DEPARTMENT OF THE INTERIOR

MINERALS MANAGEMENT SERVICE MANUAL

TRANSMITTAL SHEET

Release No. 125 April 24, 1987

SUBJECT: Administrative Series
Part 386 Safeguarding of Records and Information
Chapter 1 Safeguarding and Identification of Proprietary Data/Information
Chapter 2 Standards for Marking Proprietary Data/Information
Chapter 3 Physical Protection of Proprietary Data/Information
Chapter 4 Access, Release, and Transmittal of Proprietary Data/Information
Chapter 5 Standards for Reproduction and Destruction of Proprietary Data/Information

EXPLANATION OF MATERIAL TRANSMITTED:

These chapters establish policies, responsibilities, and procedures for the protection of proprietary data/information transmitted to or generated by the Minerals Management Service.

Director

LEFT MARGIN

RIGHT MARGIN

FILING INSTRUCTIONS:

Remove: None

Insert:

Part	Chapter	Pages	Release
386	1	1-16	125
	2	1-3	
	3	1-22	
	4	1-13	
	5	1-2	

OPR: Procurement and General Services Division
Office of Administration

1A3 40303-288

1. Purpose. This chapter establishes policy and assigns responsibilities for the safeguarding and security of proprietary data/information, regardless of its form (e.g., paper, core samples, microfilm, magnetic tape, etc.), received or generated by the Minerals Management Service (MMS).

2. Objectives.

A. Ensure that the MMS safeguards from unauthorized disclosure proprietary data/information it receives or generates.

B. Provide guidance for identifying proprietary data/information.

C. Provide uniform procedures for marking proprietary data/information.

D. Provide uniform requirements for the physical protection of proprietary data/information storage facilities.

E. Provide uniform procedures for the access, release, duplication, and transmittal of proprietary data/information.

F. Provide standards for the proper maintenance, use, and disposition of proprietary data/information.

3. Authority.

A. Outer Continental Shelf Lands Act, as amended (43 U.S.C. 1331).

B. Federal Oil and Gas Royalty Management Act of 1982 (30 U.S.C. 1701).

C. Indian Mineral Development Act of 1982 (25 U.S.C. 2103).

D. Records Management by Federal Agencies (44 U.S.C. Chapters 31 and 33).

E. Government Organization and Employees (5 U.S.C. 301 and 302).

4. References.

A. MMS Manual (MMSM) 306.7, ADP Security.

B. MMSM 316, Freedom of Information Act (FOIA).

OPR: Procurement and General Services Division
Office of Administration
Date: April 24, 1987 (Release No. 125)

LEFT MARGIN

RIGHT MARGIN

IB340303

C. MMSM 380.2 Records Management and MMSM 380.2-H, Records Management Handbook.

D. MMSM 381.7, Automated Data Processing and Electronic Recordkeeping.

E. MMSM 441, Personnel Security.

5. Definitions. Glossary, see Appendix 1.

6. Policy.

A. It is the policy of the MMS to safeguard proprietary data/information identified in Appendix 2. All MMS facilities handling proprietary data/information must conform to established and required minimum security standards and procedures.

B. Stringent administrative action will be taken against any MMS employee or representative at any level of employment who discloses proprietary data/information for any purpose other than in the performance of his/her responsibilities as an employee or representative of the MMS. If violation of criminal statutes (Appendix 3) occurs, cases will be referred to the Department of Justice.

C. Proprietary data/information will not be disclosed automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the public domain of identical or similar information. Appearance in the public domain of information currently designated as proprietary or being considered for such designation does not preclude initial or continued protection. Holders of the information must continue required protective measures in accordance with applicable laws and regulations.

7. Responsibilities.

A. All Associate/Assistant Directors, Chiefs of the Offices of Congressional and Legislative Affairs and Minerals Management Information, Equal Opportunity Manager, Program Director for Strategic and International Minerals, Regional Directors, and Administrative Service Center(ASC) Managers are responsible for:

(1) Ensuring that employees under their jurisdiction, who handle proprietary data/information adhere to the requirements of this chapter.

1A240303

(2) Planning and upgrading security facilities and practices in their respective areas of responsibility.

(3) Reviewing proprietary data/information security plans for their respective areas to ensure that resources required to upgrade security facilities are available and appropriate. Forwarding security plans to the MMS Security Officer through the servicing ASC, General Services Branch, for review and approval.

(4) Designating and reporting the designation of a Proprietary Officer to the Security Officer and the Records Manager. It is recommended that the appropriate Records Officer be designated as the Proprietary Officer. If there is no Records Officer on site or proprietary data/information is maintained by individual offices, it is recommended that the office supervisor be designated as the Proprietary Officer.

(5) Ensuring that offices under their jurisdiction designate the sensitivity of positions which must access proprietary data/information to adequately perform required duties. Ensuring that appropriate personnel security paperwork for these positions is submitted in accordance with MMSM 441.

B. The Assistant Director for Administration is responsible for the development and direction of the MMS's security program and will:

(1) Designate an appropriately cleared Security Officer and an alternate.

(2) Provide written notification of the names, titles, addresses, and telephone numbers of the Security Officer and alternate to the Department's Security Officer.

C. The Security Officer carries out the responsibility of the Assistant Director for Administration for implementing the requirements of the MMS security program and will:

(1) Develop security policies, standards, and procedures for the protection of proprietary data/information.

(2) Inspect MMS and MMS contractor proprietary data/information security facilities to ensure compliance with MMS policy and make recommendations for necessary improvement.

IA6 40303

(3) Provide guidance and assistance to MMS personnel concerning the safeguards and security of proprietary data/information.

(4) Review proprietary data/information security plans; approve when acceptable or return such plans for necessary correction.

(5) Coordinate with space management officials to ensure that specifications for new space include adequate security provisions.

(6) Determine the suitability of employees for critical-sensitive and noncritical-sensitive positions which access proprietary data/information and notify appropriate supervisors of investigative results.

D. The Bureau Information Resources Security Administrator is responsible for ensuring that adequate physical, administrative, and technical safeguards are established to protect all automated proprietary data/information from damage, destruction, alteration, or misappropriation.

E. The Records Manager is responsible for:

(1) Ensuring that proprietary data/information is maintained and disposed of in accordance with MMSM 380.2.

(2) Promoting the objectives and standards contained in this part.

F. Proprietary Officers are responsible for:

(1) Ensuring that proprietary data/information in their custody is handled in accordance with the requirements of this chapter and MMSM 380.2-H.

(2) Planning and upgrading security facilities and practices in their respective areas of responsibility.

(3) Preparing proprietary data/information security plans and forwarding such plans to the appropriate official.

G. Supervisors are responsible for:

(1) Ensuring that proprietary data/information released to their organization is safeguarded in accordance with this chapter.

IBT 40303

(2) Ensuring that the appropriate position sensitivity is designated for positions under their jurisdiction which require access to proprietary data/information. Submitting appropriate paperwork as required by MMSM 441.1.6A(2) to ensure that personnel security requirements for these positions are satisfied.

(3) Ensuring that subordinates understand their responsibilities for safeguarding proprietary data/information and comply with applicable MMS policy.

(4) Ensuring that subordinates are aware of applicable penalties as stipulated by Federal regulations and Federal Criminal Statutes (see Appendix 3).

