Department of Health and Human Services

Centers for Medicare & Medicaid Services
IT Modernization Program

Cognos ReportNet Guidelines

Version 1.1

March 3, 2006

Table of Contents

List of Figures

List of Tables

1. Introduction

CMS is migrating to a three-zone, web-enabled, and secure infrastructure based on a standard set of criteria documented in the *CMS Internet Architecture*. Likewise, in the document *CMS Target Architecture*, CMS identifies a set of standard commercial off-the-shelf (COTS) products for new applications being deployed in the CMS Internet Architecture. CMS has selected Cognos ReportNet as one of the standard tools for creating and managing reports.

This document, *Cognos ReportNet Guidelines*, is one in a set of documents aimed at providing architecture-compliant recommendations for successful integration of COTS-based applications into the CMS Internet Architecture. This document addresses specific recommendations for the deployment of Cognos ReportNet into the CMS Internet Architecture.

To the extent practical, the guidance provided in this document tries to prescribe specific implementation detail and conventions, but it is by no means all inclusive, and where appropriate should be adapted to individual projects based on the cost, complexity, and criticality of the proposed solution.

The *Cognos ReportNet Guidelines* are intended for teams involved in system development, for project managers, and for the CMS IT offices, government contractors, and product vendors participating in the COTS product reviews.

2. Cognos ReportNet Architecture

Cognos ReportNet is a Web product for creating and managing ad hoc and managed reports. ReportNet is built on a services-based architecture allowing its components to be distributed across multiple servers in a three-zone architecture that corresponds to the CMS Internet Architecture:

- Presentation Zone – provides presentation services to users who interface with a Cognos-based application from a web browser.
- Application Zone – contains the business and control logic for the applications and services.
- Data Zone – consists of content store and data servers.

Cognos' flexible, three-tier architecture ensures fail-over protection and dynamic load balancing for high availability. The zones are separated by firewalls and ReportNet user interfaces sit above the zones as shown in Figure 1.

ReportNet components communicate with each other, and with any additional products integrated with ReportNet, using the Cognos business intelligence (BI) Bus API protocol. The BI Bus API is an open, documented API based on Web Services Definition Language (WSDL) and Simple Object Access Protocol (SOAP).

Figure 1 depicts the three-zone ReportNet architecture and user interfaces.

