers;

(d) a description of major security accomplishments or activities conducted during the previous fiscal year. Do not include those activities conducted by the BIRSA;

(e) all security documentation produced/issued by the program area;

(f) a descriptive, summarized list of major ADP equipment, including telecommunications equipment;

(g) a description of any actual or perceived security problems facing the program area;

(h) a milestone schedule of any security activities planned for the current fiscal year; and

(i) other items as the OIRM updates its requirements.

(2) Computer Security Plans. The ADP Managers will provide the BIRSA with Computer Security Plans prepared according to guidance provided in OMB Bulletin Number 88-16, as requested.

(3) Ensuring that each individual involved in the management, use, or operation of all MMS systems is periodically trained in computer security awareness and accepted computer security practices.

(4) Providing the BIRSA with status updates on ADP internal control evaluations, as requested.

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources

Administrative Series

Management Program

Automated Information

Chapter 19 Resources Security Program

375.19.10

10. Program Components.

A. Risk Analyses. A qualitative risk analysis must be performed for each ADP installation and will be available to the BIRSA upon request.

(1) Frequency. The analysis will be conducted at least every 5 years, or whenever any of the following circumstances occurs:

(a) Whenever a major security incident occurs either dramatically affecting the continuity of operations and/or incurring significant loss; and,

(b) Prior to an equipment or installation relocation significantly affecting the outcome of the most recent analysis.

(2) Risk Analysis and Report. There are many automated tools which can be used to conduct the analysis. The Handbook, MMSM 375.19-H-1, Conducting an ADP Risk Analysis, may also be followed for the purposes of this analysis. The handbook contains all of the components recommended by the Department including guidance on the required report. Deviation from this standard approach is permitted without BIRSA approval if the exercise and resultant report minimally accomplish the following:

(a) Identify both the nature and potential source of all relevant physical, personnel, administrative, and technical threats to a specific facility, installation, or system;

(b) Detail the probability of occurrence of each potential threat and the likely extent of damage;

(c) Evaluate the nature of the information being stored, processed or communicated and determine whether it should be designated "sensitive";

(d) Discuss the impact which would result from the loss or misuse of information resources; and,

(e) Propose safeguards based upon the results of the analysis.

(3) Distribution. The risk analysis report is considered a sensitive document and is for MMS internal use only.

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources

Administrative Series

Management Program

Automated Information

Chapter 19 Resources Security Program

375.19.10B

B. Contingency Planning.

(1) Mainframe and Minicomputer Centers. A detailed Continuity of Operations or Contingency Plan will be developed for each mainframe and minicomputer center and will be available to the BIRSA upon request. The plan may be limited to the center or may be expanded to include an entire installation. The Handbook, MMSM 375.19-H-2, Preparing an ADP Continuity of Operations Plan, should be followed in developing the plan. The Handbook contains all of the components recommended by the Department. Deviation from this standard approach is permitted without BIRSA approval provided all of the components of the MMS Handbook are included in the plan. At a minimum, the plan will be:

- (a) Documented;
- (b) Maintained current;
- (c) Certified by both the highest ranking official directly responsible for the installation and the IADPSO;
- (d) Tested annually, providing written test results to the BIRSA with the required Annual Bureau Security Plan for review and reference;
- (e) Disclosed to others, with the exception of the BIRSA, in accordance with the requirements of the Privacy Act; and,
- (f) Stored offsite.

(2) Other ADP Environments. Informal contingency plans will be developed for all other sensitive/critical ADP systems by the system managers or other individuals directly responsible for these systems. These plans will be maintained current, stored offsite when deemed necessary or for all critical systems, and will be available to the BIRSA upon request. The purpose of these informal contingency plans is to ensure continued operation of the organization in the event of a disaster, i.e., from a power outage during a lease sale, to complete destruction of the building during a critical processing time. These plans are intended to prepare the user for an emergency situation where continued processing is necessary. At a minimum, these plans will include:

- (a) Possible alternate processing sites, within the same building and/or elsewhere;

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources

Administrative Series

Management Program

Automated Information

Chapter 19 Resources Security Program

375.19.10B(2)(b)

(b) A list of all software, equipment (including all internal upgrades), cable configurations, etc.;

(c) The schedule and responsibility for regular backups;

(d) Maintenance and repair information;

(e) A copy of all applicable major requisitions; and,

(f) A copy of all operating procedures for systems developed in-house or by contractors and any other pertinent documentation which cannot be readily obtained or replaced. The plan may reference this documentation if it is available elsewhere offsite in the event of an emergency.