(5) Ensuring that proprietary data/information received or generated by their organization is marked as "PROPRIETARY - FOR U.S. GOVERNMENT USE ONLY."

H. Individual MMS Employees are responsible for the safeguarding and the security of proprietary data/information.

I. Contracting Officers are responsible for ensuring that the MMS proprietary data/information security standards, requirements, and procedures are incorporated into contractual agreements when contractors will be involved in handling proprietary data/information. Contractors and subcontractors performing under contract for the MMS must also comply with MMS policy (see MMSM 386.4.5E). Appropriate regulations and manual chapters will be referenced in solicitation and contract documents.

J. Contracting Officer's Technical Representatives are responsible for advising contracting officers of the need to address the handling of proprietary data/information in contract documentation.

K. Contractors having access to proprietary data/information for which the MMS is liable are responsible for:

(1) Designating a U.S. citizen (generally the Site Manager or Project Manager) to act as a security supervisor to direct security measures to ensure that proprietary data/information released to their organization is safeguarded in accordance with this chapter.

(2) Identifying in writing the designated security supervisor to the Contracting Officer's Technical Representative.

BOI

1B6 40303

FOR

(3) Limiting contract employees requiring access to the proprietary data/information to the absolute minimum necessary for performance of the job.

(4) Ensuring that contract employees understand their responsibilities for safeguarding proprietary data/information.

(5) Ensuring that contract employees are aware of applicable penalties identified in Appendix 3.

L. Freedom of Information Act (FOIA) Officer is responsible for ensuring compliance with MMSM 316 for all requests concerning proprietary data/information under the FOIA.

IA740303

GLOSSARY

Access. The ability and opportunity to obtain knowledge of proprietary data/information.

Authorized Officials or Persons. Individuals granted access to or authorized to receive proprietary data/information by the designated office head of an Agency. The Primary Office of Control determines whether an individual's duties require proprietary data/information access, receipt, or possession. The FOIA Officer and program personnel are authorized officials when the information is covered by an FOIA request.

Automated Data Processing (ADP) Security. Data integrity and the protection of automated information resources from modification, loss, destruction, or unauthorized access, disclosure, or use.

Closed Storage Room. A room designated as a repository for the overnight storage of proprietary data/information. Within the room, all material is secured in approved General Services Administration (GSA) security containers.

Compromise. The known or suspected exposure of proprietary data/information to an unauthorized person.

Custodian. An individual who has possession of or is otherwise charged with the responsibility for safeguarding proprietary data/information.

Data. Facts and statistics or samples which have not been analyzed or processed.

Document. Any recorded information regardless of its physical form or characteristics, including: written or printed matter, data processing cards and tapes; maps; charts; paintings; drawings; engravings; sketches; working notes and papers; or reproductions by any means or process; and sound, voice, magnetic or electronic recordings in any form.

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

Need-to-Know. The need to access particular proprietary data/information or material in order to satisfactorily perform required duties. The Primary Office of Control determines whether an individual's duties require proprietary data/information

IA8 40303

access, receipt, or possession. Requests for access to proprietary data/information must be evaluated both in terms of its sensitivity and the purpose for which it will be used. The FOIA Coordinator and program personnel have a need-to-know when information is covered by an FOIA request.

Primary Office of Control. The MMS office authorized to receive the proprietary data/information directly from an industry source and to reproduce and release the data/information as required. Any office to which proprietary data/information is later transferred becomes a Secondary Office of Control. The Primary Office of Control has the authority to grant reproduction and limited release to the Secondary Office of Control. For the purpose of this chapter, MMS personnel physically located in the same facility as the office receiving proprietary data/information will be regarded as a part of the Primary Office of Control or the Secondary Office of Control, as appropriate, and will have access to such information in accordance with their need-to-know.

Open Storage Room. Room(s) with controlled access which is used as a repository for the overnight storage of proprietary data/information. Within the room, the material is maintained on shelves or in cabinets, some or none of which are approved GSA security containers.

Physical Security. Physical safeguards designed for the protection of facilities, employees, equipment, and information.

Proprietary Data/Information. See Appendix 2, Identification of Proprietary Information.

Proprietary Data/Information Security Plan. A document that contains information about proprietary data/information storage facilities.

Secondary Office of Control. The office which is authorized to receive proprietary data/information from the Primary Office of Control for the conduct of official business. May also be granted by the Primary Office of Control limited authority to disseminate and reproduce proprietary data/information.

Visitor Control Station. A specific place in a particular facility where visitors are registered and cleared to see a particular individual and/or visit a specific facility site.

IBS 40303

IDENTIFICATION OF PROPRIETARY DATA/INFORMATION

1. Introduction. The following contains an explanation and examples of the types of data/information that are usually proprietary. The initial proprietary data/information designation is determined by the industry source providing the data or information to the Government. Broadly defined, proprietary data/information is either:

A. Prohibited from release by statute;

B. Submitted to the Government in expectation of confidentiality, and its protection is required in order to prevent competitive harm;

C. 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,

D. 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.

2. Proprietary Data/Information--Minerals Management Service (MMS).

A. Offshore Operating Records. Proprietary data/information consists of electric logs; core descriptions and analyses; well completion reports; maps; other geological, geophysical, seismic sections; and engineering information, etc., regardless of physical form. Data/information is furnished by industry sources to the MMS in compliance with the terms of leases, permits, and operating regulations. Such information, acquired at considerable cost to the industry source, is considered valuable property and has competitive value.

(1) Any data/information which reveals a specific company's or individual's interest in bidding for or in exploring a block(s) or areas on the Outer Continental Shelf is considered proprietary. For example, in response to a call for nominations, the specific identity of a block(s) or groups of blocks associated with an industry source is proprietary data/information. The combination of an industry source's name and the block(s) nominated by an industry source is commercial information concerning its future plans. This information is submitted in confidence to the

181 40303

MMS and could be used by a competitor to gain a commercial advantage if disclosed. However, the specific information may be summarized to reveal only the total number of industry source respondents and the total number of respondents interested in a specific block (i.e., a total of 10 industry sources responded, 8 of which expressed an interest in Block 264). Summary information which does not reveal an industry source's name and the block(s) nominated by that industry source is not proprietary.

(2) Records of wells drilled on OCS leases contiguous to, or cornering on, unleased tracts which reveal information pertaining to such unleased tracts are considered proprietary. A competitor could gain an advantage from this type of information if improperly released. Material which does not reveal proprietary data/information but does reveal information pertaining to an unleased tract only is not proprietary.

(3) Reserve Estimates. Computerized computations of oil and gas reserve estimates are generated by the MMS. These computations are derived from a variety of proprietary source documents submitted by individual industry sources. The computations of reserve estimates identify an individual industry source by specific lease and the reservoir of oil and gas remaining in the lease. These computations have competitive value and contain privileged and financial information concerning specific industry sources and may not be released. A summary report of oil and gas reserve estimates which does not contain proprietary data/information is generated by the MMS. The summary report contains an aggregation of oil and gas reserve estimates by field and may be released.

(4) Plans. Portions of Exploration Plans and Development and Production Plans that are required to be submitted to the MMS by individual industry sources contain proprietary data/information which may not be released.

(5) See OCS Order No. 12, "Public Inspection of Records," for guidance on the release of specific information.

