DEPARTMENT OF THE INTERIOR
MINERALS MANAGEMENT SERVICE MANUAL

TRANSMITTAL SHEET

Release No. 312

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

EXPLANATION OF MATERIAL TRANSMITTED:

This manual chapter prescribes policies, procedures, and responsibilities for the implementation and management of the IT security program within the MMS.

Director

FILING INSTRUCTIONS:

REMOVE:				INSERT:			
Part	Chapter	Pages	Release	Part	Chapter	Pages	Release
375	19	10	295	375	19	10	312

OPR: Information Management Division
Office of Administration and Budget
Date: August 18, 2008

Minerals Management Service
Minerals Management Service Manual

Effective Date: August 18, 2008
Release No.: 312
Series: Administrative
Part 375: Information Management Program
Chapter 19: Information Technology (IT) Security Program

Originating Office: Information Management Division

1. **Purpose.** This chapter prescribes policies, procedures, and responsibilities for the implementation and management of the IT security program within the Minerals Management Service (MMS).

2. **Objective.** The MMS IT security program is designed to protect the confidentiality, integrity, and availability of all IT resources owned by or operated on behalf of the MMS. To meet this objective, the MMS will maintain a level of IT security commensurate with the risks associated with its IT resources while complying with Federal and Department of the Interior (DOI) laws, regulations, and guidance.

3. **Authority.**

A. 118 DM 2 MMS Organization Structure, September 22, 2006

B. 375 DM 19 IT Security Program April 15, 2002

C. DOI Policies on Limited Use of Government Equipment and Telephone Use, June 14, 2000

D. Presidential Decision Directive 63, "Protecting America's Critical Infrastructures," May 22, 1998

E. Office of Management and Budget (OMB) Memorandum 00-07, Incorporating and Funding Security Information Systems Investments, February 28, 2000

F. OMB Memorandum 99-20, Security of Federal Automated Information Resources, June 23, 1999

G. OMB Circular No. A-123, Management Accountability and Control, as revised December 21, 2004

H. OMB Circular No. A-127, Financial Management Systems, as revised by Transmittal Memorandum Number 3, December 1, 2004

I. OMB Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, as revised by Transmittal Memorandum Number 4, November 28, 2000

J. Public Law 93-502, Freedom of Information Act of 1980

K. Public Law 99-474, Computer Fraud and Abuse Act of 1986

L. Public Law 100-235, Computer Security Act of 1987

M. Public Law 104-13, Paperwork Reduction Act of 1995, Revised

N. Public Law 104-106, Clinger-Cohen Act – IT Management Reform Act of 1996

O. Public Law 104-294, National Infrastructure Protection Act of 1996

P. Public Law 105-277, Government Paperwork Elimination Act of 1998

Q. Public Law, 106-398 Title X, Subtitle G, Government Information Security Reform Act, October 30, 2002

R. Public Law, 107-347, Title III Federal Information Security Management Act of 2002, December 17, 2002

4. **Policy.** It is the policy of the MMS to ensure the protection of its IT resources and government assets, based upon IT security policies set forth by Federal laws, regulations, guidelines, and directives; the DOI, and the MMS. The MMS IT security program will be consistent across all installations while making allowances for geographic location, installation size, scope, physical layout, environmental factors, and other site specific elements.

5. **Responsibilities.**

A. The Director is responsible for fulfilling the role as the Head of the Bureau, as prescribed by 375 DM 19. Additionally, the Director serves as the Bureau's Designated Approving Authority (DAA).

B. The MMS Chief Information Officer (CIO) serves as the Senior Security Officer (SSO) and is responsible for supporting the strategic requirements of the Bureau IT Security Program (ITSP). This includes ensuring that adequate funding, training, and resources are provided to the ITSP to support the Bureau mission. In addition to the responsibilities detailed in 375 DM 19 and the DOI IT Security Policy Handbook, the MMS CIO:

(1) Authorizes the shutdown of MMS network or systems to protect the confidentiality, integrity, and availability of IT resources.

(2) Performs all IT program coordination functions and acts as the primary liaison with the DOI's Office of the CIO.

(3) Implements all IT security-related activities in accordance with 375 DM 19 and the DOI IT Security Policy Handbook. This includes the development, coordination, interpretation, and implementation of IT security policy through bulletins and correlative process, standards, procedures and guidance, and the planning and monitoring of compliance with Federal and DOI policy.

C. The Bureau Chief Information Security Officer (BCISO) (formerly known as the Bureau IT Security Manager) is responsible for the overall management of the MMS IT security program and fulfills the role of the BCISO, as prescribed by 375 DM 19 and the DOI IT Security Policy Handbook. The BCISO must be a Certified Information Systems Security Professional. The BCISO must be an MMS employee and knowledgeable of IT and IT security matters. The BCISO will act as the Bureau focal point for all IT security matters. In addition, the BCISO:

(1) Manages the Bureau ITSP including the coordination of program activities with the Information System Security Managers (ISSM).

