Department of Health and Human Services

Centers for Medicare & Medicaid Services
IT Modernization Program

CMS Technical Reference Architecture

Version 1.0

May 1, 2008

Foreword

This *Technical Reference Architecture, Version 1.0,* provides the technical architecture approach and technical reference standards of the Centers for Medicare & Medicaid Services (CMS).

This Architecture standard has been reviewed and accepted as a foundational component of CMS' Enterprise Architecture in accordance with CMS' Information Technology (IT) governance process.

This document complements the *CMS Internet Architecture (Including Minimum Platform Security Requirements),* Document Number: CMS-CIO-STD-INT01, dated July 2003 and supersedes the *CMS Target Architecture*, Document Number: CMS-CIO-STD-ARC01, dated September 2004.

CMS' Chief Technology Officer leads the development of this Architecture with the support of all components of the Office of Information Services (OIS) and input from CMS's IT contractors.

Any changes to the Technical Reference Architecture must be approved by the Chief Information Officer and the CMS Chief Technology Officer.

/s/ 5/5/08
Julie Boughn Date
Chief Information Officer (CIO) &
Director, Office of Information Services
Centers for Medicare & Medicaid Services

/s/ 5/2/08
Henry Chao Date
Chief Technology Officer (CTO)
Office of Information Services
Centers for Medicare & Medicaid Services

Record of Changes

Number	Date	Reference	A=Add, M=Modify, D=Delete	Description of Change	CR #
1	April 30, 2008	All		Initial Release, v 1.0	NA

CR: Change Request

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Background

The Centers for Medicare & Medicaid Services (CMS) are undertaking the development of a large-scale Information Technology (IT) Modernization initiative to improve the quality and delivery of healthcare services to beneficiaries, providers, and business partners. This initiative spans the CMS enterprise and includes development and implementation of mid-tier infrastructure known as the CMS Internet Architecture, a multi-zone architecture that is crucial to the effective operations of all CMS production environments, including the Enterprise Data Centers (EDC) Program, Baltimore Data Center (BDC), and CMS business. As CMS implements the components of the IT Modernization, the Agency needs new policies, processes, and procedures for implementing CMS' technical vision and a secure operating environment for the CMS enterprise.

1.2 Vision for the CMS Technical Architecture

This *CMS Technical Reference Architecture* (*TRA*) was developed to provide a standard technical reference for all of the CMS Production Environments and to communicate the architecture decisions determined by CMS/Contractor partnerships to date. It is anticipated that CMS will require several years to fully implement this TRA and its associated supplements throughout the CMS Production Environments.

The *CMS TRA* is intended to:

- Provide technical reference standards for all CMS Production Environments and future application designs to ensure a secure operating environment
- Communicate CMS' architecture approach and standards as determined by CMS
- Identify CMS' target technical environments to assist Agency contractors in developing their transition approaches
- Provide technical standards for use in future EDC, Enterprise System Development (ESD), and CMS task orders.

The current EDCs are built to CMS TRA standards. The Office of Information Services (OIS) recognizes that the CMS TRA will be implemented in a phased approach on an Agency-wide basis. CMS application owners and the owners of non-EDC production operations, including the Baltimore Data Center, will work with OIS to establish transition plans for implementing these standards. These transition plans will establish the priorities for addressing how existing operations and applications will minimize CMS' security risks until migration to an EDC or a fully TRA-compliant operational environment.

1.3 Purpose

This document articulates the technical architecture of the CMS Production Environments, and is designed to assist all CMS Business Partners in developing to, transitioning to, and maintaining the CMS Production Environments in accordance with CMS' enterprise technical architecture.

The CMS technical architecture supports five critical technical objectives that enable the CMS healthcare mission: (1) secure the CMS operating environment, (2) move CMS Production workloads efficiently, (3) provide appropriate and sufficient disaster recovery capability, (4) facilitate the migration and transition of CMS business owner applications into new production environments, and (5) build an enterprise technical architecture that anticipates and responds to the CMS mission and business needs.

This document complements the previous *CMS Internet Architecture (Including Minimum Platform Security Requirements),* Document Number: CMS-CIO-STD-INT01, dated July 2003 and supersedes the *CMS Target Architecture,* Document Number: CMS-CIO-STD-ARC01, dated September 2004 as the controlling technical standards documentation for CMS.

1.4 Scope

This document and its associated supplements represent the agreements on standard architecture to date by the CMS/Contractor partners for the CMS Production Environments. The requirements stated in this document reflect the agreed upon industry and government best practices to support the most viable approach for CMS that meets legislatively mandated security and privacy requirements and current technical standards.

1.5 Technical Reference Documentation Framework

This *CMS TRA* lays the foundation for additional, more specific, technical architecture and implementation documentation for all CMS Production Environments. Figure 1 provides the overall framework for the evolution of CMS technical documentation.

As depicted in Figure 1, the *CMS TRA* provides the foundation of CMS' technical reference documentation. The *CMS TRA* supports the next two more specific layers of detail, namely the documentation of CMS infrastructure at the second layer and CMS' application services at the third layer, respectively. The CMS Infrastructure Services supply the foundation for the CMS Application Services. The CMS Application Services provide the foundation for CMS workloads and applications.

The CMS Technical Documentation Framework establishes a clear, direct, and auditable linkage between all documentation of the CMS technical architecture and its implementation, from the *CMS TRA* through CMS Infrastructure Services and CMS Application Services. This *CMS TRA* provides the basis for the increasing level of detail and definition of the infrastructure and application services that operate within all of the CMS Production Environments.

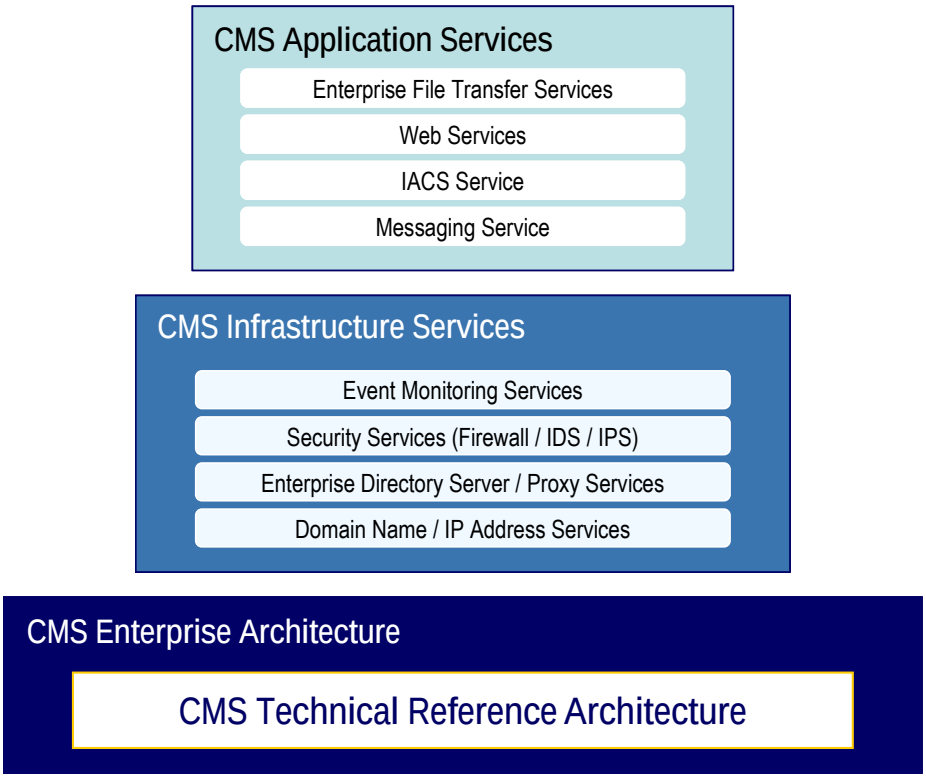

Figure 1. CMS Technical Documentation Framework

This *CMS TRA* is intended for use by CMS stakeholders. Additional supplemental volumes will be published on specific technical solutions. For example, Firewall rules will be published in the *CMS Technical Reference Architecture – Web Services Supplement*.

1.6 Alignment of FEA Technical Reference Model and CMS Technical Reference Architecture

To facilitate efforts to transform the federal government into one that is citizen centered, results oriented, and market based, the Office of Management and Budget (OMB) established the Federal Enterprise Architecture (FEA) Program, which is building a comprehensive business-driven blueprint of the entire federal government. The FEA is constructed through a collection of five interrelated "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across agencies.

The FEA Technical Reference Model (TRM) provides the standards, specifications, and technologies that collectively support the secure delivery, exchange, and construction of business and application components (Service Components) that may be used and leveraged in a Component-Based or Service-Oriented Architecture. It also unifies existing agency TRMs and E-Gov guidance by providing a foundation to advance the reuse and standardization of technology and Service Components from a government-wide perspective.

The FEA TRM is comprised of four core Service Areas. Each Service Area represents a technical tier supporting the secure construction, exchange, and delivery of Service Components. Each Service Area also aggregates and groups the standards, specifications, and technologies into lower-level functional Service Categories as follows:

1. **Service Access & Delivery.** Refers to the collection standard and specifications to support external access, exchange, and delivery of Service Components or capabilities. This area also includes the Legislative and Regulatory requirements governing the access and usage of the specific Service Component.
2. **Service Platform and Infrastructure.** The Service Platform and Infrastructure Area define the collection of platforms, hardware, and infrastructure specifications that enable Component-Based Architectures and Service Component re-use.
3. **Component Framework.** The Component Framework Area defines the underlying foundation and technical elements by which Service Components are built, integrated, and deployed across Component-Based and Distributed Architectures. The Component Framework consists of the design of application or system software that incorporates interfaces for interacting with other programs and for future flexibility and expandability. This framework includes, but is not limited to, modules that are designed to interoperate with each other at runtime. Components can be large or small, written by different programmers using different development environments, and may be platform independent. Components can be executed on standalone machines, a Local Area Network (LAN), intranet, or on the Internet.
4. **Service Interface and Integration.** The Service Interface and Integration Area defines the discovery, interaction, and communication technologies joining disparate systems and information providers. Component-based architectures leverage and incorporate Service Interface and Integration specifications to provide interoperability and scalability.