B. Royalty Management Records. Data/information, regardless of the physical form, revealing the identity of a royalty payor/reporter and combined with production processing/volumes, and/or values is considered proprietary data/information. This proprietary data/information is furnished to the MMS by industry sources in order to comply with Federal contracts, leases, permits, and operating regulations. Unless permission to disclose this data/information is given by the submittee, the MMS must consider the

IA4 40303

information proprietary and protect it accordingly. This safeguards the Government from revealing commercial or financial information about an individual organization that could be used by a competitor to gain unfair advantage. For example, the amount of royalty paid by an individual payor is proprietary information. The share of production of an individual payor or reporter also is proprietary data/information. The names of payors only are not proprietary.

(1) Payor/Reporter Data/Information. Proprietary data/information is collected by the MMS from payors/reporters by electronic and written communications. Examples of two reporting forms are the MMS-2014, Report of Sales and Royalty Remittance (Oil and Gas), and the MMS-4014, Report of Sales and Royalty Remittance (Solid Minerals), which reveal the payor's name, address, telephone number, share of production, and royalty rates. Such data/information is proprietary and may not be released.

(2) Indian Leases. All production and royalty data/information at the lease level on Indian leases is considered proprietary. All requests for such information should be referred to the Bureau of Indian Affairs, Department of the Interior. However, an Indian lease number, itself, may be released if requested.

(3) Federal Leases. All production and royalty data/information at the lease level on Federal leases is not considered proprietary and may be released if requested. The release of this data/information is accomplished by the ALE-303R (microfiche) report that contains accumulated production and royalty information by lease number for Federal leases.

(4) Division Orders (Onshore). Division orders reveal the name of the payor, share of production, and royalty rates. Such data/information is considered proprietary and may not be released.

(5) Sales Contracts/Purchase Agreements. Generally, sales contracts/purchase agreements are not released due to the large volume of proprietary data/information contained in such documents. Data/information which reveals the marketing strategy of the industry source, price of gas, reimbursable considerations, etc., is considered proprietary.

3. Proprietary Records Subject to an FOIA Request. In accordance with the MMSM 316.1, Freedom of Information Act (FOIA), when proprietary records are subject to an FOIA request, particular

2A3 40303

facts and circumstances will be examined by the MMS employee responsible for the FOIA action. A determination will be made if records or portions of records are exempt or if applicable exemptions are mandatory or discretionary. When a discretionary determination is made, the decision to withhold information should be exercised.

A. Exempt Information.

(1) The Indian Mineral Development Act of 1982 (25 U.S.C. 2103(c)).

(2) MMS, Department of the Interior, 30 CFR Chapter 2.

(3) OCS Order No. 12, Public Inspection of Records.

B. FOIA Exemptions. The FOIA lists nine categories of information which are exempt from disclosure. Exemptions 4 and 9 are particularly applicable to proprietary data/information received in the MMS.

(1) Exemption 4. Trade secrets and commercial or financial information obtained from a person and privileged or confidential.

(a) Trade Secrets generally are developed as a result of major financial investments by the industry source and are considered assets. In the mineral industry, trade secrets are often special processes, mineral development and recovery techniques, special engineering designs, etc. Trade secrets generally are considered to give an industry source a competitive advantage.

(b) Commercial Information regarding an industry source's future plans, organization stability, or other information which a competitor could use to gain an advantage, and information as to what public and Indian land is of interest to the industry source, development costs, production records for Indian lands, etc.

(c) Financial Data concerning an industry source's production costs, royalty payments, smelter returns, or contract/lease terms. This information can be used by the competition to determine organizational solvency or production rates of a well or mine. The production rates/volumes of an organization can be used by a competitor to determine how much to bid on an adjacent tract.

2B240303

(2) Exemption 9. Geological and geophysical information and data, including maps concerning wells. These are data from which the mineral characteristics of a particular area are determined. Many private sector organizations maintain large staffs for the gathering of the data as they require expensive equipment and highly skilled technicians and professionals to gather. Therefore, the release of such data would jeopardize the ability of the industry source to profit from its collection if a competitor gains information from the data without paying for it. Large skilled staffs are maintained to gather the data at great expense.

2B340303

TITLE 43 UNITED STATES CODE, SECTION 1350
OUTER CONTINENTAL SHELF LANDS ACT
REMEDIES AND PENALTIES

(a) Injunctions, restraining orders, etc.

At the request of the Secretary, the Secretary of the Army, or the Secretary of the Department in which the Coast Guard is operating, the Attorney General or a United States attorney shall institute a civil action in the district court of the United States for the district in which the affected operation is located for a temporary restraining order, injunction, or other appropriate remedy to enforce any provision of this subchapter, any regulation or order issued under this subchapter, or any term of a lease, license, or permit issued pursuant to this subchapter.

(b) Civil penalties, hearing

If any person fails to comply with any provision of this subchapter, or any term of a lease, license, or permit issued pursuant to this subchapter, or any regulation or order issued under this subchapter, after notice of such failure and expiration of any reasonable period allowed for corrective action, such person shall be liable for a civil penalty of not more than $10,000 for each day of the continuance of such failure. The Secretary may assess, collect, and compromise any such penalty. No penalty shall be assessed until the person charged with a violation has been given an opportunity for a hearing.

(c) Criminal penalties

Any person who knowingly and willfully (1) violates any provision of this subchapter, any term of a lease, license, or permit issued pursuant to this subchapter, or any regulation or order issued under the authority of this subchapter designed to protect health, safety, or the environment or conserve natural resources, (2) makes any false statement, representation, or certification in any application, record, report, or other document filed or required to be maintained under this subchapter, (3) falsifies, tampers with, or renders inaccurate any monitoring device or method of record required to be maintained under this subchapter, or (4) reveals any data or information required to be kept confidential by this subchapter shall, upon conviction, be punished by a fine of not more than $100,000, or by imprisonment for not more than 10 years, or both. Each day that a violation under clause (1) of this subsection continues, or each day that any

2A6 40303

monitoring device or information recorder remains inoperative or inaccurate because of any activity described in clause (3) of this subsection, shall constitute a separate violation.

(d) Liability of corporate officers and agents for violations by corporation

Whenever a corporation or other entity is subject to prosecution under subsection (c) of this section, any officer or agent of such corporation or entity who knowingly and willfully authorized, ordered, or carried out the proscribed activity shall be subject to the same fines or imprisonment, or both, as provided for under subsection (c) of this section.

(e) Concurrent and cumulative nature of penalties

The remedies and penalties prescribed in this subchapter shall be concurrent and cumulative and the exercise of one shall not preclude the exercise of the others. Further, the remedies and penalties prescribed in this subchapter shall be in addition to any other remedies and penalties afforded by any other law or regulation.

August 7, 1953, c. 345, § 24, as added Sept. 18, 1978, Pub. L. 95-372, title II, § 208, 92 Stat. 659.

2B740303

1. Purpose. This chapter establishes the marking standards and prescribes the procedures to ensure that proprietary data/information received or generated by the Minerals Management Service (MMS) is clearly marked.