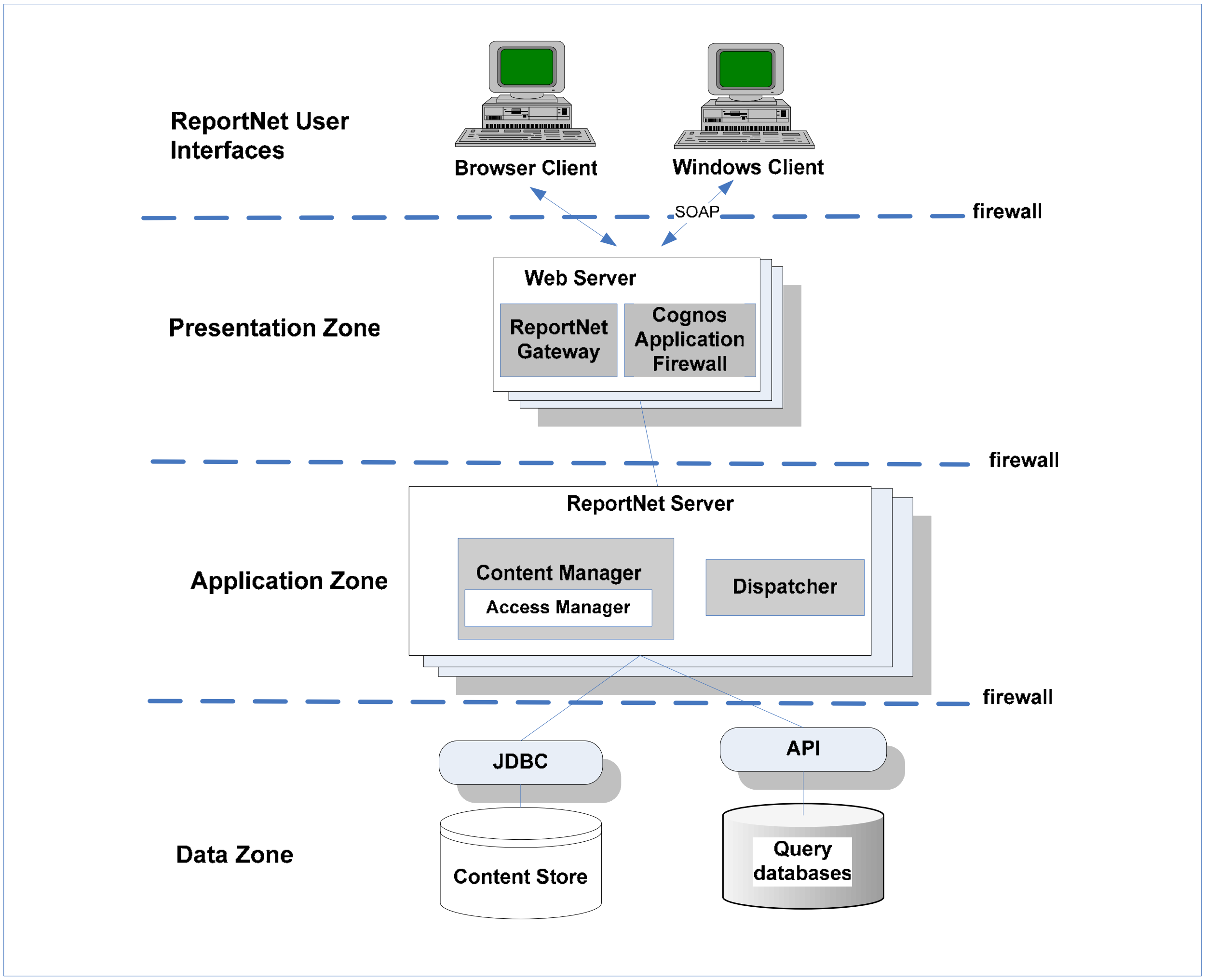

Figure 1: Recommended Cognos ReportNet Architecture

Presentation Zone

The Presentation Zone contains the Cognos Application Firewall and one or more ReportNet gateways. The gateways support all Web communications in ReportNet. Several types of Web gateways are supported, including CGI, ISAPI, apache-mod, and servlet.

Application Zone

Within the Application Zone, the ReportNet Servers handle requests, such as reports and queries, and manage ReportNet information. The ReportNet server consists of a number of processes, each specializing in a specific task related to report management and operation. Some of these processes are written in Java to facilitate integration with external applications and others are written in C++ to facilitate performance.

Each ReportNet installation includes a Dispatcher. The Dispatcher operates all ReportNet services configured and enabled on the ReportNet Server, routes requests, and distributes configuration changes. The services managed by the Dispatcher include the presentation service, batch report and report services, job and schedule monitoring service, and log service. The technology underlying the ReportNet Server consists of:

- A Java application server running the Dispatcher Java servlet.
- A non-Java component based on C++: The batch report and report services are native C++ applications that run as separate processes. The Dispatcher communicates with the report service using a port acquired at run time.

Figure 2 depicts the ReportNet Server configuration in the Application Zone.