The CMS Enterprise Architecture and Strategy Group supports ongoing alignment of the CMS TRA with the FEA TRM. One of the goals of this effort is to maintain clear and auditable linkage between federal standards and CMS' standards.

CMS has accomplished this alignment by correlating FEA TRM Service Areas and Service Categories to *CMS TRA* infrastructure and application services throughout this document and in Appendix A, *CMS Products / Standards Selection List*.

1.7 Intended Audience

The *CMS TRA* communicates the shared infrastructure architecture decisions that have received explicit approval from the CMS CIO/CTO. The CMS Engineering Review Panel (ERP), CMS' Contractors supporting the CMS Production Environment, and other stakeholder entities made these decisions in partnership. The distribution of this document is expressly restricted to Production Environment Contractors; the CMS ERP; The MITRE Corporation, CMS' federally funded research and development contractor (FFRDC); and any entity that has received explicit access to this document from CMS executive management.

1.8 Relevant Documents

This document is not all inclusive and complements CMS' existing standards documentation, including but not limited to the following documents:

- *CMS Enterprise Messaging Infrastructure (Including Architecture, Standards and Implementation Requirements*), Document No. CMS-CIO-STD-INT02, December 2003
- *CMS Enterprise File Transfer (EFT) Infrastructure*, Version 1.1, Document No. CMS-CIO-STD-ARC02, June 2006 (updated October 2006)
- *CMS Information Security Acceptable Risk Safeguards (ARS)*, Version 3.1, April 24, 2008

Where there are conflicts, the *CMS TRA* and its corresponding Supplemental documents supersede and take precedence over other existing CMS documentation. An exception is in the case of the *CMS Information Security Acceptable Risk Safeguards* document.

1.9 Document Organization

This document is organized as follows:

Section	Overview
Section 2: CMS Infrastructure Architecture	Provides an overview of the CMS Production Infrastructure Architecture. This is the fundamental layer in the stack and provides the foundation for both CMS Infrastructure and Application Services.
Section 3: CMS Infrastructure Services	Provides an overview of the CMS Production Infrastructure Services. This is the next layer in the stack and provides the foundation for CMS Application Services.
Section 4: CMS Application Services	Provides an overview of the CMS Production Application Services. This is the final layer in the stack and provides the foundation for CMS workloads and applications.
Appendix A: CMS Products / Standards Selection List	Presents the CMS Product Selection List updated from the previous *CMS Target Architecture*.
Acronyms	Defines the acronyms used in this document.
List of References	Lists the references used in preparing this document.

2. CMS Infrastructure Architecture

The architecture for the CMS Production Environment is characterized as a "Multi-Zone" architecture with each zone separated by firewalls to support application systems' security. The first or outermost zone—the "Presentation Zone" or "De-Militarized Zone (DMZ)"—supports web servers. The second or middle zone—the "Application Zone"—supports business logic for the applications. The third or innermost zone—the "Data Zone" or "Secure/Protected Zone"—contains the database servers used by the applications. Additional network segments support specialized network services such as Public Key Infrastructure (PKI), Domain Name Services (DNS), etc. Other zoned regions are as described below.

The *CMS TRA* supports a single, unified interface with both internal and external users/ customers, as well as an operational approach to the applications developed and implemented by and/or for CMS. Various applications hosted in the CMS Production Environment will be able to access data, where and when appropriate, in the data warehouse/data marts and a variety of operational databases located within CMS and its contracted sites in the Data Zone.

The databases accessed by applications are on operational database servers or reside in data warehouses or data marts. Thus, the innermost zone, the "Data Zone," contains database servers supported within CMS and databases accessed across all of CMS, securely linking CMS' Fiscal Agents (FA), Fiscal Intermediaries (FI), Medicare Administrative Contractors (MAC), and Carriers. A common, message-oriented interface between the CMS Production Environment application servers and the database servers facilitates access to the databases at various physical sites.

2.1 Presentation, Application, and Data Zones

The *CMS TRA* supports the Presentation, Application, and Data Zones and their specific access requirements and protections to support the needs for customers of each zone. Each CMS Production Environment employs these three zones to separate user and application connectivity for security purposes. The major drivers for the *CMS TRA* implementation are to:

- Provide a standardized, secure computing environment for new CMS applications
- Provide the necessary control to implement policy and requirements changes so CMS can comply with statutes and regulations on a timely basis, and to ensure the operational flexibility to handle processing reconfigurations, e.g., for workload distributions and balancing
- Enhance interaction with the CMS Production Environments by providing standard interfaces for entities that access CMS applications and data (e.g., beneficiary data, claims history)
- Improve CMS' capability to be more independent, responsive, and effective in handling Business Operation Contractor transitions (e.g., departures or replacements).
- The permitted operating system (OS) type for the platforms in the CMS Multi-Zone Architecture is UNIX and restricted to Sun Microsystems Solaris® and IBM Mainframe z/OS® implementations.

Figure 2 depicts the latest accepted standards of the CMS Multi-Zone Architecture. The CMS Multi-Zone Architecture consists of four main groups of infrastructure components: the Transport Zone, Standard UNIX Zone, Legacy Windows Zone, and the Management Zone.

The Transport Zone is composed of router, IDP, and switch infrastructure for the sole purpose of managing and controlling network traffic. The external sources of network traffic destined for CMS Production Environments are the Internet, On-Net (which is comprised of CMSnet, HHSnet, and MDCN traffic), Off-Net (also known as Extranet), and Core Networks. Both inbound and outbound Internet, On-Net, and Extranet traffic are governed by two discrete stacks of border routers, IDP, and physical switches. Both On-Net and Off-Net border routers are provided by the ISPs. The Core Network, comprised of two routers, connects inbound and outbound traffic destined to other CMS Production Environments. Inbound Internet, On-Net, Extranet, and Core traffic are routable to the other groups of infrastructure components.

The Standard UNIX Zones are comprised of Presentation, Application, and Data Zones that separate user, application, and database connectivity to ensure defense-in-depth. All inbound and outbound traffic to each of these Zones route through redundant switches and Firewalls (Netscreen, Checkpoint, and PIX, respectively) and are protected by redundant passive IDS systems. The UNIX Presentation Zone is the first zone that separates the user or end-application from the Application and Data Zones. This Zone is supported by redundant SSL-based, F5 Big IP load balancers and external DNS servers on a dedicated IPSec-based VLAN. The UNIX Application Zone resides behind the UNIX Presentation Zone and controls the operation of application-specific business functionality and is supported by redundant F5 Big IP load balancers. The UNIX Data Zone resides behind the UNIX Application Zone and contains all data access logic and data sources, including data warehouses and data marts as well as operational databases for applications. All information to be stored in the Data Zone comes through the Application Zone with the exception of file transfers for FFS applications which connect directly into the Data Zone for trusted CMS partners.

The Legacy Windows Zones are comprised of Windows Proxy DMZ, Presentation/Application, and Data Zones. These zones separate user, application, and database connectivity to ensure defense-in-depth. The Windows Proxy DMZ is located in the first physical segment and provides BlueCoat proxy services for web traffic and is protected by redundant IDS systems. The Windows Presentation and Application Zones are collocated in the second physical segment and have functional characteristics similar to the Presentation and Application Zones in the Standard UNIX Zones. The Windows Data Zone is in the third physical segment and has functional characteristics similar to the UNIX Data Zone. All inbound and outbound traffic to each of these Zones route through redundant switches and Firewalls (Netscreen, Checkpoint, and PIX, respectively) to provide filtering between Zones and are protected by redundant passive IDS systems.

The Management Zone provides security, monitoring, and management in support of all other Zones via redundant Netscreen firewalls and physical switches. All network traffic destined for this Zone is routed by redundant border routers, physical switches, firewalls, and active Netscreen IDP systems. The only routing exception is that approved support users may connect directly from Vendor Managed Networks. The Management Zone is separated into seven functional areas by IPSec-based VLANs: Management DMZ, Shared Tools, Firewall Management Tools, Security Tools, Backup Tools, UNIX Tools, and Legacy Windows Tools. Production Environment Contractor sessions into the Management DMZ are routed IPSec based

VLANs via redundant Cisco VPN 3030 Concentrators. The Shared Tools segment houses redundant, internal DNS servers that service all applications in the Transport, Standard UNIX, Legacy Windows, and Management Zones.