C. Physical Security.

(1) Mainframe and Minicomputer Centers. All mainframe and minicomputer centers will be designed to meet the minimum physical security specifications of 444 DM, Physical Security.

(2) Proprietary Information. All proprietary data or information provided to or generated by the MMS will be protected in accordance with MMSM 386, Safeguarding of Records and Information.

(3) Networked and Stand-Alone Microcomputer Systems. All microcomputer systems will be located in access restricted or lockable offices when possible. External locks will be installed for those systems located in public offices or other offices in which physical access is not or cannot be enforced. These external locks will serve to hinder, deter, or prevent theft of the equipment.

(4) Equipment Accountability. Most ADP equipment is subject to the provisions of MMSM 400 Property Management, Chapter 1, Accountability and Responsibility. Hardware upgrades, cables, data switches, power surge protectors, etc., are not covered under the provisions of MMS property accountability policy. IADPSO's and/or supervisors are encouraged to devise their own accountability systems to properly manage nonaccountable equipment.

(5) Printouts. All sensitive computer printouts will be either retained in locked bins or controlled in some manner prior

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources
Management Program

Administrative Series

Automated Information

Chapter 19 Resources Security Program

375.19.10C(5)

to pickup by authorized individuals. Upon request, printout bins will be covered in such a way as to conceal the contents from view.

(a) Mainframe and Minicomputer Centers. Printouts are the responsibility of the computer center operator prior to pickup. Sensitive trash will be stored in a locked trash container or in a locked room prior to shredding. Each center will make locked trash containers or other secured areas available to users for sensitive trash disposal.

(b) Users. Users are responsible for sensitive printouts after pickup. These printouts must be stored in a desk, cabinet, or someplace out of view when unattended. Printouts containing proprietary data/information will be handled in accordance with MMSM Part 386, Safeguarding of Records and Information. All sensitive printouts to be disposed of will be stored in a locked trash container or in a locked room and then shredded.

D. Technical Security.

(1) Access Control. All ADP systems will be internally protected against unauthorized access to the degree possible, practical, or economically beneficial. Additionally, all systems applications, models, programs, routines, etc., will have more than one authorized user when there is no provision or capability for password override or bypass.

(2) Backups. All ADP systems will be regularly backed up. Backups for systems are the responsibility of the supervisor or systems manager directly responsible for the system. Backups of all critical and sensitive systems will be stored offsite.

(3) Audit Trails. Internal audit controls are required for all mainframe and minicomputer center systems, all local and wide area networks, and recommended for all other systems.

(4) Data Communications. All systems sending and receiving information electronically will employ some measure of data communications security. All data communications for critical systems will include backup communications capability or plan in the event of a communications outage.

E. Copyrighted and Licensed Material. No software, accompanying documentation, etc., protected by copyright laws and license agreements will be illegally duplicated. Restrictions of licensed software may vary, but all use is subject to the limitations of copyright laws and software/documentation licenses.

DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

Part 375 Information Resources

Administrative Series

Management Program

Automated Information

Chapter 19 Resources Security Program

375.19.10E

Actual and suspected violations of copyright laws and licensed material will be immediately reported to the IADPSO or to the BIRSA.

F. Personnel Security.

(1) IADPSO's. IADPSO's may be called upon by the supervisor to assist in determining position sensitivity with respect to sensitive ADP activities.

(2) MMS Personnel Security Program. Personnel security information required by the various auditing and oversight authorities will be forwarded to the MMS Security Officer for action as appropriate.

G. Security Incidents. Actual or suspected security incidents must be reported to the proper authorities as categorized below.

(1) MMS Security Officer. The MMS Security Officer will be notified in the event of physical (property theft or destruction), personnel, or national security incidents.

(2) Records Manager. The Records Manager will be notified in the event of the unlawful removal, defacing, alteration, or destruction of records.

(3) Privacy Act Officer. The Privacy Act Officer will be notified in the event of any Privacy Act violations.