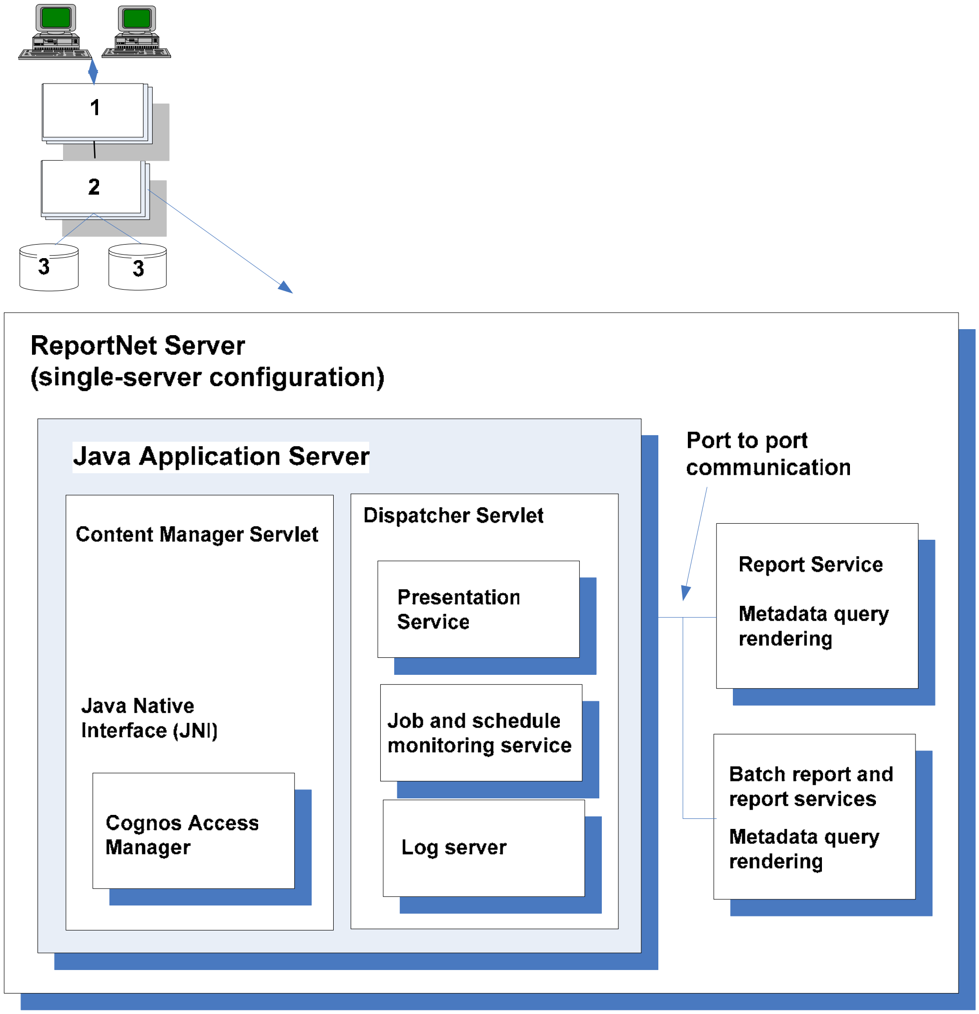

Figure 2: Recommended ReportNet Server Configuration

Each ReportNet installation also includes the Content Manager. The Content Manager stores and manages ReportNet information. The Content Manager, which is a Java servlet, contains Cognos Access Manager, the primary security component of ReportNet. The Content Manager servlet communicates with Cognos Access Manager through a Java Native Interface (JNI). The

Cognos Access Manager can leverage an organization's existing security server, such as Lightweight Directory Access Protocol (LDAP) authentication directory, to perform user authentication.

Figure 3 shows additional detail for the Content and Access Managers.