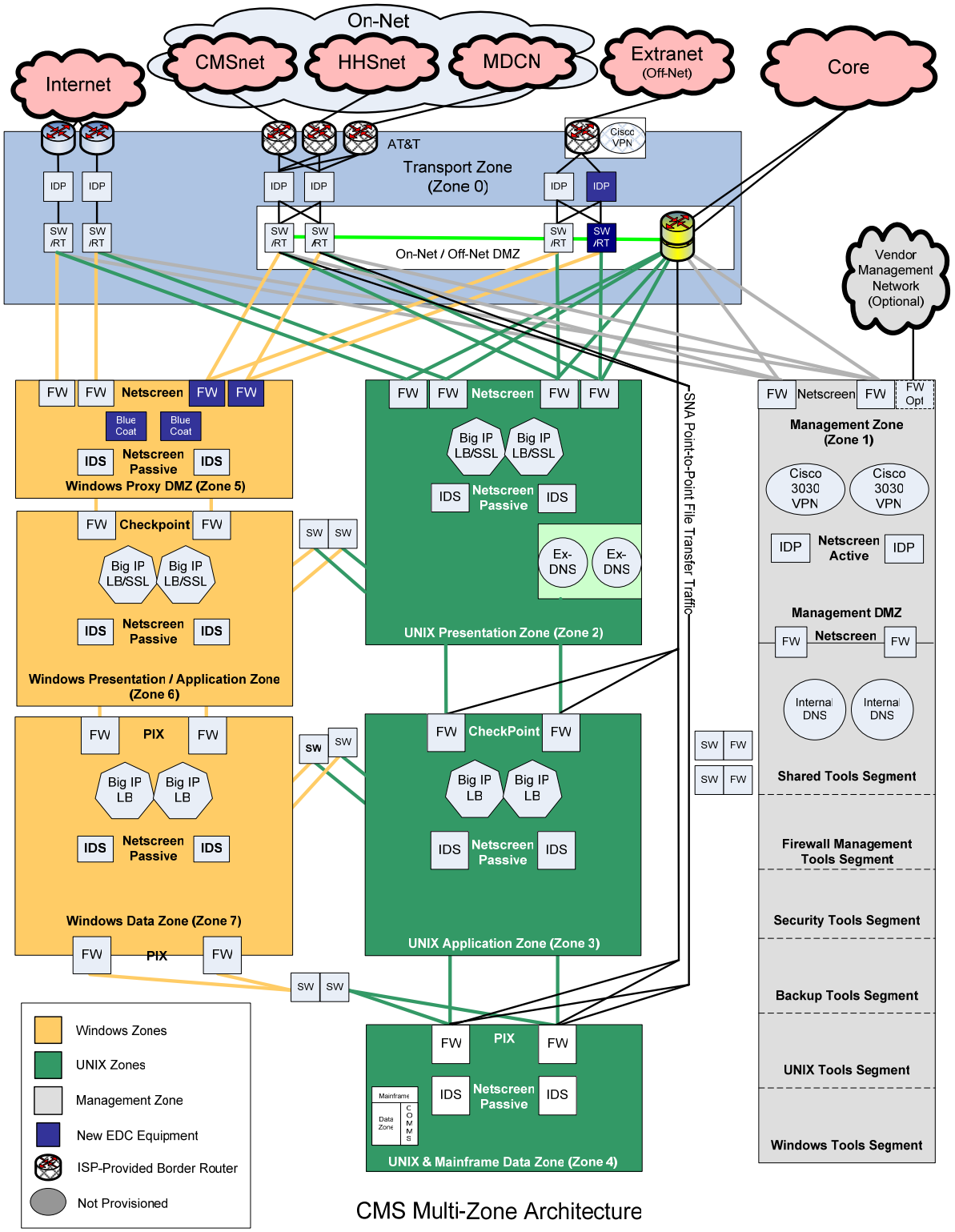

Figure 2. CMS Multi-Zone Architecture

2.1.1 Presentation Zone

The Presentation Zone is the first zone that controls how users and applications interface with CMS Production Environments. The Presentation Zone separates the user or end-application from the Application and Data Zones. This separation provides the first layer of security for the CMS Production Environments. All screen forms and Graphical User Interfaces (GUI) are located in the Presentation Zone.

The Presentation Zone contains the web pages for public and private websites and all web servers. The Presentation Zone servers contain presentation logic (HTML) for websites containing static content. No application/business/database logic/processing are executed on servers in the Presentation Zone. Furthermore, all support applications, business logic, databases, tables, and sensitive information for the CMS Internet and Private Network applications resides on dedicated servers in the Application Zone and the Data Zones. Tables 2 and 3 (see pages 22 and 26, respectively) provide a list of infrastructure and application services that reside in the Presentation Zone.

The Presentation Zone is supported by redundant F5 Big IP (Internet Protocol) load balancers to ensure high availability. Redundant, external Domain Name Service servers also reside in the Presentation Zone on a dedicated IPSec-based Virtual Local Area Network (VLAN) (enclave) to provide name resolution for external-facing applications.

All inbound and outbound traffic to the Presentation Zone routes through a redundant pair of switches and Netscreen Firewalls to provide filtering between Zones and is protected by redundant, dedicated passive Netscreen Firewalls and passive Netscreen Intrusion Detection Systems (IDS). The dedicated Firewalls and IDSs provide a concentration of security services that include, at a minimum, packet and protocol filtering, information hiding, and audit logging consistent with the *CMS TRA* and its Supplements.

2.1.2 Application Zone

The Application Zone resides behind the Presentation Zone and contains application servers. This separation ensures that connectivity from the Internet, Private Network, EDC4 Intranet, EDCs, and all other CMS Production Environments must traverse the Presentation Zone before connecting to the Application Zone. The Application Zone controls the operation of application-specific business functionality. These application-specific business functions include data validation, execution of business rules, calculations, manipulation of data, and control of the environment. When an Application Zone application requires information or actions from the Data Zone, the application makes the request, and processes the response, using a redundant WebSphere MQ messaging facility. Business results from the Application Zone are then returned to the Presentation Zone and formatted by the Presentation Zone for delivery to the end user or application for viewing or further processing. Tables 2 and 3 (see pages 22 and 26, respectively) provide a list of infrastructure and application services that reside in the Application Zone.

All inbound and outbound traffic to the Application Zone is routed by a redundant pair of switches and Checkpoint Firewalls to provide filtering between Zones and is protected by redundant, dedicated Checkpoint Firewalls and passive Netscreen IDSs. In addition, all load-balanced traffic is managed by redundant F5 Big IP load balancers to ensure high availability. The dedicated Firewalls and IDSs provide a concentration of security services that include, at a minimum, packet and protocol filtering, information hiding, and audit logging consistent with the *CMS TRA* and its Supplements.

2.1.3 Data Zone

The Data Zone resides behind the Application Zone and contains all data access logic and data sources, including data warehouses and data marts as well as operational databases for applications. All information to be stored in the Data Zone comes through the Application Zone. The Data Zone interfaces with the Application Zone via a redundant WebSphere MQ messaging, WBI Broker, and WAS facilities, and is separated from the Presentation Zone for security purposes. Tables 2 and 3 (see pages 22 and 26, respectively) provide a list of infrastructure and application services that reside in the Data Zone.

File transfers for Fee-For-Service (FFS) applications are the only exception to these data transfer restrictions. In support of FFS, file transfers are enabled via Connect:Direct directly into the Data Zone for trusted CMS partners (i.e., MACs and CMS Regional Offices).

All inbound and outbound traffic to the Data Zone is routed by a redundant pair of switches and PIX Firewalls to provide filtering between Zones and protected by redundant, dedicated PIX Firewalls and passive Netscreen IDSs. The dedicated Firewalls and IDSs provide a concentration of security services that include, at a minimum, packet and protocol filtering, information hiding, and audit logging consistent with the *CMS TRA* and its Supplements.

2.2 Legacy Windows Zones

The legacy Windows Architecture consists of three physical network segments, distinct from the standard UNIX Multi-Zone Architecture described in Subsection 2.1. The Windows Proxy DMZ is located in the first physical segment and provides a proxy services for web traffic. The Windows Presentation and Application Zones are collocated in the second physical segment and have functional characteristics similar to the TRA Presentation and Application Zones in the standard UNIX Multi-Zone architecture. The Windows Data Zone is in the third physical segment and has functional characteristics similar to the TRA Data Zone in the standard UNIX Multi-Zone architecture.

Some current applications running in the production Windows Zone are not in compliance with the standard UNIX Multi-Zone Architecture because they have “front-end” components on Windows servers and “back-end” components on UNIX servers. For instance, the architecture of both the Health Plan Management System (HPMS) (EDC Task Order 0002) and National Data Warehouse (NDW) (EDC Task Order 0004) applications place their “front-end” components—those in the Presentation and Application Zones—on Windows servers and their “back-end” components—those in the Data Zone—on UNIX servers. The architectural design of these applications is not standard because the applications do not reside in the standard UNIX Multi-Zone Architecture and they employ mixed Windows and UNIX platforms.

The Windows Presentation Zone houses Windows servers and is segmented from the standard UNIX Multi-Zone segments. The OS implementations permitted in the Windows Zones are restricted to Windows (i.e., Windows 2000/2003)**. The Windows Zones are not part of the standard CMS TRA and, as such, are considered a waiver to the UNIX Multi-Zone Architecture. CMS does not permit new platforms in the Windows Zone without explicit consideration and an approved waiver by the CMS CTO.**

All inbound and outbound traffic to the Windows Proxy DMZ is routed by a redundant pair of switches and Netscreen Firewalls to provide filtering between Zones and is protected by redundant, dedicated Netscreen Firewalls and passive Netscreen IDSs. All inbound and outbound traffic to the Windows Architecture Presentation and Application Zones is routed by a redundant pair of switches and protected by redundant, dedicated Checkpoint Firewalls and passive Netscreen IDSs. All inbound and outbound traffic to the Windows Architecture Data Zone is routed by a redundant pair of switches and protected by redundant, dedicated PIX Firewalls and passive Netscreen IDSs. The dedicated Firewalls and IDSs in these Zones provide a concentration of security services that include, at a minimum, packet and protocol filtering, information hiding, and audit logging consistent with the *CMS TRA* and its Supplements.