2. Proprietary Data/Information Marking Standards.

A. "Proprietary--FOR U.S. GOVERNMENT USE ONLY." The marking "Proprietary--FOR U.S. GOVERNMENT USE ONLY" will be used to identify documents, in whole or in part, that contain or reveal proprietary information. The purpose of this marking is to alert the recipient to the sensitivity of the information involved and to indicate that it requires protection from unauthorized disclosure. Proprietary data/information received or generated by the MMS will be marked in the manner prescribed in paragraph 3.

(1) Information classified in the interest of national security only will be marked "Top Secret," "Secret," or "Confidential." The use of these markings for other than national security information is prohibited.

(2) Terms such as "Administrative," "Company," or "Proprietary" may not be used in conjunction with the national security classification designations (e.g., do not mark information as "Administrative Confidential," "Company Confidential," or "Proprietary Confidential").

(3) Proprietary material received in the MMS that is improperly marked should be remarked. Improperly marked file material should be remarked if it, or copy thereof, is transferred to another office or Agency.

B. Compilations of Information. A compilation of nonproprietary items of information normally should not be marked. However, certain nonproprietary information may require marking when combined or associated with other unrestricted information. In rare circumstances, the proprietary marking may be warranted if the combination of unrestricted items of information provides an added dimension that contains or reveals proprietary information. (For example, unrestricted documents that when combined would associate the royalty payments and/or production statistics with the payor/reporter's name.) In these rare circumstances, the procedures for marking proprietary information in paragraph 3 will be followed.

LEFT MARGIN

RIGHT MARGIN

2B6 40303

C. Reference Citations. The fact that a document makes reference to a proprietary document normally is not a basis for marking. However, if the reference citation, standing alone, reveals proprietary data/information, the marking procedures in paragraph 3 will be followed.

D. Extracts of Proprietary Information. A document generated by the MMS that contains unrestricted information extracted from a proprietary source document should not be marked. When proprietary data/information is extracted from a proprietary source document, the resulting document will be marked proprietary as described in paragraph 3 below.

3. Procedures for Marking Proprietary Data/Information. All proprietary data/information generated by the MMS or forwarded to the MMS from an industry source will be forwarded immediately to the appropriate Primary Office of Control for marking. The marking procedures are as follows:

A. Each page of a proprietary document will be marked "Proprietary--FOR U.S. GOVERNMENT USE ONLY" on the basis of the proprietary data/information it contains or reveals. Documents or pages of documents that contain both proprietary and nonproprietary items must be marked to clearly indicate which items are proprietary. This should be indicated in the text of the document itself or in a separate written statement that will be provided with the document.

LEFT MARGIN

RIGHT MARGIN

B. Documents other than paper should indicate the required marking on the material itself or, if that is not practical, in related or accompanying documentation.

C. Rolled documents and the packaging materials the documents are stored in are to be marked proprietary on both the document as well as the packaging material (e.g., seismic sections, well logs, tubes, etc.).

D. Automated proprietary data/information should be labelled both internally and externally (see MMS Manual (MMSM) 381.7).

4. Removal of Proprietary Marking. The marking "Proprietary--FOR U.S. GOVERNMENT USE ONLY" will be removed by the Primary Office of Control in the following instances:

A. In accordance with applicable laws and regulations or when the lease, license, permit, or contract terminates. The related data/information furnished to the MMS should have all

2A740303

restrictions removed because there are no further reasons to warrant its protection.

B. When the data/information is cleared for release by the industry source.

C. When the data/information is released by a State in accordance with State laws or regulations.

D. When a determination has been made that inadvertent or unauthorized disclosure has so compromised the information that removal of the proprietary marking is warranted (see MMSM 386.1.6C).

LEFT MARGIN

RIGHT MARGIN

2A8 40303

1. Purpose. This chapter establishes policy and sets forth the physical protection requirements for the storage and safekeeping of proprietary data/information.

2. Policy. It is the policy of the Minerals Management Service (MMS) to ensure that proprietary data/information is stored under conditions which will prevent unauthorized persons from gaining access to it.

3. Storage. Proprietary data/information will not be stored in a private residence, automobile, office, room, or in any other location not specifically authorized for proprietary storage.

A. Primary Office of Control. When not in use or in the protective custody of an authorized person, proprietary data/information will be stored in:

(1) Open Storage Room. An open storage room must meet the minimum construction standards contained in Appendix 1. Within an open storage room, proprietary material is maintained on shelves or in cabinets, some or none of which are approved General Services Administration (GSA) security containers. Knowledge of the combination or issuance of control cards affording access into the room shall be kept to an absolute minimum and be subjected to stringent controls. The primary entrance door combination or matrix will be changed when required in paragraph 4.

(2) Closed Storage Room. A closed storage room must meet the minimum construction standards contained in Appendix 1. Within a closed storage room, all proprietary data/information is stored in approved GSA security containers. An approved GSA security container is:

(a) A security filing cabinet, as outlined in the Federal Supply Schedule (FSC Group 71, Part XI); or in

(b) A steel filing cabinet fitted with a steel locking-bar device, secured by a three-position, dial-type, changeable combination padlock (Illustration 1). All keepers of the steel locking-bar device will be secured to the cabinet by bolts, rivets, or welding so that they cannot be removed and replaced without leaving evidence of entry. The locking-bar device must be installed to ensure that all drawers of the container are held securely so that their contents cannot be removed by forcing open the drawer(s). Combination padlocks

2B8 40303

will either be placed inside of the open container or secured to a hasp or handle of the container while it is open. Stringent key control and accountability are required for all door locks to room(s) containing a security container. Knowledge of the security container combination should be kept to an absolute minimum and be subjected to stringent controls. Combinations will be changed as required in paragraph 4.

B. Secondary Office of Control. When not in use or in the protective custody of an authorized person, proprietary data/information will be stored in the same manner as that authorized for the Primary Office of Control. If an open storage room or a closed storage room is not located in the same facility as a Secondary Office of Control, proprietary data/information will be stored in approved GSA security containers as required for a closed storage room in paragraph 3A(2). Stringent key control, accountability, and security container combinations are required as described in paragraph 3A(2). The requirements for changing security container combinations are described in paragraph 4.

C. Mailroom. At the time of receipt, all incoming/outgoing mail designated as proprietary must be secured in approved GSA storage containers (see MMS Manual (MMSM) 386.4.4E) until delivery.

4. Changing Combinations. Combinations will be changed at least once every 12 months and immediately under any of the following circumstances:

A. When the lock is initially put into use;

B. When an employee having knowledge of the combination is reassigned or terminates employment;

C. Upon knowledge or suspicion that the combination has become known to an unauthorized person or upon the discovery of an unlocked and unattended open storage room or open security container; or,

D. When the security container locking mechanism is taken out of service or returned to storage as a surplus item. Before taking security containers out of use, custodians must thoroughly inspect them to ensure all proprietary data/information has been removed and that the container is emptied before the standard combination is set. The combination to a security container will be changed to the manufacturer's original setting of 50-25-50. Combinations to security padlocks will be changed to 10-20-30.

2AS 40303

5. Safeguards. Employees using proprietary data/information or responsible for its custody must take every precaution to prevent deliberate or casual access to it by unauthorized persons.

A. Posting Within the MMS. Areas where proprietary data/information are stored or otherwise maintained will be posted with the proprietary data/information poster, which can be obtained from the General Services Branch (see Illustration 2).