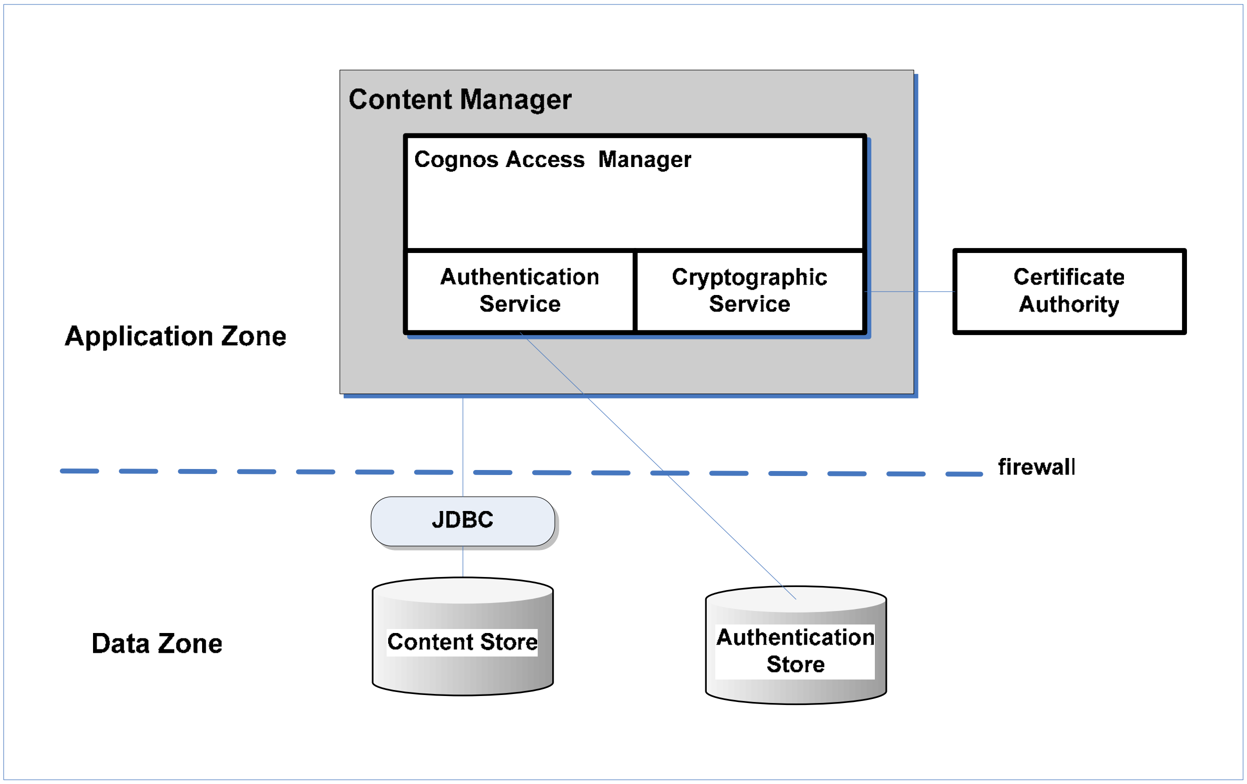

Figure 3 Content and Access Managers

Data Zone

The Data Zone contains the Content Store, which is an Oracle or IBM DB2 UDB relational database management system (DBMS). The Content Store is used by the Content Manager to store all ReportNet information, managed by Cognos Connection or an existing enterprise portal. The Content Manager uses Java Database Connectivity (JDBC) API to access the Content Store. The Content Store contains information about packages, folders, reports, saved results, directories, server configurations, and ReportNet deployment.

Any query databases located in the Data Zone are accessed by the report services located in the Application zone access using native APIs or ODBC.

2.1 ReportNet User Interfaces

ReportNet user interfaces include the following:

- Web-based Cognos Connection, Cognos, Report Studio, and Query Studio

- Windows-based Framework Manager

Cognos Connection is a Web portal that comes with ReportNet. Cognos Connection provides a single point of entry to ReportNet for creating, running, viewing, scheduling, organizing, and distributing reports as well as for performing administrative tasks.

Users can run Cognos Report Studio and Query Studio through Cognos Connection. In addition, ReportNet's open architecture enables organizations that have already implemented an enterprise-wide portal solution to integrate ReportNet portal into existing web portal products, such as the IBM WebSphere Portal. Depending on the implementation strategy, organizations may choose to embed specific Cognos Connection functionality within an enterprise portal or access Cognos Connection from within the enterprise portal.

Cognos Query Studio and Report Studio are *zero footprint*, web-based products for creating reports. Query studio enables users with little or no training to design, create, and save ad hoc reports. Query Studio can present only one table or chart. Report Studio provides trained users with more flexible and capable mechanisms to create and edit a wide range of professional reports, as well as capability to edit and modify reports created in Query Studio.

Cognos Framework Manager is a Windows-based tool to create and manage business-related metadata for authoring reports in ReportNet.

