Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS Operational Policy for Separation of Duties for System Security Administration and Auditing

March 2006

Document Number: CMS-CIO-POL-INF07-01

TABLE OF CONTENTS

1. PURPOSE 1

2. BACKGROUND 1

3. SCOPE 1

4. OPERATIONAL POLICY 2

5. ROLES AND RESPONSIBILITIES 2

5.A. IT INFRASTRUCTURE SYSTEM ADMINISTRATORS 2
5.B. IT INFRASTRUCTURE SECURITY ADMINISTRATORS 3
5.C. CMS SECURITY AUDITORS 3

6. APPLICABLE LAWS/GUIDANCE 3

7. EFFECTIVE DATES 4

8. INFORMATION AND ASSISTANCE 4

9. APPROVED 4

10. ATTACHMENTS 4

1. PURPOSE

This document establishes an operational policy for the separation of duties among the personnel responsible for security administration, system administration, database administration, system operation, and auditing of CMS' security management infrastructure.

2. BACKGROUND

CMS operates and maintains a complex, distributed security management infrastructure. The security management infrastructure encompasses mainframe security (e.g., z/OS), server security (e.g., Windows and UNIX), database security (e.g., Oracle, DB2, and SQL), firewall security, router security, and other security devices maintained within the CMS and the Medicare Data Communication Network (MDCN) infrastructures.

The control and management of CMS' security management infrastructure necessitates a separation of duties among the key administrative components, such as:

- System administration of the physical devices (including the operating systems and all components running under the operating systems);
- Database administration of development, test, and production database systems;
- Security administration of distributed security management devices; and
- Auditing of security management devices and administrative activities.

Separation of job duties and responsibilities ensures that no one person has the authority and the ability to circumvent normal checks and balances. Separation of duties can help prevent malicious actions from occurring and help catch those that do occur. For example, the separation of administrative duties from auditing functions is necessary in order to prevent possible tampering of critical system log files.

3. SCOPE

This operational policy applies to all CMS infrastructure devices, systems, and databases controlled and operated by CMS or its designated IT Infrastructure Implementation Agent(s) or Contractor(s) at all Central and Regional Office locations (includes CMS Single Site, Lord Baltimore, Building 7111, Enterprise Data Centers, and other offsite facilities). This policy also applies to system security devices controlled and maintained by the MDCN Contractor (i.e., Ashburn, Koll, and other MDCN Contractor and Subcontractor sites that support the Medicare network). Security devices, systems, and databases controlled and operated by other CMS contractors not previously designated are not covered by this policy.

4. OPERATIONAL POLICY

Separate and distinct responsibilities and privileges must be associated with distinct security-relevant operations. Security personnel must, however, work closely with all system and database administration personnel to maximize system performance and security.

Security administration is an independent responsibility and shall not be assigned to a system/ application programmer, database administrator, system administrator, system operator, or security auditor. Functions performed by security administrators shall be entirely separated from the functions performed by system/application programmers, database administrators, system administrators, system operators, and security auditors.

Functions performed by security administrators shall be separated from the functions performed by personnel charged with auditing the security of CMS' infrastructure, systems, and databases to reduce the likelihood of fraudulent actions being taken, not detected, and/or not reported.

Security auditors shall have full administrative control over all security audit and log files. These personnel, however, will not have data altering capability for security devices, security management devices, audit and security logs, or CMS infrastructure devices.

5. ROLES AND RESPONSIBILITIES

The following entities have responsibilities related to the implementation of this operational policy:

5.A. IT Infrastructure System Administrators

IT Infrastructure System Administrators are responsible for the following activities:

- Daily operation of the CMS data and security systems, including administration of infrastructure operating systems;
- Designing, testing, installing, maintaining, and upgrading CMS' infrastructure devices (hardware and software);
- Performing setup and configuration of audit system and security log files;
- On a daily basis, ensuring that the system job that collects security and system log audit data from all CMS system devices are transferred to one of the following central collection points: Kiwi Syslog Server, Net Forensic Server, or other defined collection point);
- Maintaining and generating reports and journals on all audit reviews;
- Configuring and scheduling daily audit log runs, including the backup of all security log data based on the current backup and archiving strategy;

- Restoring security audit data at the request of the Office of Information Services (OIS) / Technology Management Group (TMG) Information System Security Officer (ISSO) or other security entities; and
- Reviewing system log and security audit files for anomalies on a daily basis, and reporting all identified anomalies as appropriate.

5.B. IT Infrastructure Security Administrators

IT Infrastructure Security Administrators are responsible for the following activities:

- Managing all CMS distributed security management devices;
- Reviewing system logs and security audit files for anomalies on a daily basis, and reporting all identified anomalies as appropriate; and
- Maintaining and generating reports and journals on all audit reviews.

5.C. CMS Security Auditors

CMS Security Auditors are responsible for the following activities:

- Defining and maintaining procedures for auditing infrastructure and contractor-maintained systems and security management log and audit files;
- Performing continuous in-depth security audits and penetration tests on all CMS systems and infrastructure devices;
- Controlling access to all CMS security audit and log file systems and devices;
- Reviewing security audit logs on an ongoing basis to ensure that security processes are followed and security anomalies are identified, reported, and corrected;
- Ensuring that security log data are properly retained and archived;
- Maintaining and generating reports and journals on all audit reviews;
- Researching all identified security anomalies or vulnerabilities, and generating associated CAPs as appropriate; and
- Recording all security audit findings and maintaining their associated CAPs in the CISS Database.

6. APPLICABLE LAWS/GUIDANCE

The following laws and guidance are applicable to this operational policy:

- Office of Management and Budget (OMB) Circular A-130
- CMS Policy for the Information Security Program, May 2005

7. EFFECTIVE DATES

This operational policy becomes effective on the date that CMS' Chief Information Officer (CIO) signs it and remains in effect until officially superseded or cancelled by the CIO.

8. INFORMATION AND ASSISTANCE

Contact the Director of the Technology Management Group (TMG) within the Office of Information Services (OIS) for further information regarding this operational policy.

9. APPROVED

/s/	3/31/06
D. Dean Mesterharm CMS Chief Information Officer and Director, Office of Information Services	Date of Issuance

10. ATTACHMENTS

There are no documents that currently augment this operational policy.