B. Work Areas. A specific room, office, or area will be designated for the use of proprietary data/information after removal from an open or closed storage room or an approved security container. If the room or area is located on the ground level of the facility, all windows should be equipped with shades, venetian blinds, or drapes. Window coverings will be at least partially closed to deny inadvertent visual access during the working day when proprietary data/information is in use and exposed. Work areas are not authorized for the overnight storage of proprietary data/information. At the end of each working day, or when the material is not in actual use and may become physically unattended, it must be secured in the designated open or closed storage room or approved security container.

C. User Safeguards. Proprietary data/information must not be left in unoccupied rooms or be left inadequately protected in an occupied office, or an office occupied by other than authorized employees. When not safeguarded as required above, and when not in actual use by authorized personnel, proprietary data/information will be protected as follows:

(1) Kept under the constant surveillance of an authorized person who is in a physical location to exercise direct security controls over the material;

(2) Covered with a prescribed cover sheet, turned face down, placed in designated storage rooms or containers, or otherwise protected (e.g., positioning computer terminal screen away from visibility or clearing the screen) when unauthorized persons are present; or

(3) Returned to appropriate storage as soon as practicable after use.

D. Meetings and Conferences. In conducting meetings/conferences where proprietary data/information will be involved, every precaution will be taken to ensure that:

(1) In the interest of technical security, proprietary meetings are held on official premises;

2A/ 40303

(2) Proper physical security measures are implemented to provide protection for proprietary data/information equal to the measures required during normal operations;

(3) Participants are authorized access to proprietary data/information and have an established need-to-know; and

(4) Proper procedures for the release and transmittal of proprietary data/information are followed.

6. Physical Security.

A. Visitor Control. The administrative control of visitors is necessary to control/preclude freedom of entry/departure by all visitors and unauthorized personnel in proprietary storage and work areas during the normal workday when the data/information is in use and exposed.

(1) Primary Office of Control. A Visitor Control Station (VCS) will be established in a specific location of the facility. The location of the VCS is optional but, ideally, a VCS should be located in the vicinity of both storage and work areas. All visitors will be required to present some form of personal identification which includes a photograph of the bearer and to complete a register which reflects the visitor's name, Agency or firm represented, date and time of visit, purpose of visit, identity of sponsor, time of departure, and badge number.

(a) The use of a badge system is recommended; however, if work and storage areas are separate or in multiple locations, a badge system is mandatory to enhance security and possibly prevent inadvertent access by unauthorized persons. Badges should be numerically accountable. They may be color-coded to denote degree of access (e.g., work and storage areas, work area only, storage area only, or other specific degrees of access).

(b) The VCS must be manned continuously during the working day. The person manning the VCS and all other employees should be instructed to challenge all unauthorized persons attempting to enter either the storage or work areas.

(c) All employees and authorized visitors must be advised that all visitors are required to report to the VCS prior to being afforded access to either the storage or work areas. All visitors must report to the VCS prior to their departure from the facility. When visitors exit, they should be questioned to prevent their unauthorized removal of

LEFT MARGIN

RIGHT MARGIN

BOTTOM MARGIN

2B4 40303

proprietary data/information, they should record their time of departure on the register, and surrender their badges if a badge system is implemented.

(2) Secondary Office of Control. The establishment of a VCS is not mandatory. However, adequate controls and safeguards are required to preclude visitors and unauthorized persons:

(a) From entering work areas when proprietary data/information is in use and exposed; and

(b) To ensure that rooms in which security containers storing proprietary data/information are securely locked when not in use or are not under the supervision of an authorized employee.

B. Custodial/Maintenance Personnel.

(1) During working hours, custodial, janitorial, and maintenance personnel will be permitted into open or closed storage rooms or work areas only when in the company of authorized employees who can maintain continuous visual observation of their activities. All material must be adequately covered, protected, or secured within storage containers to preclude unauthorized visual access.

(2) After working hours, custodial, janitorial, and maintenance personnel will not be permitted into open/closed storage rooms. Procedures should be established to provide emergency access into storage rooms after working hours. There are no security restrictions governing access into work areas. Therefore, overnight storage of proprietary data/information is not authorized in these areas.

C. Establishing, Relocating, or Changing Proprietary Information Storage Facilities. Proprietary data/information security plans will be established and implemented for all planned and existing facilities which store and protect proprietary data/information. The procedures for establishing, relocating, or changing proprietary data/information storage facilities follow.

(1) Clearly determine the need to establish, relocate, or change existing storage facilities.

(2) Plan new facilities, relocation, or change in consultation with the MMS Security Officer and/or the servicing Administrative Service Center (ASC), General Services Branch,

28/ 40303

using the physical protection requirements contained in this chapter and the minimum construction standards contained in Appendix 1.

(3) A proprietary data/information security plan will be prepared (see MMSM 386.1.7A(3)) that includes:

(a) A narrative description of the planned facilities and the procedures that will be adopted to protect the proprietary data/information;

(b) A completed checklist-survey (Illustrations 3 and 6) of planned storage and work areas and the VCS;

(c) A floor plan or diagram that fully identifies the planned work and storage areas and the location of doors, windows, and the VCS; and

(d) When applicable, a narrative description of the plan for maintaining security during a change from old to new facilities is required. The description will include information about who will be present at the time of relocation and how the information will be transported.

(4) The completed proprietary data/information security plan will be submitted through the appropriate management official and the servicing ASC, General Services Branch, to the MMS Security Officer for review and approval.

(a) The appropriate management official will review the proprietary data/information security plan to ensure that facilities and procedures described therein are in compliance with this chapter and that resources required to fulfill the intent of the plan are available and appropriate.

(b) The MMS Security Officer will approve the proprietary data/information security plan or will return the plan with recommended changes. The proprietary data/information security plan will be returned to the initiating office through the servicing ASC, General Services Branch.

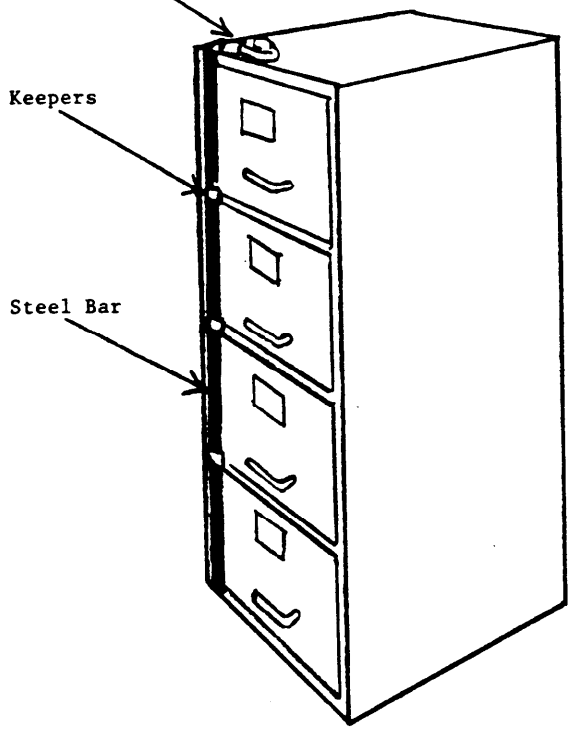
(5) Upon receipt of an approved plan, the responsible manager or supervisor will prepare requisition(s) reflecting recommended changes and submit them through normal channels.