(4) BIRSA/IADPSO. The BIRSA/IADPSO will be notified in the event of any security incidents involving automated information resources. Other reporting requirements are outlined under the responsibilities described for both the BIRSA and IADPSO's.

GLOSSARY

ADP Installation. Refers to an organizational component so designated in compliance with departmental policy.

ADP Managers. MMSM 376.1.6.C. states that the Associate Directors are responsible for designating ADP Managers to serve as a point of contact for the Bureau ADP Manager and to carry out program ADP activities. The Bureau ADP Manager is the Chief, IRM Division, Office of Administration. For the purposes of this policy, the other ADP Managers are as follows: Chief, Systems Management Division, Royalty Management Program; Manager, Offshore Systems Center; and Chief, Office of Offshore Management Support, Offshore Minerals Management.

Annual Bureau Security Plan. The OIRM requires that each Bureau submit an annual planning document which describes Bureau automated information resources security activities. This planning document, required by OIRM, is not to be confused with the Computer Security Plans required by P.L. 100-235.

Automated Information Resources. All hardware and software resources associated with mini-, mainframe, micro-, personal, or other computer system.

Computer Security Plans. The Computer Security Act of 1987 (P.L. 100-235) requires the identification of each computer system which contains sensitive information and the preparation of plans for the security and privacy of such systems. The format and content of the Computer Security Plans are established in OMB Bulletin Number 88-16. These documents, required by P.L. 100-235, are not to be confused with the Annual Bureau Security Plan, a separate OIRM requirement.

Classified. Refers to defined, specific sensitivity levels for anything pertaining to National security.

Computer System. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related services as defined by regulations issued by the General Services Administrator pursuant to section iii of the Federal Property and Administrative Services Act of 1949.

Critical Systems. Refers to systems whose functions are essential to the continued operation or mission of the Bureau.

Information Resources. All resources, regardless of physical form or characteristics, involved in the collection, storage, processing, transmission, etc., of information/data.

Installation Manager is that individual directly responsible for the mainframe or minicomputer center. In Offshore, this is frequently the ADP Unit or Section Chief; in the Office of Administration, this refers to the Chief, Administrative Systems Branch; in the Royalty Management Program, this refers to the Chief, Systems Management Division. However, in some instances, the Installation Manager could be interpreted to mean the Associate Director.

Internal Control. The plan of organization and methods and procedures adopted by management to provide reasonable assurance that obligations and costs are in compliance with applicable law; funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and revenues and expenditures applicable to Agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets. See OMB Circular Number A-123.

Internal Control Component. A major organization, program, or functional subdivision requiring one or more separate systems of internal control to:

- (1) Safeguard resources;
- (2) Assure the accuracy and reliability of timely reports and information;
- (3) Assure adherence to applicable laws, regulations, policies, and procedures; and
- (4) Promote operational economy and efficiency.

Mainframe and Minicomputer Centers. Refers to each mainframe and minicomputer physical facility and all of the associated hardware, software, systems, etc.

Management Control Plan is a report prepared by the MMS Internal Control Coordinator. It contains an inventory of components, indicates the results of prior and current assignment ratings, and includes a schedule of detailed internal control reviews of

appropriate components. The plan is updated annually and requires input from program managers who direct or control resources.

MMS Internal Control Coordinator. The Office of Policy and Planning official designated to coordinate and facilitate compliance with OMB Circular Number A-123 as set forth in relevant guidance issued by OMB, GAO, OIG, and PFM.

Proprietary Data/Information. In general, proprietary data/information is that which is:

- (1) Prohibited from release by statute;
- (2) Submitted to the Government in expectation of confidentiality, and its protection is required in order to prevent competitive harm;
- (3) Obtained by the Government under the requirements of the law or for the purpose of evaluating any facet of the resource programs. The unauthorized release of the data/information is capable of causing substantial competitive harm to persons, organizations, corporations, etc., about whom the information is obtained, or;
- (4) Created by the Government in its own interest for the purpose of gaining full value for its resources or for protecting those resources from exploitation.

Sensitive. Refers to that which the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Does not include defense and intelligence related systems, systems operated at all times under rules designed to protect classified information, or mixed systems classified or unclassified at other times provided they are operated at all times under classified rules.