Minerals Management Service
Interim Policy Document

IPD No: 06-01

Effective Date: October 20, 2005
Title: Protection of Data from Unauthorized Access and Enforcement of Data Validation
Originating Office: Information Technology Division, Offshore Minerals Management (OMM)

1. Purpose. This IPD establishes policy and guidelines for the protection of OMM data from unauthorized access, supports the enforcement of business rules for data validation and integrity assurance, and limits the writing and edit/update capability to the Enterprise Master Data Store to authorized methods and technology mechanisms.

2. Objectives. The objectives of this IPD are to:

A. Establish a framework for mitigating data and system risks by managing methods and technology mechanisms that could allow writing, updating, or deleting data in the Enterprise Master Data Store.

B. Facilitate the consistent application of business rules for processing, validating, and verifying writing, editing and updating from all possible sources.

3. Scope. This IPD applies to all OMM employees, contractors, vendors, agents, and any users of OMM systems accessing corporate data stores. It is intended for all users of OMM systems.

4. Authority.

A. Federal Information Security Management Act (FISMA) of 2002 (Public Law 107-347, Title 111).

B. OMB Circular A-130.

FISMA, defines 'information security' as: "(1)…protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide – integrity, which means guarding against improper information, modification, or destruction, and includes ensuring information non-repudiation and authenticity;…"

OMB Circular A-130, states: "Agencies will: (g) protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information;..."

5. Definitions.

A. Data Access involves the authorization of system users to view data, including sensitive and proprietary information, in addition to the rights to write, update, and delete instances of data in the corporate data store.

B. Data Stakeholders are OMM designated Data Stewards or the entity (person or office) responsible for the integrity of specific data sets.

C. Enterprise Master Data Store consists of structured and unstructured data repositories as designated by OMM to be corporate data assets and managed accordingly.

D. Structured Data is data that resides in fixed fields within a record or file. Relational databases and spreadsheets are examples.

E. Unstructured Data is data that does not reside in fixed locations within a record or file. Free-form text in a word processing document is a typical example. This IPD is addressing unstructured data that resides in one or more OMM IT systems such as OCS-Connect.

6. Policy. Consistent with Federal security mandates, it is the policy of OMM to:

A. Protect all OMM enterprise data and information.

B. Restrict access to data and information to authorized individuals only.

C. Restrict the capabilities to write, update, and delete data in the Enterprise Master Data Store to methods and technology mechanisms for which prior approval has been granted. By default, write/update/delete capabilities will be limited to methods provided by the system housing the data. For example, unless prior approval has been granted, only OCS Connect applications specifically selected or designed for the purpose of maintaining specific data sets will be used to insert, update, or delete those respective OCS Connect data sets.

D. Analyze access methods based on standards and impact to the system, resources (i.e. support, maintenance, life cycle), security, data, and other appropriate areas.

E. Use standard application methods wherever possible. Exceptions to the standards will be kept to a minimum.

7. Responsibilities.

A. MMS Employees, Contractors, Vendors, Agents, and other Internal Customers will:

(1) Request in writing, through established MMS security procedures, approval of their

appropriate level of data access.

(2) Utilize only the MMS systems and/or approved mechanisms for writing, editing or updating enterprise data. This includes alternative mechanisms approved as described below.

(3) Request exceptions according to the procedures below for alternative mechanisms to be used for writing, editing, and updating enterprise data if required to meet business requirements.

B. The ITD will:

(1) In coordination with OMM management and appropriate data stakeholders, designate and publish authorized methods and software for the writing, editing or updating of data in the OMM enterprise master data store.

(2) Working with OMM offices, analyze requirements and assist in the documentation and preparation of exception requests, where necessary, to be submitted for OMM Management consideration. This assistance will include analysis of system/data quality impacts of the proposed exception and, if necessary, mitigation recommendations designed to limit impacts.

(3) Approve requests with no significant impacts.

(4) Forward requests involving significant system/data impacts to the Chairman of the IMC, together with ITD recommendations regarding system/data quality impacts and potential mitigations of those impacts. Mitigations can include a recommendation to deny the request.

C. The OMM Information Management Committee (IMC) Chairman will approve or disapprove exception requests submitted through the ITD.

8. Procedures.

A. Offices requesting use of non-standard/alternative data write, update, or delete technologies (software) will contact the ITD New Orleans office with specifics of the requested technologies/software, methods of use, and data to be accessed.

B. ITD will analyze the request for potential data, system, resource, security, and other appropriate impacts. If no significant impacts are identified then ITD will approve the non-standard/alternative use.

C. If significant impacts are identified, then ITD will, if desired by the requesting office, assist in preparing an exception for evaluation by the IMC Chairman. It will contain a description of potential system/data quality impacts and recommendations for mitigating these impacts.

D. The ITD will submit the request to the IMC Chairman for a decision.

9. Effective Dates. This IPD will become effective immediately upon adoption. However, data access methods currently in use within OMM for legitimate business purposes will remain tentatively approved until the IMC determines requirements for currently existing uses.

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

Thomas A. Readinger
Associate Director,
Offshore Minerals Management