(6) The MMS Security Officer will be notified through appropriate channels when construction is completed.

LOTTOV

2AA 40303

APPROVED STEEL FILING CABINET



Typical steel filing cabinet fitted with a locking-bar device

3A3 40303

N O T I C E

1. Access to records maintained in this area is limited to authorized individuals only.

2. Unauthorized disclosure is subject to penalties provided in 43 U.S.C. 1331 et seq., and/or 30 U.S.C. 1701 et seq.

303 40303

CHECKLIST--Survey of Sensitive Proprietary "Open" Storage Room(s)

If determined that the quality and/or dimensions of proprietary data/information cannot be adequately maintained in approved security containers, within a "closed" storage room, and as a result, establishment of an "open" storage room is required, define each room separately using the following format. Reflect the location and pertinent remarks for each room on an attached floor plan/diagram.

Facility: _____

Date of Survey: _____ Conducted by: _____

Room Number: _____ Floor Level: _____

Floor Construction:

- Concrete slab ____
- Wood ____
- Other (define) _____

Wall Construction:

- Dry wall ____
- Cinder block ____
- Brick ____
- Extended floor to floor ____
- Reinforced with steel mesh ____
- Other (define) _____

Ceiling Construction:

- Concrete slab ____
- Dry wall ____
- Acoustic tile ____
- False ceiling (removable tiles) ____
- Reinforced with steel mesh ____
- Other (define) _____

Windows:

- Total number ____
- Number barred ____
- Number with steel mesh grill ____
- Number alarmed ____
- Number with blinds, shades, drapes ____

Door Construction (Primary entrance):

- Solid wood ____
- Hollow-core wood ____
- Metal-clad wood ____
- Metal fire-rated ____
- With glass panels ____
- Other (define) _____

Door Construction (Alternate doors):

- Number solid wood ____
- Number hollow-core wood ____
- Number metal-clad wood ____
- Number metal fire-rated ____
- Number with glass panels ____
- Other (define) _____

Door Locking Device (Primary entrance):

- Built-in combination with escape mechanism ____
- Cypher with fail-safe ____
- Card operated access with fail-safe ____
- Dead-bolt lock ____
- Spring-loaded lock ____
- Padlock ____
- Other (define) _____

3D340303

Door Locking Service (Alternate doors):

Number dead-bolt devices fitted on inside of doors _____
Number bar devices on inside of doors _____
Number dead-bolt locks _____
Number spring-loaded locks _____
Other (define) _____

Magnetic Contact Alarm (Primary entrance door):

Yes _____
No _____

Magnetic Contact Alarms (Alternate doors):

Yes _____
No _____
Number of doors equipped _____

Door Hinges (Primary and alternate doors):

Hidden (not exposed) _____
Exposed from inside _____
Exposed from outside _____
Pins/bolts welded _____
Pins/bolts peened _____
Other (define) _____

Vents/Openings in Walls, Floor, and Ceiling (less than 90 square inches):

Total number _____
Number air-conditioning _____
Number heating _____
Number combined heating and air-conditioning _____
Number utility _____
Other (define) _____

Vents/Openings in Walls, Floor, and Ceiling (90 square inches or larger):

Total number _____
Number air-conditioning _____
Number heating _____
Number combined heating and air-conditioning _____
Number utility _____
Other (define) _____

Vents/Openings (90 square inches or larger):

Number alarmed _____
Number fitted with bars _____
Number fitted with steel mesh grills _____

Volumetric Room Alarm (ultrasonic/acoustic/motion detection):

Yes _____
No _____

Alarm Monitoring System (doors, windows, vents/openings, volumetric):

Define: _____

3C240303

Custodial/Maintenance Access:

During working hours ____
After working hours ____

Describe frequency of access and office security controls: ___

Remarks:

3B340303

CHECKLIST--Survey of Sensitive Proprietary "Closed" Storage Room(s)

If determined that the quantity and/or dimensions of proprietary data/information do not require establishment of an "open" storage room and can be adequately maintained in approved security containers, within a "closed" storage room, define each room separately using the following format. Reflect the location and pertinent remarks for each room on an attached floor plan/diagram.

Facility: _____
Date of Survey: _____ Conducted by: _____
Room Number: _____ Floor Level: _____

Floor Construction:

Concrete slab ____
Wood ____
Other (define) _____

Wall Construction:

Dry wall ____
Cinder block ____
Brick ____
Extended floor to floor ____
Reinforced with steel mesh ____
Other (define) _____

Ceiling Construction:

Concrete slab ____
Dry wall ____
Acoustic tile ____
False ceiling (removable tiles) ____
Reinforced with steel mesh ____
Other (define) _____

Windows:

Total number ____
Number barred ____
Number with steel mesh grill ____
Number alarmed ____
Number with blinds, shades, drapes ____

Door Construction:

Number solid wood ____
Number hollow-core wood ____
Number metal-clad wood ____
Number metal fire-rated ____
Number with glass panels ____
Other (define) _____

Door Locking Devices:

Number with dead bolt locks ____
Number with spring-loaded locks ____
Other (define) _____

Door Hinges:

Hidden (not exposed) ____
Exposed from inside ____
Exposed from outside ____
Pins/bolts welded ____
Pins/bolts peened ____
Other (define) _____

Alarm System (if employed)

Define _____

Vents/Openings (90 square inches or larger):

Number ____

3A6 40303

Type of Security Containers:	Custodial/Maintenance Access:
Number of GSA approved security filing cabinets (FSC Group 71, Part XI) ____ Number of steel filing cabinets fitted with steel locking-bar devices ____ Other (define) _____	During working hours ____ After working hours ____ Describe frequency of access and office security controls _____

Remarks:

3B740303

CHECKLIST--Survey of Sensitive Proprietary Work Area(s) (Non-Storage)

Define each room/area separately using the following format. Reflect the location and pertinent remarks for each room/area on an attached floor plan/diagram.

Facility: _____
Date of Survey: _____ Conducted by: _____
Room/Area Number/ID: _____ Floor Level: _____

Floors, Walls, Ceiling (Vents and openings 90 square inches or greater), and Doors:

Briefly describe the construction standards _____

Doors:

Total number for each room designated as a work room, or number of perimeter doors for a suite of joined offices which are designated as a work area. ____

Door Locking Devices:

Number with dead bolt locks ____
Number with spring-loaded locks ____
Other (define) _____

Door Hinges:

Hidden (not exposed) ____
Exposed from inside ____
Exposed from outside ____
Pins/bolts welded ____
Pins/bolts peened ____
Other (define) _____

Windows:

Total number ____
Number fitted with blinds, shades, or drapes ____

Alarm System (if employed):

Define _____

Custodial/Maintenance Access:

During working hours ____
After working hours ____
Describe frequency of access and office security controls _____

Remarks should be shown on reverse.

3C640303

CHECKLIST--Survey of Visitor Control Station

Define each control station separately using the following format. Reflect the location and pertinent remarks for each control station on an attached floor plan/diagram.