3. J2EE Application Integration with Cognos ReportNet

Integration of J2EE applications with Cognos ReportNet is accomplished in several ways. For simple tasks, applications can communicate with ReportNet through URL commands. For more complex tasks, such as scheduling, Cognos provides the ReportNet Software Development Kit (SDK) API.

URL commands can be used with Report Viewer, Report Studio, or Query Studio, to run, view, and edit authored reports retrieved from the ReportNet content store.

URL commands can be used to

- view a previously run report in Report Viewer
- run a saved report, specifying different run options, and display it in Report Viewer
- open and edit an existing report in Report Studio or Query Studio
- pass environment variables from ReportNet to an external application

Typically, an application will dynamically construct URL commands with parameter values which are then embedded as links in web pages.

For more complex integration, the ReportNet SDK provides a platform-independent automation interface for working with ReportNet services and components. These ReportNet services and components are linked through the BI Bus, which issues calls and returns replies in the form of standard, Simple Object Access Protocol (SOAP) messages.

The SDK can be used to

- create and modify reports and queries
- administer, schedule, and deploy reports and other objects
- administer ReportNet servers
- administer Cognos groups and roles, and ReportNet access permissions
- authenticate users
- let other applications or Web portals interact directly with Cognos information content

The SDK can be used with any toolkit that conforms to SOAP 1.1, including a Java toolkit such as Axis. ReportNet includes a Java toolkit based on Apache Axis (http://xml.apache.org/axis/index.html).

To build SDK clients using the ReportNet Java toolkit, developer's can use the CMS standard J2EE development environment, WebSphere Studio Application Developer.

The following files will be needed for development:

- axis.jar
- axisReportNetClient.jar
- jaxrpc.jar

To run SDK clients using the ReportNet Java toolkit, the following files are needed:

- axis.jar
- axisReportNetClient.jar
- commons-discovery.jar
- commons-logging.jar
- jaxrpc.jar
- saaj.jar
- xml-apis.jar
- xercesImpl.jar

In general, a Java program will access ReportNet with the following steps:

1. Create a CognosReportNetServiceLocator object and a CognosReportNetPortType object to connect to a ReportNet server.
2. Use the ReportNet methods that are available through the CognosReportNetPortType object to work with ReportNet.

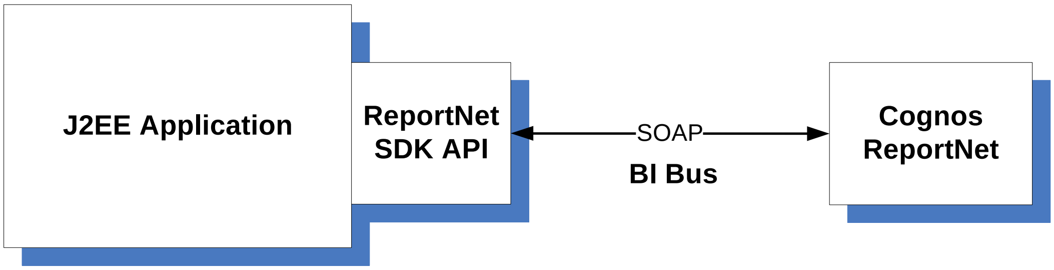

Figure 4: J2EE Application Integration with ReportNet SDK API

For more information on integrating J2EE applications with Cognos, see the *Cognos ReportNet Software Development Kit Developer Guide*.

4. Recommended Configuration

This section presents the recommended configuration for the deployment of Cognos ReportNet in a CMS Internet Architecture compliant implementation. The recommended configuration includes the hardware and software, gateways, security and data architectural components.

4.1 Hardware and Software Recommendations

Within the CMS Internet Architecture, ReportNet will run on the Sun Solaris platform and the server components can reside on one or multiple machines. Table 1 lists specific minimum hardware and software requirements for configuring Cognos ReportNet in a UNIX environment.

