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

CMS Operational Policy for
Use of IP Addresses in Applications

June 2005

Document Number: CMS-CIO-POL-INF03-01

TABLE OF CONTENTS

1. PURPOSE

This document establishes an operational policy for designing and implementing business applications/systems using Internet Protocol (IP) addressing capabilities for deployment and use within the Centers for Medicare & Medicaid Services (CMS).

2. BACKGROUND

One of CMS' strategic goals is to streamline our information technology environment so that existing and new systems can work more effectively by sharing information, and so that CMS can be more responsive to the demands of changing business needs and the promises of emerging technology. CMS plans to make our data more readily accessible to our beneficiaries, partners, and stakeholders in a secure, efficient, and carefully planned manner.

In striving to meet these goals, CMS has established a target enterprise architecture and modernization strategy that is based upon several key design principles:
- An established, secure Internet architecture for the CMS enterprise
- Defined products for the target enterprise architecture
- Defined security classifications and controls for CMS applications
- Defined security services that support the architecture and implement the controls
- Prescriptive application development standards and guidelines for the target environment

Use of IP addressing capabilities is fundamental to the design and implementation of business applications/systems planned for the CMS target enterprise architecture.

3. SCOPE

This operational policy applies to all applications developed for deployment and use within CMS-controlled IT systems infrastructure, including those of CMS' agents, contractors, or other business partners when acquired or supported by CMS funding.

4. OPERATIONAL POLICY

All CMS applications shall be designed and implemented to make logical resource access requests (e.g., for services, servers, etc.) using domain names that are dynamically translated into IP addresses via IT infrastructure domain name services. The use of hard-coded IP addresses within application programs is prohibited. All existing or legacy applications that utilize hard-coded IP addresses must be fully converted to using only dynamically translated IP addresses by no later than June 30, 2007.

5. ROLES AND RESPONSIBILITIES

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

5.A. System Owners/Managers

System Owners/Managers are responsible for ensuring that the applications comprising their systems do not use hard-coded IP addresses and instead use logical service name references.

5.B. Office of Information Services (OIS)/ Technology Management Group (TMG)

The OIS/TMG is responsible for the following activities:

- Providing IT infrastructure domain name services to dynamically translate logical resource reference requests from applications;
- Implementing controls to inhibit the use of hard-coded IP addresses within applications; and
- Assisting application/system designers and developers with designing CMS business applications/systems to conform to the CMS target enterprise architecture standards.

5.C. IT Infrastructure Implementation Agent or Contractor

CMS' IT Infrastructure Implementation Agent or Contractor is responsible for the following activities:

- Engineering the implementation, operation, and maintenance of IT infrastructure domain name service capabilities to dynamically translate logical resource reference requests from applications;
- Operating and maintaining IT infrastructure system controls to inhibit the use of hard-coded IP addresses within applications; and
- Supporting application/system designers and developers in the design, development, and implementation of CMS business applications/systems to conform to the CMS target enterprise architecture standards.

6. APPLICABLE LAWS/GUIDANCE

There are no laws and guidance specifically applicable to this operational policy.

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/	6/13/05
Dean Mesterharm	Date of Issuance
CMS Chief Information Officer and	
Director, Office of Information Services	

10.   ATTACHMENTS

There are no documents that currently augment this operational policy.