Minerals Management Service
Interim Policy Document

Effective Date: November 2, 2007 **IPD No. 08-01**
Series: Administrative
Part: 386
Title: Safeguarding and Protection of Proprietary and Business Confidential Information

Originating Office: Information Management Division, Administration and Budget

1. Purpose. To establish policy and guidance regarding the protection and safeguarding of Proprietary and Business Confidential Information. This Interim Policy Document (IPD) establishes the requirement that every employee of MMS understand their obligation to - and compliance with - the requirements set forth in the governance of Proprietary and Business Confidential Information as defined by the Department and MMS.

2. Scope. This IPD shall apply to all permanent, temporary and part-time employees and contractors who access proprietary and business confidential information – regardless of media format. All users shall be aware of their responsibilities, acknowledge their actions, and comply with these requirements. Media formats include, but are not limited to, paper records, electronically stored information, computer equipment, software, operating systems, storage media, and network accounts providing electronic mail and web browsing.

3. Objective. To provide an interim policy to MMS employees regarding the handling of proprietary and business confidential information while MMS Directives and governance are reviewed and updated to meet and clarify employee relevant obligations and requirements.

4. Authority.

A. Minerals Management Service Manual Chapter 386

B. Minerals Management Service IT Rules of Behavior

C. OMB Circular A-130

D. Departmental Manual (DM) 375, Chapter 19

5. Definitions.

A. Proprietary information/data are trade secrets and commercial or financial information provided by the government from a company or a private individual on a privileged or confidential basis that, if released, would result in competitive harm to the company or private individual, or impair the government's ability to obtain like information in the future. This proprietary information/data is furnished by industry in compliance with the terms of leases, permits, regulations, or contracts. Proprietary information/data means information, knowledge, or data of an intellectual, business,

technical, scientific or industrial nature in which the submitter claims a proprietary or ownership interest, or has a legal or contractual duty to protect. Proprietary information/data is contained in media-neutral forms, i.e., paper, electronic forms, databases, files, audio and video files, etc.

B. Information may be identified as "business-confidential" if (1) a person having the information may derive an economic benefit from it or obtain a competitive advantage over those who do not have it, (2) the information is not generally known or publicly available from other sources, and (3) the owner of the information has not previously made it available without imposing in a timely manner an obligation to keep it confidential.

6. Policy. It is the policy of the Minerals Management Service (MMS) to ensure that offices and individuals provided access to proprietary, sensitive or business confidential information are obligated to fully understand their legal and ethical responsibilities regarding the safeguarding and protective handling of such information - that they have an established need-to-know, and, that positive security control measures are maintained over information entrusted to them.

7. Responsibilities.

A. Associate Directors are responsible for ensuring that MMS employees and contractors under their direction, who handle proprietary information/data, adhere to the requirements of this Interim Policy Document.

B. Associate Director for Administration and Budget is responsible for developing and directing the MMS security program and designating a Bureau Security Officer.

C. Bureau Security Officer carries out the responsibilities of the Associate Director for Administration and Budget for implementing the security program and for:

(1) Developing security policies, standards and procedures.

(2) Inspecting MMS and MMS contractor proprietary information/data security facilities.

(3) Providing guidance and assistance to MMS personnel.

(4) Determining the suitability of employees for public trust and non-sensitive positions who access proprietary information/data in accordance with established law, regulation, and rule.

D. Supervisors are responsible for:

(1) Ensuring that proprietary information/data received by or released from MMS is safeguarded.

(2) Ensuring that all positions under their supervision are properly designated in terms of program placement and position sensitivity/risk levels.

(3) Ensuring that employees/contractors meet the "need-to-know" requirement for access to proprietary information/data. "Need-to-know" access is limited to those MMS officers, employees or contractors who have a need for the record in the performance of their official duties and/or when access is required to discharge an employee's official duties.

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

(5) Ensuring that subordinates are aware of applicable penalties as stipulated by Federal Regulations and laws for unauthorized disclosure of proprietary information/data (43 U.S.C. 1360 and 18 U.S.C. 1905).

E. Individual Bureau Employees are responsible for safeguarding proprietary information/data in their physical custody and for handling such material in accordance with 375 DM 19.

8. Cancellation. This IPD will remain in effect until incorporated into the MMS Manual or until no longer needed.

Robert E. Brown
Associate Director for
Administration and Budget