(2) Oversees the development and implementation of a Bureau-wide IT security plan for all MMS IT systems.

(3) Oversees the formulation and review of internal Bureau security policy (process, procedures, bulletins, and guidance) and supports implementation, testing, and integration into the Bureau culture. This includes managing the policy review process to ensure all documents are forwarded through the appropriate approval channels and adhere to accepted processes.

(4) Updates MMS IT security policy to accommodate Federal, DOI, and technological changes.

(5) Ensures that the appropriate oversight reviews are conducted; maintains copies of each review conducted; informs appropriate managers of any security deficiencies and/or noncompliance with regulations; and conducts a follow up review to ensure that actions are completed.

(6) In conjunction with Human Resources, coordinates mandatory annual security awareness and role-based IT security training requirements.

(7) Issues IT security newsletters, bulletins, guidance, or other documentation, as necessary.

(8) Chairs the Security Working Group (SWG).

D. The Certification and Accreditation (C&A) Manager is an individual dedicated to the Bureau's C&A compliance goals. The C&A Manager must be an MMS employee and knowledgeable of DOI's C&A process. The C&A Manager must maintain a Certification and Accreditation Professional certification. In addition to the responsibilities detailed in 375 DM 19 and the DOI IT Security Policy Handbook, the C&A Manager:

(1) Develops the MMS C&A process, establishing C&A prioritization schedules, tracks system C&A activities, generates reports, and coordinates Bureau C&A procurement activities.

(2) Coordinates the annual IT Internal Control Review (ICR) process for all systems and submits the IT ICRs to the DOI.

(3) Serves as a member of the SWG.

E. The Plan of Actions and Milestones (POA&M) Coordinator is dedicated to the Bureau's POA&M compliance goals. The POA&M Coordinator must be an MMS employee and knowledgeable of DOI's POA&M process. In addition to the responsibilities detailed in 375 DM 19 and the DOI IT Security Policy Handbook, the POA&M Coordinator:

(1) Develops and oversees the Bureau's POA&M implementation process.

(2) Coordinates quarterly status briefings with the Bureau DAA.

(3) Ensures Bureau POA&Ms and certification letters are submitted to the DOI in accordance with predetermined schedules.

(4) Ensures that updates to the POA&M process are incorporated, as necessary, and that all changes to the POA&M process are communicated throughout the Bureau to the appropriate staff.

(5) Tracks corrective actions to reduce or eliminate vulnerabilities for information systems.

F. The Information Systems Security Managers (ISSM) (formerly known as Program IT Security Managers) are responsible for their respective program's IT security objectives, written policies and procedures, reviewing and contributing to MMS and DOI policies, developing program-specific policies and procedures, user security activities, and acting as their program's liaison with the BCISO. The ISSMs must be MMS employees and knowledgeable of IT and IT security matters. The ISSMs will serve as the primary point of contact for all IT security matters within their respective program offices. In addition to the responsibilities detailed in 375 DM 19 and the DOI IT Security Policy Handbook, the ISSMs:

(1) Develop and implement a program-level security plan for their respective program office that is consistent with Federal, DOI, and Bureau security requirements.

(2) Develop supplemental policies and procedures for the program and issue them to the Information Systems Security Officers (ISSO) (formerly known as Installation IT Security Managers), employees, and contractors within their program office, as necessary.

(3) Provide input and review towards the development of DOI and Bureau related security policies, procedures, bulletins, plans, and guidance.

(4) Maintain IT security-specific information in the Departmental Enterprise Architecture Repository for systems under their purview.

(5) Serve as their program office's representative on the SWG.

G. The ISSO are responsible for the day-to-day security operations within their program or area of assigned responsibility. Theirs is an operational security effort regarding the systems and locations for which they are responsible. In addition to the responsibilities detailed in 375 DM 19 and the DOI IT Security Policy Handbook, the ISSOs:

(1) Provide information to the appropriate program manager for the completion of the program-level security plan, contingency plan, risk assessment, and other security issues.

(2) Ensure that a risk analysis is conducted and approved by management for the systems and locations for which they are responsible.

(3) Conduct or track annual security awareness and role-based IT security training for all users.

