MINERALS MANAGEMENT SERVICE
INTERIM POLICY DOCUMENT

Effective Date: March 29, 2007
IPD No. 07-03
Series: Administrative
Title: Emergency Preparedness Planning – MMSNet

Originating Office: Information Management Division, Administration and Budget

1. Purpose. The purpose of this policy is to establish emergency preparedness standards for MMSNet, the general support system for the Minerals Management Service (MMS). It includes policy, responsibilities and standards (see attachment) necessary to meet policy requirements and to measure the success of policy implementation.

2. Objective. To establish an integrated capability to respond to emergencies for MMSNet.

3. Authorities.

A. Federal Preparedness Circular 65, Federal Executive Branch Continuity of Operations, June 2004.

B. FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

C. H.R. 2458-48 Federal Information System Management Act (FISMA) Title III –Information Security, 2002.

D. NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, June 2002.

E. NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, February 2005.

F. NIST Special Publication 800-53 Annex 2, Recommended Security Controls for Federal Information Systems: Moderate Baseline, June 2005.

G. OMB M-06-20, Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 2006.

4. Scope. This policy applies to all MMS staff and contractors involved in the preparation of emergency preparedness plans, including the MMS computer Incident Response Plan (IRP), Continuity of Operations (COOP) Plan, contingency plan (CP), and disaster recovery plan (DRP). These plans shall be developed for each MMS location. The Business Impact Analysis (BIA) parts of the CP and DRP shall include requirements in sufficient detail to clearly establish what data, hardware, software, and services shall be needed to securely restore essential business functions in the event of a disruption. This policy shall be reviewed annually from the effective date and updated as needed.

5. Definitions.

A. BIA (CP and DRP only) – Business Impact Analysis: The foundation of an IT contingency plan or disaster recovery plan. A BIA evaluates and prioritizes the functions necessary for the business to continue and lists the hardware, software, skills, and personnel functions necessary to provide the IT service for the business function.

B. COOP – Continuity of Operations: A COOP plan outlines the restoration of the MMS's essential functions after a catastrophic event, at an alternate site and performing those functions for 12 hours and up to 30 days before returning to normal operations. Implementation of a viable COOP plan is mandated by Federal Preparedness Circular 65, Federal Executive Branch of Continuity of Operation, dated June 15, 2004. Standard elements of a COOP plan include Delegation of Authority Statements, Orders of Succession, Vital Records (legal and financial records), essential personnel, and interoperable communication based on essential functions. Because it emphasizes the recovery of an organization's operational capability at an alternate site, the plan does not necessarily include IT operations although a CP is often an appendix to a COOP plan. A COOP plan does not address minor disruptions that do not require relocation to an alternate site, but may include other emergency preparedness documents as an appendix.

C. CP – Contingency Plan: Provides procedures and capabilities for recovering the IT functionality necessary for the business functions in the MMS. CPs are required by OMB Circular A-130 Appendix III which requires continuity of support plans for General Support Systems (GSS) and contingency plans for major applications (MA). For the purposes of this policy, the term contingency plan refers to both GSS and MA IT Contingency Plans. Information in it is used to recover from short-term disruptions and stays active through the end of restoration to normal IT function. It is sufficiently detailed to contain all information necessary to restore IT functions.

D. DRP – Disaster Recovery Plan: Provides detailed procedures to facilitate recovery of capabilities at an alternate site. They apply to major catastrophic events that deny access to the normal facility for an extended period. Typically, DRP refers to an IT focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The scope may overlap a CP; however, it is narrower in scope and does not address minor disruptions that do not require relocation. A DRP can be invoked at any time for disruptions up to 1 day and can be used for disruptions more than 30 days (beyond the time frame of a COOP plan so that essential functions are sustained or it is clear that an alternate facility must be acquired permanently or for an extended period of time). It details what to do to restore functions, services, and facilities. It lays out the criteria to determine if the CP or the COOP plan should be activated. It covers both IT and broad non-IT functionality.

E. IRP – Incident Response Plan (or cyber incident response plan): Provides strategies to detect, respond to, and limit consequences of malicious cyber incidents. The IRP includes developing procedures to address cyber attacks against an organization's IT system(s), such as malicious computer incidents; unauthorized access to a system or data; or unauthorized changes to system hardware, software, or data.