2.3 Management Zone

In addition to the Presentation, Application, and Data Zones, the CMS Multi-Zone Architecture provides security, monitoring, and management in the Management Zone. All Internet, Private Network, EDC intranet, or CMS Production Environment network traffic destined for the Management Zone is routed by a redundant pair of border routers and physical switches. This is the same network infrastructure that provides access to the standard Multi-Zone Architecture. The only exception is that approved users have the option to connect to the CMS Production Environments for maintenance and management support directly from Vendor Managed Networks, or other outside networks, via Management Zone components. Vendors can install redundant Netscreen firewalls in the Management Zone to establish private IPSec-based VLANs to meet their specific needs. Inter-connection security agreements should be explored for external maintenance and management support vendors.

All traffic into the Management Zone is protected by redundant firewalls and active Netscreen Intrusion Detection and Prevention (IDP) systems. These firewalls and network-based IDP systems provide a concentration of security services that include, at a minimum, packet and protocol filtering, information hiding, and audit logging. All of the network traffic is monitored via redundant IDP systems and each system is configured as required by the *CMS TRA* and its Supplements. In addition, all access to the Management Zone must be authenticated in accordance with CMS' standards.

The Management Zone is separated into the following functional areas by IPSec-based VLANs as follows:

- Management DMZ
- Shared Tools
- Firewall Management Tools
- Security Tools

- Backup Tools
- UNIX Tools
- Legacy Windows Tools.

Each segment is separated from the others to ensure that no connectivity between the VLANs and/or physical switches is allowed in this Zone. In addition, connectivity from each of the Management Zone functional segments to the standard UNIX and legacy Windows Presentation, Application, and Data Zones is protected by redundant Netscreen firewalls and physical switches.

2.3.1 Management DMZ Segment

The Management DMZ is similar to the Presentation Zone in the standard UNIX Multi-Zone Architecture. The Management DMZ is the first of the IPSec-based VLANs that provides an interface to the other IPSec-based VLANs in the Management Zone. The subsequent IPSec-based VLANs contain the security and management tools for use by the Production Environment Contractors.

All inbound and outbound traffic to the Management DMZ is routed by a redundant pair of switches and protected by a dedicated, redundant pair of border firewalls and active Netscreen IDP systems. Connectivity from the Management DMZ to the rest of the Management Zone segments is further protected by another dedicated, redundant pair of Netscreen firewalls. The dedicated border firewall and IDP systems provide a concentration of security services including, at a minimum, packet and protocol filtering, information hiding, and audit logging consistent with the *CMS TRA* and its Supplements. Additionally, all access from the Management DMZ to the other Management Segments must be secured via two factor authentication.

Production Environment Contractor sessions into the Management DMZ are routed to the appropriate IPSec-based VLANs via redundant Cisco® Virtual Private Network (VPN) 3030 Concentrators to manage IPSec (Internet Protocol Security) VPN connections.

2.3.2 Shared Tools Segment

The Production Environment Contractor installs and manages the tools that reside in this segment. All tools in this segment manage the Shared Services that have been contracted to the Production Environment Contractor. The Production Environment Contractor is responsible for maintaining all tools in accordance with CMS Change Management and Configuration Management processes and tracking all updates to these systems for consistency across the Production Environments. These tools also must comply with the *CMS TRA and its Supplements, CMS Information Security Acceptable Risk Safeguards,* and National Institute of Standards and Technology (NIST) Special Publications (SP) 800-12 and 800-52.

The Shared Tools segment also houses redundant, internal DNS servers that provide name resolution for all applications in the standard UNIX Multi-Zone Architecture, legacy Windows Architecture, and Management Zones.

2.3.3 Firewall Management Tools Segment

The Production Environment Contractor installs and manages the tools that reside in this segment. All tools in this segment manage the Firewall Management services that have been contracted to the Production Environment Contractor. The Production Environment Contractor is responsible for maintaining all tools in accordance with CMS Change Management and Configuration Management processes and tracking all updates to these systems for consistency across the Production Environments. These tools also must comply with the *CMS TRA* and its Supplements, the *CMS Information Security Acceptable Risk Safeguards,* NIST SP 800-12, NIST SP 800-41, and NIST SP 800-52.

2.3.4 Security Tools Segment

The Production Environment Contractor installs and manages the tools that reside in this segment. All tools in this segment manage the Security Services that have been contracted to the Production Environment Contractor. The Security Services located in this segment are, but are not limited to, Intrusion Detection and Prevention tools, security alert tools, and Syslog tools. The Production Environment Contractor is responsible for maintaining all tools in accordance with CMS Change Management and Configuration Management processes and tracking all updates to these systems for consistency across the Production Environments. These tools should also comply with the *CMS TRA* and its Supplements, the *CMS Information Security Acceptable Risk Safeguards,* NIST SP 800-12 and NIST SP 800-52.

2.3.5 Backup Tools Segment

The Production Environment Contractor installs and manages the tools that reside in this segment. All tools in this segment manage the Backup/Restore Services that have been contracted to the Production Environment Contractor. The Production Environment Contractor is responsible for maintaining all tools in accordance with CMS Change Management and Configuration Management processes and tracking all updates to these systems for consistency across the Production Environments. These tools also must comply with the *CMS TRA* and its Supplements, the *CMS Information Security Acceptable Risk Safeguards,* NIST SP 800-12 and NIST SP 800-52.

2.3.6 UNIX Tools Segment

The Production Environment Contractor installs and manages the tools that reside in this segment. All tools in this segment manage the UNIX administration services that have been contracted to the Production Environment Contractor. The Production Environment Contractor is responsible for maintaining all tools in accordance with CMS Change Management and Configuration Management processes and tracking all updates to these systems for consistency across the CMS Production Environments. These tools also must comply with the *CMS TRA* and its Supplements, the *CMS Information Security Acceptable Risk Safeguards,* and NIST SP 800-7, NIST SP 800-12, and NIST SP 800-52.

2.3.7 Windows Tools (Legacy) Segment

The Production Environment Contractor installs and manages the tools that reside in this segment. All tools in this segment manage the Windows Services that have been contracted to the Production Environment Contractor. The Production Environment Contractor is responsible for maintaining all tools in accordance with CMS Change Management and Configuration Management processes and tracking all updates to these systems for consistency across the CMS Production Environments. These tools also must comply with the *CMS TRA* and its Supplements, the *CMS Information Security Acceptable Risk Safeguards,* NIST SP 800-12 and NIST SP 800-52.

2.4 Certification & Accreditation

The Production Environment Shared Infrastructure must pass a Certification & Accreditation (C&A) prior to beginning to execute production applications. The Production Environment Contractor will support a third party C&A evaluation team selected by CMS. The necessary EDC Contractor support for this activity includes supplying physical access to the CMS Production Environment facilities, including the Security Operations Center/Network Operations Center (S/NOC); supplying access to the CMS infrastructure hardware; and supplying access to any documentation identified by the C&A evaluation team. The C&A team use the *CMS TRA* during the evaluation process. All CMS Production Environment C&As must comply with CMS' published C&A procedures.

2.5 Wide Area Network

2.5.1 Current WAN

The Medicare Data Communications Network (MDCN) connects the CMS headquarters in Baltimore with CMS Regional Offices and provides remote dial-up access for more than 75,000 users. The MDCN also supports connectivity among such CMS business partners as FIs, Insurance Service Providers, and State Medicaid agencies and with CMS. The MDCN is a private, Frame Relay "Managed Network Service" provided by a third-party service provider, AT&T. In addition to the MDCN, AT&T provides Internet access over a separate network to CMS facilities and CMS employees. Although the MDCN is a private network for CMS' Extranet and intranet users, the environment is not a dedicated environment; AT&T owns and operates the actual facilities that manage the network and these facilities are shared with other AT&T customers.

CMS' current MDCN WAN comprises approximately 500-plus connections with CMS locations and trusted business partners. CMS pays for more than 500 of these connections. These locations only access the CMS MDCN; Internet usage is not allowed on the MDCN except for CMS Regional Office locations.

The Medicare Data Communications Network (MDCN) connects the CMS headquarters in Baltimore with the CMS Regional Offices and provides remote dial-up access for more than 75,000 users. In addition, the MDCN supports connectivity between CMS business partners as FIs, Insurance Service Providers, and State Medicaid Agencies.

To support CMS' Systems Network Architecture (SNA) legacy applications like the Common Working File (CWF), the MDCN contract with AT&T also provides four (4) IBM mainframe computers to route SNA data to and from various CMS and Operational Business Partner (OBP) locations. At present, the centralized management functionality includes:

- Routing of SNA data
- SNA address maintenance
- SNA address translation
- Storage Area Network (SAN) application session management.

It is estimated that approximately 70-plus unique SNA networks are configured within the core of the MDCN network (Net Ids). These unique SNA networks support more than 60,000 CMS users and Operational Business Partners that access these SNA mainframe applications.

Various approaches are deployed to support SNA transport from location to location over the MDCN. CMS and business partners use either IBM's Enterprise Extender (EE) or Cisco's Data Link Switching Plus (DLSw+) to interface to the MDCN via IP connection (over Frame Relay).

For Internet access, CMS uses AT&T's Managed Internet Services (MIS) to provide access to each of CMS' locations. Internet access for CMS Regional Offices is backhauled via the MDCN to the CMS Baltimore Data Center where redundant, dedicated T-3 leased lines access the Internet.

