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

CMS Operational Policy for Infrastructure Router Security

September 2005

Document Number: CMS-CIO-POL-INF05-01

TABLE OF CONTENTS

1. PURPOSE

This document establishes an operational policy for the secure configuration, monitoring, and administration of infrastructure routers at the Centers for Medicare & Medicaid Services (CMS).

2. BACKGROUND

CMS operates and maintains a complex, distributed Wide Area Network (WAN) and Local Area Network (LAN) infrastructure. Key components of CMS' WAN and LAN are the infrastructure routers that direct network data messages, or packets, based on internal addresses and tables of routes, or known destinations, that serve certain addresses. The secure configuration of CMS' infrastructure routers is necessary to enhance the security of CMS' infrastructure and also to provide an enhanced layer of protection for devices such as firewalls, proxy servers, and mail servers. This operational policy establishes parameters for CMS' infrastructure router security based on acceptable government and private industry standards for securing router devices.

The proper configuration of crucial CMS infrastructure routers is necessary in order for the router to act as the first line of defense against unauthorized intrusions by preventing denial of service attacks, and other forms of penetration attempts. The review of router accounting, security, and auditing logs provides a means of ensuring that router configuration files meet the security standards set forth by Federal guidelines, ensures that log files have not been altered, and provides a means to ensure that change control documents have been submitted for each change to the router's configuration.

3. SCOPE

This policy applies to routing devices (CMS Single Site facility, Lord Baltimore Bldg, 7111 Building, and other offsite facilities) controlled and operated by CMS or its designated IT Infrastructure Implementation Agent or Contractor for the CMS Central and Regional Office infrastructure. Routing devices controlled by contractors other than the CMS IT Infrastructure Implementation Agent(s) or Contractor(s) are not covered by this policy.

4. OPERATIONAL POLICY

4.A Physical Controls

Routing devices shall be placed in a secure area of the CMS Single Site Baltimore Data Center, ADP Satellite Rooms, or outlying building ADP Rooms. Routing devices located in these facilities must have card access capability or be placed in a lockable rack or in a locked, caged area. Routing devices shall not be placed in unsecured areas. All interfaces on the router not being used are to be disabled, with the exception of the Console interface.

4.B Logical Controls

Logical configuration management of routers shall entail, at a minimum, the following:

- Disabling all TCP and UDP ports not required for normal router operation;
- Enhancing all vendor-supplied default security parameters;
- Providing controls to restrict remote access to a routing device; and
- Maintaining and reviewing router activity logs for anomalies on a regular basis.

Remote access to routing devices shall be restricted to a private, isolated, and protected management network. If Telnet access to a router is required, router administrators must use a secure TCP wrapper (e.g., Secure Shell).

Router access passwords shall conform to the following requirements:

- Passwords that are not easily guessed and conform to CMS' password standards;
- MD5 password encryption as the minimum level of encryption for all new and currently installed routers; and
- Future encryption upgrades on routers will include either 3DES data encryption or the ASA encryption standard, including the MD5 password hashing and secure authentication methods (e.g., TACACTS) to restrict access to router devices.

5. ROLES AND RESPONSIBILITIES

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

5.A Office of Information Systems (OIS)/Technology Management Group (TMG)

The OIS/TMG is responsible for the following activities:

- Providing oversight and frequent auditing of CMS infrastructure routers that are maintained by CMS' IT Infrastructure Implementation Agent(s) or Contractor(s); and
- Ensuring all reported router security incidents are fully and appropriately addressed.

5.B CMS IT Infrastructure Implementation Agent(s) or Contractor(s)

CMS' IT Infrastructure Implementation Agent(s) or Contractor(s) are responsible for the following activities:

- Providing router security services to CMS and adhering to the areas of router security defined in Section 4 of this document;
- Providing build documentation and implementation procedures that cover acceptable router security processes (within NIST and NSA guidelines); and
- Implementing changes (operating system upgrades and security patches) to infrastructure routers in a timely manner following CMS' change control procedures.

6. APPLICABLE LAWS/GUIDANCE

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

- Router Security Configuration Guide, National Security Agency, Version 1.1, September 27, 2002
- Computer Security Incident Handling Guide, National Institute of Standards and Technology, NIST Special Publication 800-61, January 2004
- DHHS Information Systems Security Program Policy, December 15, 2004
- CMS Information Systems Security Policy, Standards, and Guidelines Handbook, Version 1.2, July 19, 2004
- CMS Policy for the Information Security Program, CMS-CIO-POL-SEC02, 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/ 10/2/05

D. Dean Mesterharm
CMS Chief Information Officer and
Director, Office of Information Services

Date of Issuance

10. ATTACHMENTS

The following documents augment this operational policy:

- CMS Information Security Incident Handling Procedures, Version 1.0, March 9, 2004
- CMS Information Security Acceptable Risk Safeguards (ARS), Version 1.2, October, 25, 2004