H. Program managers have the responsibility for fulfilling their role, as prescribed by 375 DM 19 and the DOI IT Security Policy Handbook. In addition, the Deputy Directors, Associate Directors, Regional Directors/Manager, Chief of the Office of Congressional Affairs, Chief of the Office of Public Affairs, and the Administrative Service Center Managers are responsible for fulfilling the duties of the program managers prescribed by 375 DM 19 and the DOI IT Security Policy Handbook. Program managers may designate an ISSO in writing to assist them with their IT security responsibilities. They will ensure compliance with the standards, requirements, and procedures as prescribed by 375 DM 19 and the DOI IT Security Policy Handbook. In addition to the responsibilities detailed in 375 DM 19 and the DOI IT Security Policy Handbook, program managers:

(1) Ensure that IT resources are adequately safeguarded throughout their respective program offices.

(2) Coordinate activities to ensure compliance of each program office with Federal, DOI, and MMS security policies and directives.

(3) Report immediately any security incident to the ISSO, ISSM, and/or BCISO.

I. Information System Owners have the responsibility for fulfilling the role of the Information System Owner, as prescribed by 375 DM 19 and the DOI IT Security Policy Handbook. In addition to the responsibilities detailed in 375 DM 19 and the DOI IT Security Policy Handbook, the Information System Owners:

(1) Ensure the overall security and proper use of their IT systems and that all information and data are labeled according to sensitivity.

(2) Ensure that adequate security controls are incorporated into the system or contract specifications prior to the acquisition or design of the system in accordance with NIST guidance.

(3) Ensure General Support System or Major Application System Security Plans are prepared according to guidance provided by the DOI, OMB, and NIST Special Publications.

(4) Conduct risk analyses periodically for their systems and ensure concurrence of management.

(5) Provide for the continuity of operations for sensitive applications and the IT systems which process them.

(6) Conduct annual IT ICRs for their respective systems.

J. System Managers have the responsibility for fulfilling the role of the System Manager as prescribed by 375 DM 19 and the DOI IT Security Policy Handbook.

K. System Security Managers have the responsibility for fulfilling the role of the System Security Manager, as prescribed by 375 DM 19 and the DOI IT Security Policy Handbook.

L. All MMS supervisors shall:

(1) Ensure that each subordinate is aware of their IT security responsibilities.

(2) Provide appropriate technical, physical, and administrative security safeguards for the IT resources for which they are responsible.

(3) Ensure compliance with this policy.

(4) Contact the appropriate IT security manager (ISSO or ISSM) to identify IT security requirements in the procurement of new or replacement equipment, software, and services.

(5) Ensure that the MMS Exit Clearance process is initiated for all departing employees and contractors.

(6) Ensure that departing employees do not access any IT resources after completing the Employee Exit Clearance Form. If the departing employee poses any risk to those resources after initiating an Employee Exit Clearance Form, access must be removed immediately. Supervisors may be held accountable for any damage to these IT resources by the departing employee.

(7) Inform the ISSO of any intra-bureau transferring employee so that appropriate IT resource accesses are reassigned.

M. All MMS employees have the responsibility for fulfilling the role of the Users of IT Resources, as prescribed by 375 DM 19. In addition, they shall:

(1) Comply with all IT security requirements pertaining to the IT resources they use and accounting for all activities performed under their user IDs and/or passwords.

(2) Report any suspicion of IT security violations to their supervisors, the ISSO, and the MMS Customer Support.

(3) Attend and/or complete all mandatory IT security training requirements as required by 375 DM 19 and the DOI IT Security Policy Handbook.

N. The SWG is comprised of the BCISO; C&A Manager; ISSMs from Administration and Budget (A&B), Minerals Revenue Management (MRM), and Offshore Minerals Management (OMM); and Security Operations representatives from A&B, MRM, and OMM. The SWG shall:

(1) Work with their ISSOs in the program and regional offices to maintain communications on important security matters and to ensure that policies are being carried out at all levels of the MMS.

(2) Develop and recommend security and information protection policy and guidance for the MMS.

(3) Make recommendations and providing IT security guidance in the MMS IT strategic planning process.

6. Procedures. The MMS shall comply with all Federal and DOI IT security policies and procedures.

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

8. Oversight.

A. The MMS shall have a BCISO and a Deputy BCISO designated in writing with a copy to the DOI's Chief Information Security Officer. The BCISO will report directly to the CIO and/or Deputy CIO for IT security matters and will be delegated in writing sufficient organizational authority to exercise this responsibility. An additional performance element pertaining to this function will be included in the BCISO's performance standards and will state or carry the following intent: "IT Security Management: Manages the MMS IT Security Program."

The BCISO is responsible for managing the Information System Security efforts for the entire Bureau. This responsibility includes planning, budget review, consolidation, and preparation of Bureau security reports, DOI reporting requirements, Incident Response Liaison activities, and coordination of the ITSP into the culture of the entire organization.