For either MDCN or Internet services, CMS purchases a managed service from AT&T, which provides for the installation and configuration of all Customer Premise Equipment (CPE). The AT&T services also include performance reporting, fault management, and issue resolution for the Frame and Internet portions.

2.5.2 Current Limitations and Issues

The MDCN SNA current environment relies on proprietary software/ programming and mainframe computers at the core of the MDCN network. This reliance on proprietary products greatly minimizes CMS' flexibility to readily update or enhance systems leading to inefficiency and increased monthly operating costs. It also creates additional security risks because proprietary applications seldom are run through the IT security System Development Life Cycle. Most commercial and government organizations have moved to cost-effective and ubiquitous technologies that facilitate support of legacy SNA applications at the edge of the network such as IP in the core network.

The use of personal health information (PHI) is fundamental to CMS business operations and public services; however, CMS' current architecture does not support encryption. Data transmitted over the WAN traverses the network in the clear, which exposes the data to potential vulnerability. In particular, PHI traverses the WAN between external as well as internal business partners. As a result of the HIPAA Privacy and Security Rules, most organizations are implementing some form of encryption-based technology to transmit or store PHI.

2.5.3 WAN Modernization Goals

The future CMS WAN, as described in the *CMS WAN Modernization Concept of Operations, Draft, Version 0.6* (August 2007), must support interactive and integrated communications among many geographically dispersed organizational entities within and outside CMS. As CMS implements new application systems within the EDCs, the need for secure, reliable, and cost effective transport is imperative. CMS has set the following goals for the WAN Modernization to ensure CMS accomplishes its mission and technology needs:

- To substantially improve all aspects of CMS' network security, including privacy of PHI
- To maintain network reliability (availability) through well-defined SLAs
- To simplify SNA transport over the new CMS Private Network (CPN) and eliminate any Core-based SNA translation functions
- To deliver adequate geographic coverage (ubiquity) to support a vast healthcare community and CMS business partners
- To ensure long-term competitive environment that provides more cost-effective solutions for CMS, its business partners, and CMS beneficiaries.

2.5.4 WAN Modernization Vision and Strategy

CMS envisions the modernized WAN to support data communications services among CMS Operational Business Partners. The Modernized WAN must be highly flexible and capable of supporting today's health care initiatives and such future health care initiatives as electronic health records (EHR) well into the 21st century. To accomplish this, the Modernized WAN must be scalable, interoperable, extensible, and ubiquitous. This modernization is a major undertaking for CMS in design, implementation, and migration of existing locations (CMS and CMS Business Partners) that still must support SNA applications.

2.5.4.1 Stakeholders and Services

CMS' architectural strategy calls for creating a secure CPN that is isolated from the public network (Internet) but will still allow selected Internet traffic to access the private network in a highly secure manner. The CMS Core Network connecting CMS' data centers will integrate the CMS Private and Public Networks.

Security is a paramount objective in all aspects of this design and implementation. CMS will achieve the desired level of security by isolating selected locations into a private network with full encryption of any data transmitted over it. This strategy will support the following stakeholder classes or communities of interest:

- Enterprise Data Centers (includes EDC4—the Baltimore pre-production facility that simulates the EDC environment)
- CMS Offices
- On-Net Business Partners (ONBP), such as HIGLAS, and other governmental agencies
- Off-Net Business Partners (OFBP), such as FIs and Carriers
- Internet users, such as beneficiaries and providers.

The Modernized WAN architecture considers the unique security and operational requirements of these stakeholders. When fully implemented, the CPN will replace the MDCN.

Figure 3 3 depicts a hierarchical view of CMS' Modernized WAN infrastructure that will serve these stakeholders.

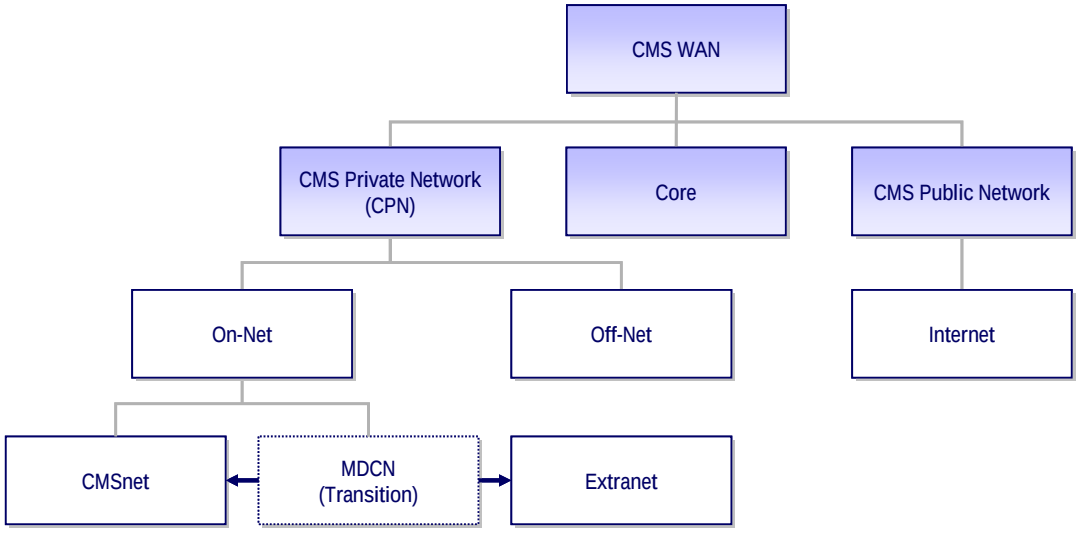

Figure 3. Modernized WAN Infrastructure: Hierarchical View

The heart of the Modernized WAN is the CMS Core Network that connects the Data Centers. The CMS Core Network consolidates the Data Centers into a virtual data center that hosts the e-Business applications, which the stakeholders access over the On-Net and Off-Net components of CPN and the public Internet.

The **CMS Private Network** will support both On-Net Business Partners and Off-Net Business Partners. The ONBPs will reside on **CMSnet** and have direct access to CMS applications via secure managed network services. The OFBPs will reside on the **Extranet** that is isolated from CMSnet (On-Net) and will connect via a gateway that resides at an EDC on the CMS Core Network.

ONBPs are business partners that conduct business in high volumes with CMS and hence have a high level of interaction with CMS. For example, future Medicare Administrative Contractors (MAC) and CMS Regional Offices are considered ONBPs. A MAC will be considered a single entity and connect to the CMSnet via highly secure Network-to-Network Interconnections (NNI). A MAC will be responsible to provide and manage connectivity to all its locations using this NNI connection. This gives the MACs greater control of operations on their network and provides clear accountability to CMS.

OFBPs are business partners that conduct business in relatively lower volumes and have a lower level of interaction with CMS. For example, the FIs and Carriers are considered OFBPs. OFBPs will purchase their managed service from a CMS-authorized distribution partner that owns and operates these Extranet gateways in accordance with CMS' standards and guidelines.

As part of the CMS WAN Modernization strategy, OIS will work with CMS business owners to define the policies that categorize business partners as ONBPs or OFBPs. All business partners now on the MDCN will transition eventually to CMSnet if they are categorized as an ONBP. Similarly, business partners on the MDCN will transition to the Extranet, if they are categorized as an OFBP.

Public Internet access is the final WAN service provided as part of the Modernized WAN. Internet access may be inbound or outbound. Beneficiaries and providers accessing a CMS application via the Internet use the inbound Internet access. CMS employees accessing the World Wide Web (WWW) use the outbound Internet access. CMS will isolate Internet traffic physically from the CPN and Core networks at all times and screen both inbound and outbound access.

2.5.5 WAN Interface to Multi-Zone Architecture

Three gateways serve as an interface to the applications that reside at the EDCs on the Core Network. The On-Net gateway interfaces with the CMSnet, HHSnet and MDCN, the Off-Net gateway interfaces with the Extranet and the Internet gateway interfaces with the Internet for inbound and outbound Internet access. A carrier managed Customer Edge (CE) router terminates the traffic from each network. All traffic then passes through an active IDP system before it accesses the services residing in the EDC Multi-Zone architecture.

All of the Zones are protected, at a minimum, by a layer of redundant and scalable traffic-filtering firewall security, which mediate all information flows among the Internet, On-Net and Off-Net. In addition, all traffic is monitored via redundant, active IDP systems and each system is configured in accordance with the *CMS TRA* and its Supplements. These Firewall and active IDP systems provide a concentration of security services, including, at a minimum, packet and protocol filtering, information hiding, and audit logging.

2.5.5.1 Customer Edge (CE) Router

The CE router is the entry point from the Internet, On-Net, or Off-Net into the CMS Multi-Zone architecture. All On-Net traffic and Off-Net traffic is encrypted by network layer (IP) site-to-site encryption using IPSec tunnels. In the case of the Internet, any encryption occurs at the transport layer (TCP) using SSL encryption that is Federal Information Processing Standard (FIPS) 140-2 compliant and NIST-validated encryption software.

The On-Net and Off-Net CEs terminate the circuits and the IPSec tunnels and direct the traffic into, and out of, and within the CMS networks. The CE is the last router that traffic traverses before it is routed to the Internet, On-Net, or Off-Net. Because all of CMS' traffic traverses this router, it functions as CMS' first and last line of defense through initial and final filtering.

2.5.5.2 Intrusion Detection and Prevention

Any incoming traffic to the CMS Production Environment must pass though the active IDP systems, depicted in Figure 2. This ensures that an attacker could only access the Customer Edge (CE) but no devices on the CPN. Redundant, active Netscreen IDP systems are deployed at the perimeter to thwart intrusions before they reach the standard UNIX Multi-Zone, legacy Windows Architecture Presentation Zone, and the Management Zone. In addition, redundant, active Netscreen IDP systems are deployed in the Management DMZ of the Management Zone to secure private vendor connections from their Vendor Management Networks.