Table 1: Cognos System Recommendations for UNIX

Requirement	Recommendation
Operating System	Sun Solaris (recommended: file descriptor limit set to 1024)
RAM	Minimum: 512 MB Recommended: 1 GB
Disk Space	1 GB
Web Servers	IBM HTTP Server
Java Runtime Environment (JRE)	JRE installed with Java application server
Application Server	IBM WebSphere
Databases Supported	Oracle (version 8.1.7.2 or later if Oracle server is on a different OS from Cognos ReportNet) IBM-DB2
Web Browser	Internet Explorer only Cookies and JavaScript enabled

4.2 Component Recommendations

This section provides specific recommendations for the selection and configuration of ReportNet components within the CMS Internet Architecture.

Recommendation 1

Consider configuring Cognos ReportNet to use an alternate gateway that replaces the default CGI program in the Web server.

Rationale: All Web communication in ReportNet is through gateways residing on one or more Web servers. The Cognos ReportNet *Installation and Configuration Guide* states that the default CGI gateway can be used for all supported Web servers, but it delivers the slowest performance. Web server performance can be improved by configuring ReportNet to use an alternate gateway replacing the default CGI program. Cognos ReportNet supports several types of gateways as alternatives to the CGI gateway.

- Internet Server Application Programming Interface (ISAPI) - ISAPI can be used for the Microsoft Internet Information Services (IIS) Web server. It delivers faster performance for the IIS.
- Apache_mod - The apache_mod gateway can be used with Apache Web servers or IBM HTTP servers.
- Servlet - To use a servlet gateway, the Web server infrastructure must support servlets.

Of the alternatives for the ReportNet gateway, the preferred choice for the applications running in the CMS 3-Zone Architecture appears to be the apache_mod configured with the IBM HTTP server. The ISAPI gateway is not appropriate because IIS is not part of the CMS target architecture. The servlet gateway does not seem to be a good choice as it appears this would require installing a servlet container in the Presentation Zone. However, before a final choice is made for the ReportNet gateway, adequate performance testing should be conducted.

Recommendation 2

Install the Content Manager on a separate server for improved performance and locate it in the Data Zone for maximum security.

Rationale: As described in the Cognos ReportNet *Installation and Configuration Guide*, ReportNet can be configured with “Content Manager in the data tier for maximum security.” Installing the Content Manager on a separate server from the report servers can improve performance, availability, and capacity.

According to the installation guide, Content Manager can be installed separately from the ReportNet report servers if the application data contains sensitive information. The Content Manager can also be installed on a separate server if the program is managing large volumes of data. ReportNet scalability can be improved by increasing the size of the processor on which Content Manager is installed. Since the Content Manager is implemented as a Java servlet, a servlet container (e.g., WebSphere Application Server) would have to be installed to host the Content Manager on a separate server.

Recommendation 3

Configure Framework Manager to communicate through the Web server gateway.

Rationale: If a Web server other than Microsoft IIS is used, Cognos recommends that Framework Manager be configured to communicate through the Web server gateway. This eliminates the need to set up additional communications channels through the firewalls which separate Framework Manager, the Web server, and the ReportNet server.

4.3 Administration and Security Recommendations

This section provides recommendations for administration and security of the implementation of Cognos ReportNet.

Recommendation 4

The Cognos ReportNet should use the security framework offered by CMS LDAP services for user authentication to enable an integrated authentication mechanism for the CMS Architecture.

Rationale: Use of the CMS enterprise-wide LDAP services to perform user authentication for Cognos ReportNet application will enable a practical solution for user IDs and passwords for all CMS systems.

Recommendation 5

Use of role-based grouping to restrict users to certain metadata layers, individual reports, and data is strongly recommended. Rules that define roles or groups of users for authorization of report creation and viewing capabilities should be defined. The recommendation is to use the CMS LDAP authentication server to define and maintain the authorization rules and explore creative ways to have the ReportNet Access Manager read them.

Rationale: The definition and maintenance of roles or groups authorization rules for ReportNet-based applications within the LDAP server, where users are authenticated with their IDs and passwords, will minimize the problems of multiple sets of user IDs and passwords and the need to maintain them in sync.

Recommendation 6

Implementers should use great care to ensure that the basic security method of “least privileged” is enforced and users do not receive more permission than they are entitled.