6. Policy.

A. Sites. The MMS sites at Anchorage, Camarillo, Denver, Herndon, Main Interior Building, Houston, and New Orleans shall prepare emergency preparedness plans for MMSNet. All emergency preparedness plans, including COOP plans, DRPs, IT CPs, and IRPs are interrelated and dependent on one another. All plans for a site shall be cooperatively developed. MMSNet plans developed at each location shall be similar in form.

B. Training. Preparedness staff shall complete designated preparedness training, annually.

C. Testing. An operational test of the MMSNet CP shall be budgeted for annually. Testing shall be rotated between Denver, Herndon, and New Orleans so that each location performs a test during the three year MMSNet accreditation period. Testing of preparedness plans shall never adversely affect operating MMSNet systems. A real emergency may be substituted for an operational test following the cessation of the emergency, as long as it meets the test requirements and the plan is updated within the time limits in this policy.

D. Auditing. Emergency preparedness plans shall be reviewed annually; and in accordance with the annual Federal Information Security Management Act (FISMA) reporting schedule.

E. Privacy. Content of preparedness plans shall be safeguarded appropriately as they contain both privacy and sensitive security information.

7. Responsibilities.

A. The Chief Information Officer/Deputy Chief Information Officer (DCIO) shall:

(1) Designate an emergency preparedness planning (EPP) coordinator for MMSNet who shall chair the EPP team.

(2) Coordinate with senior IT management for each program and shall designate an Emergency Preparedness Planning Team made up of the preparedness site coordinators from each MMS location as appropriate.

(3) Develop an audit process to evaluate the effectiveness of the emergency preparedness plans.

B. Emergency Preparedness Planning Team shall:

(1) Adhere to the standardized MMSNet preparedness planning process and templates.

(2) Document differences between locations.

(3) Recommend efficiencies and consolidation of preparedness functions.

(4) Prepare a communication plan that includes all preparedness plans and members.

C. Senior IT Program manager will identify an IT manager at each appropriate location who shall:

(1) Assign an IT preparedness plan coordinator in Anchorage, Camarillo, Denver, Herndon/MIB, Houston, and New Orleans with sufficient authority to represent the location's decisions on the team and time to perform team assignments.

(2) Review and approve the location's preparedness plan annually; and in accordance with the annual FISMA reporting schedule.

(3) Distribute and post the preparedness plan securely, making it available to the location's staff and to preparedness planning teams.

(4) Assign technical staff to perform monthly testing of backup media and restore capabilities.

D. The Preparedness Plan Coordinator at each site shall:

(1) Chair the location's preparedness plan team.

(2) Coordinate the location's various preparedness team activities.

(3) Participate actively and cooperatively in MMSNet IT preparedness planning team.

(4) Use the designated MMSNet preparedness plan template(s) to assure standardization across the MMS.

(5) Document and test any site specific processes not covered by the standard MMS preparedness plans.

(6) Assure all necessary updates are made to the preparedness plans from all sources; and in accordance with the annual FISMA reporting schedule.

(7) Interview the business units for input into the business impact analysis (BIA) annually or as business unit processes change ensuring IT functions provide the necessary services.

(8) Coordinate monthly testing of backup restoration tests for their site.

(9) Maintain an access list to offsite storage.

(10) Complete individual preparedness training, as assigned annually; and in accordance with the annual FISMA reporting schedule.

(11) Coordinate with the local technical staff to perform documentation and other necessary preparedness planning updates.

E. Site preparedness team members shall:

(1) Acknowledge their assigned role(s) and task(s) in an emergency.

(2) Participate in training and exercises to expand knowledge about emergency preparedness.

(3) Attend site meetings on emergency preparedness.

8. Cancellation. This IPD will remain in effect until no longer needed, or until it is incorporated into the MMS manual.

_____

Robert E. Brown
Associate Director for
Administration and Budget

Attachment

Attachment

Emergency Preparedness Standards for MMSNet

1. The MMS business processes shall be prioritized by the business process owners during the annual risk assessment performed for FISMA to determine which MMSNet subsystems and components are critical, vital, sensitive, or non-sensitive.

2. The annual risk assessment performed for FISMA shall be used to evaluate the scope of the MMS preparedness plans.

3. Each location shall prepare a business impact analysis (BIA) which will form the basis of each location's IT preparedness plan.

4. An MMSNet communication plan shall be developed, implemented and tested for all emergency operations planning, training and testing.