2.5.5.3 Firewall

CMS requires that the redundant firewall security products deployed across all EDCs (and EDC4) and other CMS Production Environments must be Netscreen for the Presentation Zone, Checkpoint for the Application Zone, and PIX for the Data Zone. This requirement ensures that any unauthorized attempt to gain access to the Application Zone and/or the Data Zone will have to break through at least two different firewall security systems. The Netscreen firewall security system used to protect the Presentation Zone is complementary to the Checkpoint and PIX systems used to protect the Application Zone and Data Zone to ensure proper connectivity to and between the zones.

2.6 Global CMS Standards

2.6.1 Data Center Naming Convention

Table 1 provides the Data Center naming conventions that are to be used to ensure standard and effective communication between CMS, Production Environment Contractors, and all other parties. Consensus agreement on this global data center naming convention was achieved at the February 2007 EDC Summit.

Table 1. Data Center Naming Conventions

Data Center Name	Production Environment Contractor
EDC1	Electronic Data Systems (EDS) Corporation
EDC2	Companion Data Services (CDS), LLC
EDC3	International Business Machines (IBM) Corporation
EDC4	Lockheed Martin Corporation (CMS Baltimore Data Center)

2.6.2 Physical Separation of Switches

Virtual Local Area Networks (VLAN) are used at each level in the standard CMS Multi-Zone Architecture. That is, CMS has approved intra-zonal VLANs if the EDC Contractors employ a

set of physical switches at each zone. Inter-zonal VLANs are not to be used without explicit written approval from the CMS CTO.

2.6.3 Infrastructure—Dedicated Versus Shared Components

A key aspect of the CMS Production Environment is the combination of dedicated components and shared components and dedicated and shared *capabilities*. CMS defines dedicated components as those that are provided exclusively for CMS Production Environment infrastructure use.[1] All other components that may be shared with other data center customers are considered shared components. The Shared System infrastructure includes, but is not limited to, Firewalls, Network-based IDS/IDP, Host-based IDS, Identity Management, Monitoring, File Transfer, WAN Connectivity (routers and switches), Backup, DNS, and SAN Storage services.

The Government reserves the right to gain login access for administrative or repair purposes on any dedicated component in the Production Environment through a Firecall process. The Government will define the Firecall process and provide it to the Production Environment Contractors following contract award.

CMS defines dedicated *capability* within the CMS Production Environment as those components that are part of a mainframe processing infrastructure are to be dedicated to CMS rather than shared with other data center customers. CMS has determined that it is not acceptable to have Logical Partitions (LPAR) on the same mainframe machine used by other data center customers. The entire mainframe computing resource must be dedicated to CMS.

2.6.4 Mid-Tier Server and Firewall Ports

Each mid-tier server in the CMS Production Environments is provisioned with a minimum of two (2) physical Network Interface Cards (NIC). Five (5) interface ports are configured on the NIC cards and dedicated for connectivity to the Production, Backup, and Security and Management Networks. Two (2) interface ports are dedicated to Production Network connectivity and are not configured on the same NIC card. The only exception to this NIC configuration is that servers in the Management Zone do not require a dedicated port for Production connectivity. A sixth interface port can be configured on either NIC card for the purpose of "console" or "lights out" management by the Production Environment Contractors. However, the sixth interface port may not be necessary for those servers with dedicated DRAC/ALOM interface cards.

Each firewall in the CMS Production Environments is provisioned with a minimum of one (1) NIC card and four (4) interface ports that are dedicated for connectivity to the Production and Security and Management Networks. Two (2) of these interface ports are dedicated to Production Network connectivity. Each firewall provides automatic fail over and load balancing.

[1] For example, all routers and switches internal to the CMS LAN infrastructure must be dedicated to CMS, but the border router (or gateway router) providing connection to an ISP can be shared with other data center customers.

2.7 Infrastructure Security Considerations

Any server operating system (i.e., Solaris, Windows 2000/2003), routers, switches, databases and other infrastructure components must be configured in accordance with the applicable National Security Agency guidelines on vulnerabilities and guidelines provided by the *CMS TRA* and its Supplements, the *CMS Information Security Acceptable Risk Safeguards* and NIST Special Publications, including but not limited to NIST SP 800-7 and 800-26 as applicable.

All web servers or proprietary applications must be configured in accordance with National Security Agency guidelines on secure web site configurations. All web servers or proprietary applications must implement SSL 3.0 or TLS 1.0 with the approved cryptographic modules that ensure CMS is in compliance with, at a minimum, NIST SP 800-52 and FIPS 140-2.

The Department of Health & Human Services (HHS) has also published minimum security configurations for infrastructure platforms and devices for which compliance is mandatory. All EDCs and other business partners must be able to measure their ongoing compliance with the baseline configuration requirements. The use of automated tools to track compliance is the preferred method although manual methods may be acceptable for infrastructure components for which the number of devices is limited. Whether automated or manual methods are used, documentation to demonstrate ongoing compliance must be maintained including actions taken to conform to the standard.

3. CMS Infrastructure Services

Infrastructure Services are those core services that are used by applications in the CMS Production Environments to facilitate communications and common tasks throughout the CMS network. The Infrastructure solutions addressed in this section are not all inclusive and provide the foundation for CMS Production Environment deployments.

To assist in implementations, Table 2 presents a matrix of the infrastructure services offered in the Presentation, Application, Data, and Management Zones. In addition, the infrastructure services listed in Table 2 align to the *Service Access and Delivery*, *Service Platform and Infrastructure, and Component Framework* FEA TRM Service Areas.

Table 2. CMS Infrastructure Services Overview

CMS TRA Service Category	CMS TRA Service Solution Category or Approved Product	Presentation Zone	Application Zone	Data Zone	Management Zone
Database Services	DB2	**No**	**No**	**Yes**	**No**
Database Services	Oracle	**No**	**No**	**Yes**	**No**
Database Services	Sun Directory Server	**No**	**No**	**Yes**	**No**
Storage Services	SAN Storage	**Yes**	**Yes**	**Yes**	**Yes**
DNS Services	DNS Resolution	**Yes**	**Yes**	**Yes**	**Yes**
DNS Services	DNS Server	**Yes**	**No**	**No**	**Yes**
Security Services	IPSec VPN	**Yes**	**No**	**No**	**Yes**
Security Services	Firewall	**Yes**	**Yes**	**Yes**	**Yes**
Security Services	Intrusion Detection	**Yes**	**Yes**	**Yes**	**Yes**
Security Services	Intrusion Prevention	**Yes**	**Yes**	**Yes**	**Yes**
Security Services	Authentication & Authorization	**Yes**	**Yes**	**Yes**	**Yes**
Security Services	PKI Certificate Authority	**No**	**No**	**No**	**Yes**
Security Services	Host-based IDS	**Yes**	**Yes**	**Yes**	**Yes**
Security Services	Auditing	**Yes**	**Yes**	**Yes**	**Yes**
Backup/Restore Services	Backup/Restore Client	**Yes**	**Yes**	**Yes**	**Yes**
	Backup/Restore Server	**No**	**No**	**No**	**Yes**
Monitoring Services	Performance Management & Fault Monitoring	**Yes**	**Yes**	**Yes**	**Yes**
Content Deployment Services	RepliWeb MKS Endeavor	**Yes**	**Yes**	**Yes**	**Yes**

The following subsections address the Database Services, Storage Services, Domain Name Services, Security Services, Backup/Restore Services, Monitoring Services and Content Deployment Services that comprise Production Environment Infrastructure Services.

3.1 Database Services

Database Services are located in the Data Zone as required by the standard CMS Multi-Zone Architecture. Database Services consist of DB2, Oracle, and Lightweight Directory Access Protocol (LDAP) solutions. The CMS CTO must approve any waiver from these database standards.

3.2 Storage Services

Storage Services are available to servers in the Presentation, Application, Data, and Management Zones within the standard CMS Multi-Zone Architecture. Storage Services consist of Storage Area Network (SAN) solutions. SAN frames are physically located in the Management Zone and logical partitions are allocated through dedicated switches to servers in the Presentation, Application, Data, and Management Zones. The CMS CTO must approve any waiver from these storage standards.

3.3 Domain Name Services

The Domain Name Services are available to the Internet, Private Network, EDC4 Intranet, other CMS Production Environments, and the Production Presentation, Application, Data, and Management Zones within the standard CMS Multi-Zone Architecture. External DNS servers are physically located in the Presentation Zone for servicing resolution of connections originating from the Private Network, EDC4 Intranet, or other CMS Production Environments. Internal DNS servers are located in the Management Zone for servicing internal resolution of connections originating in the CMS Production Environment (i.e., Presentation, Application, Data, and Management Zones). The CMS CTO must approve any waiver from these DNS standards.

3.4 Security Services

The Security Services within the standard CMS Multi-Zone Architecture consist of IPSec VPN, Firewalls, Network-based IDS/IDP, Host-based IDS, Authentication & Authorization Services, Public Key Infrastructure and Auditing. These Security Services comply with the *CMS TRA* and its Supplements and NIST SP 800-35.

3.4.1 IPSec VPN Services

IPSec VPN services are located in the Presentation and Management Zones within the standard CMS Multi-Zone Architecture. The CMS CTO must approve any requested waiver from these IPSec VPN standards. These IPSec VPN Services comply with the *CMS TRA* and its Supplements and NIST SP 800-77.