The duties and responsibilities of a BCISO are diverse, comprehensive, and complex. This position is one of high sensitivity and level of trust and therefore will be filled only by full-time

government personnel. In addition, this position has a requirement for high confidentiality due to the critical nature of the investigatory and compliance work.

The BCISO, Deputy BCISO, and ISSM/ISSO positions are considered to be High Risk Public Trust positions as defined by 5 CFR 731. The Bureau will ensure that the individuals in these positions have the appropriate level of background investigations completed. Additionally, the Bureau is responsible for determining the National Defense sensitivity level of these positions as defined in 5 CFR 732 and obtaining the appropriate level of security clearance (Critical Sensitive shall be the minimum requirement for all positions).

B. The MMS shall have a C&A Manager who will be responsible for developing the MMS C&A process, establishing C&A prioritization schedules, tracking system C&A activities, generating reports, coordinating Bureau C&A procurement activities, and coordinating the annual IT ICR process.

C. The Bureau shall be divided into organizational components, designated as Programs for the purpose of this policy. An ISSM and deputy will be assigned to each, designated in writing, with a copy to the BCISO.

D. The MMS shall have three ISSMs and deputies who will be responsible for their respective program's IT security objectives; written policies and procedures; reviewing and contributing to MMS and DOI policies; developing program-specific policies and procedures; user security; training; organizing and documenting all required security activities; acting as a liaison with the BCISO; to assist in ensuring that IT resources are adequately safeguarded throughout the program areas; and managing the tactical efforts of the program area to which they are assigned. These individuals serve as the programs' representatives on various IT security groups and interface directly with the BCISO on security matters. The ISSMs develop and implement an overall IT security plan for their respective programs that is consistent with DOI and Bureau policy. The ISSMs and deputy positions will be required to have a high risk security clearance, and the position descriptions of each will include reference to specific security responsibilities.

E. The Bureau shall be divided into physical components, designated as IT installations for the purpose of this policy. An ISSO and deputy will be assigned to each, designated in writing, with a copy to the ISSM and BCISO.

F. The ISSO will be responsible for installation-related IT security matters and will be delegated in writing sufficient authority to exercise this responsibility. Certain ISSO functions may be delegated, yet overseen, by the ISSO at their discretion. The ISSO positions may be less than full-time; e.g., one ISSO can oversee multiple installations/systems/applications as long as appropriate separation of duties and accountability is maintained. The ISSO and deputy positions will be designated high risk, and the position descriptions of each will include reference to specific security responsibilities required of the incumbents.

G. Any program manager, in conjunction with the ISSM/ISSO, may establish additional policy and guidance as deemed necessary, provided such policy/guidance does not conflict with

established Federal, DOI, or MMS policy or procedures. A copy of all such additional policy and guidance shall be sent to the BCISO for review and reference.

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

(1) The Government Accountability Office

(2) The Office of Management and Budget

(3) The Department of Homeland Security

(4) The DOI's Office of the Chief Information Officer

(5) The DOI's Office of the Inspector General

(6) The MMS Internal Control Review Coordinator

(7) The MMS Security Officer

(8) The MMS Records Manager

(9) The MMS Privacy Officer

I. The oversight authority will notify the BCISO in the event a review is to be conducted at any IT installation. The ISSO will notify the ISSM and BCISO of any authority scheduling a review at the installation (including unannounced visits) as soon as possible. In addition, the ISSO will forward to the ISSM and BCISO a copy of any review documentation or final report issued to the installation directly by an oversight authority.

J. IT Security management shall include different levels of compensating controls. At the highest level are laws and presidential directives which may be further elaborated on by DOI policies or directives. The MMS may further elaborate and define additional controls specific to the MMS. The MMS may issue IPDs and IT security bulletins which further identify requirements pertinent to all of the MMS, as well as define responsibility and accountability. Procedures shall be written to define the necessary and mandatory steps required for the execution of policy statements.

IT Security policies (including processes, procedures, bulletins and guidance) may be developed by any Council of Information Management Officials member or subordinate staff, and where appropriate, will be coordinated among the IT community. Once prepared, policies will be forwarded to the CISO for review, coordination, approval processing, numbering, dating, and distribution.

It is the policy of the MMS to implement and maintain IT Security Bulletins for adequately protecting information and IT systems in compliance with the DOI IT Security regulations.

IT Security Bulletins are designed to distribute information bureau-wide, as policy, requirements, guidelines, or standards. IT Security Bulletins carry the same authority and enforceability as issuances under the MMS directives systems. IT Security Bulletins are not intended to circumvent the policy channels, but are intended to distribute information that is needed quickly.

K. The MMS will adopt and comply with all finalized IT security policies promulgated by the DOI. This applies to both current and future policies. The only exceptions will be in instances where the MMS has policies in place which are more stringent than those of the DOI.