Facility: _____
Date of Survey: _____ Conducted by: _____
Room/Area Number/ID: _____ Floor Level: _____

Location:

Define _____

Manned Continuously During the Working Day:

Yes ____
No ____

Positive Identification of Visitor Required:

Yes ____
No ____

Administratively Control Access to all Storage and Work Areas:

Yes ____
No ____

Register System (Sign-in/out):

Yes ____
No ____

Badge System:

Yes ____
No ____
If employed, describe _____

Exit Procedures:

Are all visitors questioned, prior to their departure from the facility to preclude/ prevent their unauthorized removal of sensitive proprietary data/information?

Yes ____
No ____
Remarks: _____

3D6 40303

MINIMUM CONSTRUCTION STANDARDS FOR OPEN STORAGE ROOMS AND CLOSED STORAGE ROOMS

1. Open Storage Room Construction Standards. Within an open storage room, all proprietary data/information is maintained on open shelves or in cabinets, some or none of which are approved GSA security containers.

A. Floor. The GSA building standard for floor construction is acceptable.

B. Walls and Ceiling.

(1) The GSA building standard for wall construction is acceptable providing that the walls are constructed of typical dry wall materials, cinder block, or common building brick. Wall construction may be further enhanced by installation of No. 9-11 gauge expanded metal with diamond shaped mesh openings of 1 to 1 1/4 inches if the local civil community experiences a high crime rate or the designated room is highly vulnerable to entry.

(2) The ceiling must be constructed of materials to preclude entry (e.g., concrete slab, dry wall materials, or nonremovable tiles or panels). If the designated room has a false ceiling (e.g., removable panels suspended on metal frames), the false ceiling must be replaced by suitable materials to preclude entry or the walls must be extended slab-to-slab (floor-to-floor). The walls may be extended by use of dry wall materials.

C. Windows. Windows are not authorized in the construction of new open storage rooms. All windows in existing open storage rooms will be equipped with shades, venetian blinds, or drapes which will be closed at all times to preclude visual access. All windows located below the third level will be barred, fitted with a steel mesh grill, or alarmed.

D. Doors and Door Hardware.

(1) All doors must be metal firerated doors, solid wood doors, or metal clad hollow-core wood doors. Normally, all door hinges are exposed only from within the room. If hinges are exposed from the exterior surface of the door, they must be mounted to preclude easy removal (e.g., bolted through the door and frame). All exterior bolts must be peened or spot-welded to preclude their easy removal.

3B6 40303

(2) The primary entrance door must be fitted with a built-in, three position, GSA-approved dial-type combination lock having an inside escape mechanism, a card operated access control system having fail-safe characteristics, or other cypher-type locks having fail-safe characteristics. Fail-safe means that if the power source fails, the locking mechanism remains locked. All other doors must be fitted with a manual dead-bolt device with at least a 1-inch bolt which is mounted on the inside surface of the door to preclude exterior access.

E. Alarm Systems. All perimeter doors should be fitted with magnetic contact alarm devices. A motion detection alarm device should be installed within the room to denote unauthorized intrusion when the room is locked and unattended. All alarm devices must be linked to a monitoring control station or location having personnel capable of responding to the alarm. The alarm system also may be connected to a local alarm on the exterior perimeter of the building to provide dual protection.

F. Smoke and Fire Detection. There are no security requirements for smoke or fire detection devices.

2. Closed Storage Room Construction Standards. Within a closed storage room, all proprietary data/information is secured in approved GSA security containers. The GSA construction standards for floors, walls, ceilings, vents and openings, and doors are adequate.

A. Windows. All windows in a closed storage room will be equipped with shades, venetian blinds, or drapes which will be closed at all times to preclude visual access.

B. Door and Door Hardware. All door hangers and bolts should be exposed only from within the room. If hangers are exposed from the exterior surface of the door, they must be mounted to preclude easy removal (e.g., bolted through the door and frame). All exterior exposed bolts must be peened or spot-welded to preclude their easy removal. All doors and rooms containing approved GSA security containers will be fitted with key-operated, dead-bolt locks. Dead-bolt locks will have at least a 1-inch bolt.

3A7 40303

1. Purpose. This chapter establishes policy, sets forth standards for access, and prescribes procedures for release and transmittal of proprietary data/information.

2. Policy. It is the policy of the Minerals Management Service (MMS) to ensure that offices and individuals provided access to proprietary data/information have an established need-to-know and that positive security control measures are maintained over the use, transmittal, and disposition of the proprietary data/information entrusted to them. The use of receipts and security agreements is prescribed to ensure that accountability and security control is maintained when access to proprietary data/information is authorized.

3. Standards for Access.

A. Primary Office of Control. The Primary Office of Control has the ultimate authority regarding the duplication and release of proprietary data/information to requesting individuals. The decision to release or duplicate proprietary data/information must be based on a justified need-to-know (see MMS Manual (MMSM) 386.1, Appendix 1). Essential to the determination of a need-to-know is the purpose for which access is requested and the intended use of the proprietary data/information. All disclosure standards and protection requirements must be adhered to in accordance with MMSM 386.3. The Primary Office of Control also has the authority to grant limited duplication and release authority to the Secondary Office of Control.

B. Secondary Offices of Control. Any office to which proprietary data/information is transmitted must be designated as a Secondary Office of Control. Secondary Offices of Control must adhere to the same disclosure standards as the Primary Office of Control and to the protection requirements contained in MMSM 386.3. The Secondary Office of Control must be granted duplication and/or release authority by the Primary Office of Control prior to taking such activity. Originals and all copies of proprietary data/information will be returned promptly to the Primary Office of Control after having served their purpose.

C. Proprietary Data/Information Receipt. A Proprietary Data/Information Receipt is required when proprietary data/information is transmitted to a requesting individual or when data/information is made available for review at an MMS facility. For a sample Proprietary Data/Information Receipt and suggested format see Illustration 1.

LEFT MARGIN
RIGHT MARGIN
BOTTOM MARGIN
3A8 40303
FORM MMS 2000

D. Data/Information Security Agreement. A Data/Information Security Agreement must be completed by an authorized official of a requesting office when a request for proprietary data/information is received from an office outside of the MMS. This document is a prerelease agreement that informs the prospective recipient of the restrictions and controls required for the protection of proprietary data/information and provides the MMS assurance that the requested information will be safeguarded from unauthorized disclosure. If an authorized official is not willing to sign this document, the requestor will be referred to the Assistant Secretary - Land and Minerals Management (see paragraph 5F for procedures). A sample Data/Information Security Agreement and suggested format to be used for such requests, with the exception of the General Accounting Office (GAO), is described in Illustration 2. A sample Data/Information Security Agreement for the GAO is described in Illustration 3.

E. Cover Sheet. A protective document cover sheet (Illustration 4) will be applied to all documents when removed from storage for any reason; i.e., for release, transmittal, or to work areas. Cover sheets can be obtained from the General Services Branch.

4. Procedures for In-house Release and Transmittal. The Primary Office of Control will adhere to the following procedures when a request for proprietary data/information is received from individuals within the MMS.

A. Review Documents for Marking and Decontrol Purposes. When a need-to-know has been established, the documents to be released will be reviewed to ensure that:

(1) Proprietary markings are removed from data/information which no longer requires protection in accordance with MMSM 386.2.4,

(2) Each page of the proprietary data/information to be released is numbered and properly marked in accordance with MMSM 386.2.3, and

(3) Proprietary items are clearly marked in documents containing both proprietary and nonproprietary data/information in accordance with MMSM 386.2.