3.4.2 Firewall Services

Firewall Services are located in the Presentation, Application, Data, and Management Zones within the standard CMS Multi-Zone Architecture. All firewall implementations provide a concentration of security services that include, at a minimum, packet and protocol filtering, information hiding, and audit logging. All firewalls filter traffic based on, at a minimum, source address, destination address, source port, destination port, transport layer protocol, interface on which traffic arrives and departs, and service in accordance with the security policies established by CMS through, but not limited to, the *CMS TRA* and its Supplements and NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002. The CMS CTO must approve any waiver from these firewall standards.

3.4.3 Intrusion Detection System / Intrusion Prevention System Services

The Government requires the use of two types of Intrusion Detection Systems: Network-based IDP/IDS and Host-based IDS. Network-based intrusion detection helps to detect probes, scans, or attacks by monitoring traffic flowing thorough a network environment. Host-based intrusion detection provides information regarding security attacks against servers by detecting suspicious activity in the servers' operating system, applications, and related processes.

IDP Services are located in front of all Zones in the standard and legacy CMS Multi-Zone Architecture as well as in the Management Zone. IDS Services are located in the Presentation, Application, and Data Zones within the standard and legacy CMS Multi-Zone Architecture. These services consist of network and host-based IDS and network-based IDP solutions. The CMS CTO must approve any waiver from these IDS/IDP standards.

Intrusion *Detection* sensors watch for predefined signatures of malicious events, and are able to perform statistical and anomaly analysis. When IDS sensors detect suspicious events, they alert in several different ways, including email, paging, or simply logging the occurrence. The Intrusion Detection sensors report to a central database in the Management Zone that correlates their information for viewing the network from multiple points.

Intrusion *Prevention* sensors detect and thwart computer attacks against protected resources. The Intrusion Prevention sensors defend the target without system administrator direct involvement. Such protection involves using signature-based or behavioral techniques to identify an attack and then blocking the malicious traffic or system call before it causes harm. In essence, the Intrusion Prevention sensors combine the functionality of a firewall and IDS to offer a solution that automatically blocks offending actions as soon as it detects an attack.

All network-based IDP/IDS and host-based IDS Services comply with the security policies established by CMS through, but not limited to, the *CMS TRA* and its Supplements, NIST SP 800-41, and NIST SP 800-94.

3.5 Backup/Restore Services

The Backup/Restore Services are available to the Presentation, Application, Data, and Management Zones within the standard CMS Multi-Zone Architecture. Backup/Restore Services consist of tape backup solutions and tape archive solutions. Backup clients are located on the Presentation, Application, Data, and Management Zones components and servers. Backup servers are located in the Management Zone for servicing these backup clients. The CMS CTO must approve any waiver from these backup standards.

3.6 Infrastructure Monitoring Services

The Production Environment Contractor provides infrastructure PM/M services for monitoring operational availability, problems/incidents, performance/service level, and capacity utilization of the production environment systems. The Production Environment Contractor's PM/M collates incidents/events and presents them within a single integrated dashboard display.

Monitoring Services are available to the Presentation, Application, Data, and Management Zones within the standard CMS Multi-Zone Architecture. Monitoring Services consist of application, network and host monitoring solutions for infrastructure Performance Management data collection and Fault Monitoring. Monitoring agents are installed on servers in the Presentation, Application, Data, and Management Zones. Network and host monitoring servers are located in the Management Zone for receiving events from the monitoring agents. The CMS CTO must approve any waiver from these monitoring standards.

3.7 Content Deployment Services

Content Deployment Services are located in the Presentation and Management Zone and service the Presentation, Application, Data, and Management Zones within the standard CMS Multi-Zone Architecture. Content Deployment Services consist of RepliWeb, MKS, and Endevor solutions for deploying CMS data and applications. RepliWeb and MKS are used for content deployment to mid-tier servers and Endevor is used for content deployment to mainframe servers. The CMS CTO must approve any waiver from these content deployment standards.

3.8 Infrastructure Service Security Considerations

Any infrastructure services that reside in the standard CMS Multi-Zone Architecture must be configured in accordance with the applicable National Security Agency guidelines on vulnerabilities and guidelines provided by the *CMS TRA* and its Supplements, *CMS Information Security Acceptable Risk Safeguards*, and NIST Special Publications, including but not limited to NIST SP 800-26 and 800-35 as applicable.

4. CMS Application Services

Application Services are those services that applications in the Production Environments use to facilitate communications and common tasks for business logic throughout the CMS network.

To assist in implementations, Table 3 presents a matrix of application services offered in the Presentation, Application, Data, and Management Zones. The Applications addressed in this section are not all inclusive and provide the foundation for CMS Production Environment deployments. The application services listed in Table 3 align to the *Service Access and Delivery*, *Service Platform and Infrastructure, Component Framework, and Service Interface and Integration* FEA TRM Service Areas.

Table 3. CMS Application Services Overview

CMS TRA Service Category	CMS TRA Service Solution Category or Approved Product	Presentation Zone	Application Zone	Data Zone	Management Zone
Web Services	IBM HTTP Server	**Yes**	**No**	**No**	**No**
Web Services	Sun JES Web Server	**Yes**	**No**	**No**	**No**
Web Services	XML Firewall Appliance	**Yes**	**No**	**No**	**No**
Middleware Services	IBM WebSphere Application Server	**No**	**Yes**	**Yes**	**No**
Middleware Services	IBM WebSphere MQ	**No**	**Yes**	**Yes**	**No**
Middleware Services	WBI Broker	**No**	**Yes**	**Yes**	**No**
File Transfer Services	Connect:Direct	**No**	**No**	**Yes**	**No**
File Transfer Services	GENTRAN	**Yes**	**Yes**	**Yes**	**No**
Security Services	IACS	**Yes**	**Yes**	**Yes**	**Yes**
Monitoring Services	Performance Management & Fault Monitoring	**Yes**	**Yes**	**Yes**	**Yes**

The following subsections address the Web Services, Middleware Services, File Transfer Services, Security Services, and Monitoring Services that comprise Production Environment Application Services.

4.1 Web Services

Web Services are located in the Presentation Zone. Web Services consist of IBM HTTP Server, Sun JES Web Server, and XML Firewall Appliance solutions. Further Web Services specificity can be found in the *CMS TRA – Web Services Supplement.* The CMS CTO must approve any waiver from these Web Services standards. These Web Services must comply with the *CMS TRA* and NIST SP 800-44.

4.2 Middleware Services

Middleware Services are located in the Application and Data Zones. Middleware Services consist of IBM WebSphere Application Server, WebSphere MQ, and WBI Broker solutions. The CMS CTO must approve any waiver from these Middleware Services standards.

4.3 File Transfer Services

File Transfer Services are located in the Presentation, Application, and Data Zones within the standard CMS Multi-Zone Architecture. File Transfer Services consist of the Connect:Direct and GENTRAN solutions. The CMS CTO must approve any waiver from these File Transfer Services standards.

4.4 Application Monitoring Services

The Production Environment Contractor provides application PM/M services for monitoring operational availability, problems/incidents, performance/service level, and capacity utilization of the CMS Production Environment applications/workloads. The Production Environment Contractor's PM/M collates incidents/events and presents them within a single integrated dashboard display.

Monitoring Services are available to the Presentation, Application, Data, and Management Zones within the standard CMS Multi-Zone Architecture. Monitoring Services consist of network and host monitoring solutions for application Performance Management data collection and Fault Monitoring. Monitoring agents are installed on servers in the Presentation, Application, Data, and Management Zones. Monitoring servers are located in the Management Zone for receiving events from the monitoring agents. The CMS CTO must approve any waiver from these monitoring standards.

4.5 Security Considerations for Application Services

Any application services that reside in the standard UNIX Multi-Zone Architecture must be configured in accordance with the applicable National Security Agency guidelines on vulnerabilities and guidelines provided by the *CMS TRA* and its Supplements, the *CMS Information Security Acceptable Risk Safeguards*, and NIST Special Publications, including but not limited to NIST SP 800-26 and 800-35 as applicable.

Appendix A. CMS Products / Standards Selection List

CMS originally developed and codified the CMS Infrastructure Product Selection list in the *CMS Target Architecture*. The CMS Product Selection list, as shown in Table 4, establishes standards for the selection and deployment of products into the standard CMS Multi-Zone Architecture. Each product standard in the CMS Product Selection list is aligned to an FEA TRM Service Area and Service Category. The CMS CTO must approve any waiver to the CMS Product Selection List.