5. The MMSNet emergency preparedness plans shall be standardized across the MMS. Site specific plans shall include information unique to that location.

6. Emergency Preparedness team(s) shall be formed at each location. These teams may include COOP, DRP, CP, and IR teams and may have overlapping membership.

7. A secure, web based location for emergency plan documents shall be developed and serve as the central repository for all preparedness planning information.

8. A plan shall be developed for writing, updating, maintaining, testing and training the MMS emergency preparedness plans for each location.

9. Designated preparedness team members shall have a current "emergency preparedness kit" available to them in the event of an emergency.

10. Preparedness plans shall incorporate features to accommodate section 508 disabilities.

Training

11. Annual training based on NIST 800-84 Testing Training and Exercising IT Plans shall be provided to key Emergency Preparedness personnel; and in accordance with the annual FISMA reporting schedule.

Testing

12. Test plans shall follow NIST 800-84 Testing Training and Exercising IT Plans and be reviewed annually.

13. Preparedness plan tests shall be completed annually with results available for inclusion in the annual FISMA reporting cycle.

14. Preparedness plans shall be tested on paper (tabletop) and may be followed by a live preparedness test to determine the effectiveness, organizational readiness and ability to support MMSNet subsystems and major applications. Preparedness plan deficiencies shall be corrected within 30 days of testing or entered on the system Plan of Actions and Milestones (POA&M).

15. Business unit managers shall review the preparedness plan test results and initiate corrective actions as appropriate.

Updates

16. Updates to the preparedness plans' contact lists shall be performed quarterly or as necessary.

17. Preparedness plans shall be revised to address system/organizational issues encountered during plan implementation, execution, or testing.

18. Changes to the underlying business requirements supported by IT systems shall be addressed in the preparedness plan and updates made accordingly.

Alternate storage sites

19. Each location shall identify an alternate storage site and initiate the necessary agreements to permit the storage of backup information for their IT systems.

20. Alternate storage sites shall be geographically dispersed from the primary storage location.

21. Potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster shall be included in the preparedness plans and explicit mitigation actions documented.

Alternate Processing sites

22. Each location shall identify an alternate processing site and initiate necessary agreements to permit the resumption of information system operations for critical mission/business functions when the primary processing capabilities are unavailable for their information systems.

23. Alternate processing site agreements shall contain priority-of-service provisions in accordance with the information systems' availability requirements.

24. In order to reduce costs and simplify recovery, Denver shall be the alternate processing site for both Herndon and New Orleans. In the event of a disruptive event in Denver, Herndon shall be the alternate processing site for both Denver and New Orleans.

Alternate Work Sites

25. Each location shall prepare plans for alternate work sites in the event that temporary workspace is needed for MMS staff for more than 30 days.

Telecommunication services

26. Primary and alternate telecommunications services to support the information systems shall be identified and necessary agreements initiated to permit the resumption of system operations for critical mission/business functions when the primary telecommunications capabilities are unavailable.

27. Primary and alternate telecommunications service agreements shall contain priority-of-service provisions in accordance with the information systems' availability requirements.

28. Alternate telecommunications services shall not share a single point of failure with primary telecommunications services.

Information System Backups

29. Bureaus and offices shall conduct backups of user-level and system-level information contained in their information systems.

30. Backup information shall be stored at an appropriately secured location.

31. The frequency of information system backups and the transfer rate of backup information to alternate storage sites shall be consistent with the recovery time objectives and recovery point objectives.

32. Backup information shall be tested monthly to ensure media reliability and information integrity.

33. Backup information shall be selectively used in the restoration of information system functions as part of the preparedness plan testing.

34. Backup copies of the operating systems and other critical information system software shall be stored in a separate facility or in a fire-rated container that is not co-located with the operational software.

35. Backup hardware and software shall be standardized across MMS.

Information System Recovery and Reconstitution

36. Mechanisms with supporting procedures shall be employed to allow MMSNet to be recovered and reconstituted to the system's original state after a disruption or failure.

37. Secure information system recovery and reconstitution to the system's original state shall ensure that all:

a. system parameters are reset;

b. patches are reinstalled;

c. configuration settings are re-established;

d. secure state is active;

e. system documentation and operating procedures are available;

f. application and system software are reinstalled;

g. information from the most recent backups is available; and

h. the system is fully tested to ensure secure configurations and required functionality have been restored.