B. Attach Cover Sheet. Attach the cover sheet to the face of the document to be reviewed or released. When the document is not flat or regular sized, attach the cover sheet so that it will remain visible.

LEFT MARGIN
RIGHT MARGIN
BOTTOM MARGIN
3B540303
FORM MMS 2000

C. Preparation of a Proprietary Data/Information Receipt (Illustration 1).

(1) When proprietary data/information is to be transmitted, one original and two copies of the Proprietary Data/Information Receipt will be prepared. The original and one copy will be attached to the proprietary data/information to be transmitted to the requesting office. The third copy will be retained in a suspense file in the Primary Office of Control. The suspense file copy will be destroyed upon receipt of a signed original. Followup action will be required if the signed original receipt is not returned within 15 days after transmittal.

(2) When proprietary data/information is to be reviewed in an MMS facility, an original and one copy of the Proprietary Data/Information Receipt will be prepared. The authorized recipient will sign the receipt at the conclusion of the review. The signed original will be retained in the Primary Office of Control. The second copy should be retained by the reviewing official.

LEFT MARGIN

RIGHT MARGIN

(3) When proprietary data/information is released directly to an official of a requesting office, a Proprietary Data/Information Receipt will be prepared as required in paragraph 4C(2) and the data/information will be wrapped as required in paragraph 4E.

D. Positive Identification of Authorized Recipient. When proprietary data/information is to be reviewed in an MMS facility or is released directly to an authorized recipient, the requestor must produce positive identification before the proprietary data/information is released. Positive identification should include a photograph of the bearer (e.g., driver's license or DOI identification card).

E. Wrapping and Addressing Proprietary Data/Information for Transmittal.

(1) When proprietary data/information is to be released directly to the authorized official, the proprietary data/information will be placed in a blue "SPECIAL ATTENTION" envelope. The blue envelope must reflect an address and return address. The envelope must be sealed and marked, front and back, "TO BE OPENED BY ADDRESSEE ONLY." An outer manila envelope or manila packaging will conceal the inner blue envelope. Rolled maps or charts may be placed in tubes marked "FOR PERSONAL ATTENTION." The Proprietary Data/Information Receipt will be attached to the outer wrapping.

BOTTOM MARGIN

308 40303

(2) When proprietary data/information is to be transmitted by other approved means, the proprietary data/information and the Proprietary Data/Information Receipt will be placed in a blue "SPECIAL ATTENTION" envelope. The blue envelope must reflect an address and return address. The envelope must be sealed and marked "TO BE OPENED BY ADDRESSEE ONLY" on the back and front. An outer manila envelope or manila packaging will conceal the inner blue envelope. The outer wrapping will reflect the complete address of the recipient and the complete address of the transmitting office. Rolled maps or charts can be placed in tubes marked "FOR PERSONAL ATTENTION." A green sticker will be placed on the front of the outer wrapping, envelope, tube, etc. Green stickers may be obtained from appropriate Administrative Service Centers. The green sticker will alert mailroom personnel that the information is proprietary and requires special storage and handling. The package will be handcarried to and from the mailroom.

F. Approved Methods for Transmittal. Proprietary data/information must be transmitted by one of the following methods:

(1) Handcarried by authorized MMS personnel and delivered only to the official authorized to receive the package. Positive identification is required before the proprietary data/information is released;

(2) Transmitted by authorized courier service (i.e., DHL or Federal Express); or

(3) U.S. Postal Service--Registered Mail, return postal receipt required.

5. Procedures for Release to Offices or Individuals Outside the MMS. When a request for proprietary data/information is received from an office or individual outside the MMS, the Primary Office of Control will adhere to the following procedures.

A. Bureaus or Offices Within the DOI. Arrange to have an authorized official of the Bureau or office complete, sign, and return a Data/Information Security Agreement (see Illustration 2). Upon return of the signed agreement, see procedures for in-house release and transmittal (see MMSM 386.4.4).

B. Federal Agencies Outside of the DOI. All Federal Government Agencies outside of the DOI must make a written request to the DOI through the Assistant Secretary - Land and Minerals Management for access to proprietary data/information.

LEFT MARGIN RIGHT MARGIN BOTTOM MARGIN

3DS 40303

FORM MMS 2000

1. Purpose. This chapter establishes the Minerals Management Service (MMS) standards for reproduction and destruction of proprietary data/information.

2. Standards for Reproducing Proprietary Data/Information. The following criteria apply to the reproduction of proprietary data/information. If a copy of such information is authorized to be made and retained, a copy of the Proprietary Data/Information Sheet, required by MMS Manual (MMSM) 386.4.4C, will be made and placed on the retained copy.

A. Controls. Reproduced copies of proprietary data/information:

(1) Are subject to the same accountability and controls as the original documents and will be marked as originals.

(2) Should be discouraged and kept to the absolute minimum necessary to meet operational requirements.

(3) Will be made by the Primary Office of Control except as provided in MMSM 386.4.5E. If making the copies would be a major effort, the requesting office will make copies in the Primary Office of Control.

B. Reproduction Equipment.

(1) Reproductions of proprietary data/information must be controlled to ensure that the data/information is properly safeguarded. Reproductions of proprietary data/information must be made only on equipment specifically designated for the reproduction of such material. The majority of copying machines at a given facility should be posted with the following notice:

"REPRODUCTION OF CLASSIFIED OR PROPRIETARY INFORMATION ON THIS MACHINE IS PROHIBITED."

(2) A limited number of machines per location should be approved for the reproduction of classified or proprietary data/information. These machines should be under the supervision of Proprietary Officers. Approved machines are to be posted with the following notice:

"REPRODUCTION OF CLASSIFIED OR PROPRIETARY INFORMATION ON THIS MACHINE IS PROHIBITED WITHOUT THE APPROVAL OF (title of the Proprietary Officer)."

3B1 40303

C. After copies of proprietary data/information are made, the following actions must be taken:

(1) Reproduction equipment will be cleared of proprietary data/information immediately following copying and checked to ensure that no sensitive material remains in the mechanism.

(2) Following the last item copied, several plain sheets should be run through the machine to ensure that a latent image is not retained.

3. Standards for Destroying Proprietary Information. Proprietary data/information, when eligible, will be destroyed beyond recognition so as to preclude reconstruction of the proprietary data/information in whole or in part. Destruction may be accomplished by burning, melting, mutilating, or chemically decompositioning. In addition, pulping, disintegrating, pulverizing, or shredding may be used for the destruction of paper products. The following additional requirements pertain to destruction.

LEFT MARGIN

RIGHT MARGIN

A. Proprietary data/information will be destroyed in accordance with record requirements as established in the Records Management Handbook, MMSM 380.2-H.

B. If proprietary data/information is removed from the facility for destruction, it must be destroyed on the same day it is removed.

C. Proprietary data/information will be destroyed only by authorized individuals who will safeguard the material entrusted to them until it is destroyed.

D. Drafts, working papers, etc., containing proprietary data/information will be destroyed in accordance with the above standards.

E. Automated proprietary data/information other than printouts will be erased from the system.

BOTTOM MARGIN

3A4 40303Imp.

FORM MMS 2000