Table 4. CMS Product Selection List for CMS Technology Architecture

FEA TRM Service Area	FEA TRM Service Category	Utilities and Services	Mainframe Products / Standards	Mid-Tier Products / Standards
Service Access and Delivery	Service Requirements	Health Standard Interoperability	HIPAA Transactions, CHI-adopted Standards	HIPAA Transactions, CHI-adopted Standards
Service Access and Delivery	Service Transport	Network Transport	TCP/IP	TCP/IP
Service Access and Delivery	Service Transport	File Transfer	Sterling Connect:Direct (4.4)	Sterling Connect:Direct (3.6.0.2), GENTRAN Integration Suite (4.0.3 Patch 20)
Service Platform and Infrastructure	Support Platforms	Operating System	IBM z/OS (1.7)	Sun Solaris 10 using Containers
Service Platform and Infrastructure	Support Platforms	Programming Language	Java (1.4), COBOL (3.4)	Java (1.4.2_04)
Service Platform and Infrastructure	Support Platforms	File System Management	N/A	Veritas Volume Manager (4.0)
Service Platform and Infrastructure	Support Platforms	Clustering	N/A	SUN Clustering
Service Platform and Infrastructure	Delivery Servers	“Application Zone” Server	IBM WebSphere for z/OS (5)	IBM WebSphere (5.1) for Sun (5.1.1)
Service Platform and Infrastructure	Delivery Servers	“Presentation Zone” Web Server	N/A	IBM HTTP Server (6.0),
Service Platform and Infrastructure	Software Engineering	Java Developer Tools	N/A	J2EE SDK, Eclipse-based IDEs
Service Platform and Infrastructure	Software Engineering	Data Modeling – Logical and Physical	N/A	ALLFusion ERwin Data Modeler (4.1.4.4224)
Service Platform and Infrastructure	Software Engineering	Modeling Language	N/A	IDEF1X, UML (2.0)
Service Platform and Infrastructure	Software Engineering	Enterprise Architecture	N/A	Troux 7
Service Platform and Infrastructure	Software Engineering	Requirements Management	N/A	DOORS (7.1)
Service Platform and Infrastructure	Software Engineering	Test Tools	Expeditor – TSO (7.3), Expeditor – CICS (8)	Quality Center (9.0), LoadRunner (8.1), ITCAM (6.1)
Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Endevor (4)	MKS Integrity Solution (2006)

FEA TRM Service Area	FEA TRM Service Category	Utilities and Services	Mainframe Products / Standards	Mid-Tier Products / Standards
Service Platform and Infrastructure	Software Engineering	Monitoring	Tivoli	Cisco Works, Tivoli
Service Platform and Infrastructure	Software Engineering	Job Scheduling	IBM Tivoli Workload Scheduler for z/OS (8.2)	IBM Tivoli Workload Scheduler (8.2)
Service Platform and Infrastructure	Database / Storage	Database Management System (DBMS)	DB2 (8)	Oracle 10g (10.2.0.3), Teradata (V2R6.02-MP RAS 3.03.01)
Service Platform and Infrastructure	Database / Storage	DBMS Tuning	BMC Tools	Oracle Enterprise Manager (10.2.0.1), Teradata Utilities (8.1) & SMM
Service Platform and Infrastructure	Database / Storage	SAN Storage Management	Hitachi, SMS (1.7)	Hitachi, SUN SAN Storage Foundation Suite (4.0)
Service Platform and Infrastructure	Database / Storage	Backup	SMS (1.7)	Veritas NetBackup (5.1 MP5)
Component Framework	Security	Network Authentication/Access	RACF (1.7)	Java Enterprise LDAP (3.0) (Sun ONE) or LDAP Proxy (5.2 Patch 2)
Component Framework	Security	LDAP Authentication	N/A	Java Enterprise LDAP (Sun ONE) (3.0) or LDAP Proxy (5.2 Patch 2)
Component Framework	Security	Identification and Authentication	RACF (1.7)	SUN Identity Manager (6.0), SUN Access Manager (6.0)
Component Framework	Security	Authorization/Logical Access Control	RACF (1.7)	TBD
Component Framework	Security	PKI Certificate Authority	N/A	TBD
Component Framework	Security	Anti-virus software	N/A	McAfee for Solaris
Component Framework	Business Logic	Data Model Management	N/A	MITI Meta Integration Repository (MIR) (5.1)
Component Framework	Business Logic	Content Management/ Unstructured Data	N/A	IBM Content Manager (8.3), IBM Document Manager (8.3), Kofax Ascent Capture (7.5), Kofax Ascent Capture Internet Server (7.5)
Component Framework	Data Interchange	Metadata Integration and Repository Tool	N/A	MITI Meta Integration Repository (MIR) (5.1)
Component Framework	Data Management	Information Intelligence, Analysis, Report and Management Tools	SAS (8.2), QMF (8)	Cognos ReportNet (1.1 MR3), MicroStrategy (8.0.2) (for large databases)
Component Framework	Data Management	Statistical Analyses	SAS (8.2)	SAS (9.1.3)
Component Framework	Data Management	Extract, Transform, Load (ETL)	IBM Utilities, BMC Unload (7.2), Informatica PowerCenter (8)	Informatica PowerCenter (8)

FEA TRM Service Area	FEA TRM Service Category	Utilities and Services	Mainframe Products / Standards	Mid-Tier Products / Standards
Service Interface and Integration	Integration	Database Access Language	QMF (8), SAS (8.2)	SQL 92
Service Interface and Integration	Integration	Database Connection	IBM WebSphere MQ (6.1)	IBM WebSphere MQ (6.1), JDBC
Service Interface and Integration	Integration	Messaging	IBM WebSphere MQ (6.1), WebSphere Business Integration (WBI) (5.3)	IBM WebSphere MQ (6.1), WebSphere Business Integration (WBI) (5.0 CSD07)
Service Interface and Integration	Interoperability	Data Interoperability	N/A	XML & XML Schema (3.3.0.16 Build 119589), SOAP, WSDL

Acronyms

ALOM	Advanced Lights Out Manager
ATM	Asynchronous Transfer Mode
BCC	Beneficiary Contact Centers
BDC	Baltimore Data Center
BIND	Berkeley Internet Name Daemon
BR	Border Router
C&A	Certification & Accreditation
CE	Customer Edge
CEI	Common Enterprise Infrastructure
CHI	Consolidated Health Informatics
CIO	Chief Information Officer
CMS	Centers for Medicare & Medicaid Services
CONOPS	Concept of Operations
CPE	Customer Premises Router
CPN	CMS Private Network
CTO	Chief Technology Officer
CWF	Common Working File
DLSw+	Data-Link Switching Plus
DMZ	Demilitarized Zone
DNS	Domain Name Service
DRAC	Dell Remote Access Card
EDC	Enterprise Data Center
EDC4	Subset of the Baltimore Data Center (BDC)
ERP	Engineering Review Panel
FA	Fiscal Agent
FEA	Federal Enterprise Architecture
FFRDC	Federally Funded Research and Development Center
FFS	Fee-for-Service
FI	Fiscal Intermediary
FIPS	Federal Information Processing Standard

FW	Firewall
HPMS	Health Plan Management System
HTML	Hypertext Markup Language
IDE	Integrated Development Environment
IDP	Intrusion Detection & Prevention
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPAR	Logical Partition
MAC	Medicare Administrative Contractors
MDCN	Medicare Data Communications Network
MIS	Managed Internet Services
MPLS	Multi-Protocol Label Switching
NDW	National Data Warehouse (a.k.a. Call Center Data Warehouse)
NGD	Next Generation Desktop
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NNI	Network-to-Network Interconnections
OBP	Operational Business Partner
OIS	Office of Information Services
OMB	Office of Management and Budget
OS	Operating System
PHI	Personal Health Information
PITS	Professional Information Technology Services
PKI	Public Key Infrastructure
RACF	Resource Access Control Facility
RDBMS	Relational Database Management System
S/NOC	Security Operations Center/Network Operations Center
SAN	Storage Area Network

SLA	Service Level Agreement
SNA	Systems Network Architecture
SP	Special Publication
SP	Service Provider
SSL	Secure Sockets Layer
SW	Network Switch
TLS	Transport Layer Security
TRA	Technical Reference Architecture
TRM	Technical Reference Model
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAS	WebSphere Application Server
WBI	WebSphere Business Integration

List of References

1. *CMS Internet Architecture (Including Minimum Platform Security Requirements),* Document No. CMS-CIO-STD-INT01, July 2003.
2. *CMS Target Architecture,* Document No. CMS-CIO-STD-ARC01, September 2004.
3. *CMS Enterprise Messaging Infrastructure (Including Architecture, Standards and Implementation Requirements*), Document No. CMS-CIO-STD-INT02, December 2003.
4. *CMS Enterprise File Transfer (EFT) Infrastructure*, Version 1.1, Document No. CMS-CIO-STD-ARC02, June 2006 (updated October 2006).
5. *CMS Information Security Acceptable Risk Safeguards (ARS),* Version 3.1, April 24, 2008.
6. *Security in Open Systems*, NIST SP 800-7, July 1994.
7. *An Introduction to Computer Security: The NIST Handbook*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, October 1995.
8. *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication,* NIST SP 800-25, October 2000.
9. *Security Self-Assessment Guide for Information Technology Systems,* NIST SP 800-26, November 2001.
10. *Introduction to Public Key Technology and the Federal PKI Infrastructure,* NIST SP 800-32, February 2001.
11. *Guide to Information Technology Security Services,* NIST SP 800-35, October 2003.
12. *Guide for the Security Certification and Accreditation of Federal Information Systems,* NIST SP 800-37, May 2004.
13. *Guidelines on Firewalls and Firewall Policy*, NIST SP 800-41, January 2002.
14. *Guidelines on Securing Public Web Servers,* NIST SP 800-44, September 2002.
15. *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations,* NIST SP 800-52, June 2005.
16. *Recommended Security Controls for Federal Information Systems,* NIST SP 800-53, February 2005.
17. *Recommendation on Key Management*, NIST SP 800-57, August 2005.
18. *Guide to IPsec VPNs*, NIST SP 800-77, December 2005.
19. *Guide to Intrusion Detection and Prevention Systems (IDPS),* NIST SP 800-94, February 2007.
20. Request for Proposals for CMS Enterprise Data Centers Procurement, RFP No. CMS-2005-0003, Centers for Medicare & Medicaid Services (CMS), July 24, 2005.
21. *Concept of Operations for Wide Area Network Modernization,* Initial draft, Version 0.1, CMS, January 17, 2007.
22. NIST, *Security Requirements for Cryptographic Modules,* Federal Information Processing Standard 140-2, May 25, 2001.