Rationale: Cognos ReportNet can set permissions based on 3rd party credentials, such as a CMS LDAP centralized authentication server. Cognos ReportNet also gives users combined permissions of all the groups for which they have membership. In effect, user permissions are based on the combined permissions given to groups they are members of from groups defined in CMS LDAP authentication server as well as ReportNet groups. .

Users should not be given more permissions than is required to perform the functions of the job and/or their clearance level. Without set policies and procedures on group membership and permissions, the security mode of “least privileged” cannot be verified

Recommendation 7

All installations of Cognos ReportNet should use the highest encryption available, which in this product is 128 bit. Cognos ReportNet offers 56 bit encryption for data protection during transit as a base service, but it also offers 128 bit encryption as an add-on at an additional cost.

Rationale: As outlined in the CMS Internet Architecture, Section 5, 5.F.4, it is required that all applications secure traffic using 128 bit encryption as 56 bit encryption has been proven insecure in the past.

Recommendation 8

The Cognos ReportNet design should specify COTS configuration information to cross-reference the configuration settings necessary to maintain all hardware and software proposed in the technical architecture.

Rationale: A baseline configuration should be included in system designs to provide a starting point for the maintenance contractor.

Recommendation 9

The Cognos ReportNet system should be backed up frequently and needs strong assurances of availability. This could include load balancing, active/passive failover modes, and redundant installs of all parts of Cognos ReportNet.

Rationale: Cognos ReportNet based systems should be highly available to users, not affected by high traffic loads or faulty equipment. System design documentation should reflect periodic computer system backups of mission-critical data and archives to ensure the data is adequately preserved and protected against data loss and destruction.

Recommendation 10

Careful consideration on database security should be employed. Cognos does not have mechanisms in place to secure the back-end database from malicious or unintentional modification from the Cognos ReportNet front end. Therefore, the native security in the database should be used to restrict user’s access permissions. In addition, it is important to assign only trusted users to maintain the database.

Rationale: These assurances will protect the integrity and the health of the database. This recommendation will also ensure that users do not delete or corrupt entries or tables in the database in error.

Recommendation 11

Cognos by default supports anonymous user access. Disabling this feature is strongly recommended.

Rationale: CMS should only support authenticated users for ReportNet access. Support of anonymous users could potentially allow unauthorized users to view or modify sensitive data.

Acronyms

CGI	Common Gateway Interface
CMS	Centers for Medicare & Medicaid Services
COTS	Commercial Off-the-Shelf
DBMS	Relational Database Management System
IA	Internet Architecture
IIS	Internet Information Services
ISAPI	Internet Server Application Programming Interface
IT	Information Technology
JBDC	Java Database Connectivity
JNI	Java Native Interface
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
SDK	Software Development Kit
URL	Uniform Resource Locator

List of References

1. *CMS Internet Architecture,* CMS-CIO-STD-INT01, Centers for Medicare & Medicaid Services, July 2003.
2. *CMS Enterprise Messaging Infrastructure,* CMS-CIO-STD-INT02, Centers for Medicare & Medicaid Services, December 2003.
3. *CMS Web-Enabled Application Architecture*, CMS-CIO-STD-INT03, Centers for Medicare & Medicaid Services, March 2004.
4. *CMS Target Architecture*, CMS-CIO-STD-ARC01, Centers for Medicare & Medicaid Services, September 2004.
5. *Cognos ReportNet: The Next Generation of Enterprise Query and Reporting, A Cognos White Paper,* August 2003.
6. *Cognos Enterprise BI Series – Cognos ReportNet Installation and Configuration Guide,* Cognos Incorporated, 2004.
7. *Cognos Enterprise BI Series – Cognos ReportNet Administration and Security Guide,* Cognos Incorporated, 2004.
8. *Cognos Enterprise BI Series – Cognos ReportNet Architecture and Planning Guide,* Cognos Incorporated, 2004.
9. *Cognos Enterprise BI Series – Cognos ReportNet Software Development Kit Developer Guide*, 2004.