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

CMS Operational Policy for

VPN Access to 3-Zone Admin and Development /Validation Segments

January 9, 2008

Document Number: CMS-CIO-POL-VPN01-01

TABLE OF CONTENTS

1. PURPOSE

This document establishes an operational policy for remote access to the 3-Zone infrastructure at the Centers for Medicare & Medicaid Services (CMS) for the purpose of developing, testing/ validating, administering, and maintaining CMS IT systems and applications.

2. BACKGROUND

CMS shares data with a variety of business partners, contractors, and other federal agencies, through a number of remote access methods. CMS also provides remote access to its staff of general users including system administrative personnel, security personnel, system and application developers/maintainers, and Central and Regional Office staff and executive groups during normal and extended business hours.

The growth of the Internet and other networking technologies has introduced an increase in illicit activities, commonly known as cracking or hacking, targeted at computers and networks. The aim of this activity is to disrupt users and organizational communications, damage their systems, or obtain information to which the attacker is not entitled and the victim may wish to keep private. With the increasing visibility of such crime, new regulations have been passed requiring organizations to be more diligent in securing the data they possess. Organizations are recognizing the value of the data they possess and are increasingly searching for measures to keep it private and secure.

CMS information falls into the categories of Privacy Act-protected data, proprietary data, procurement data, inter-agency data, and privileged system information. CMS has a legal and practical responsibility to maintain the confidentiality, integrity, and availability of this information. Access to these types of information is controlled by the Privacy Act of 1974, the Computer Security Act of 1987, and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. In addition, various rules, regulations, policies and guidelines promulgated by the Department of Health and Human Services (DHHS), the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST) delineate required or preferred access controls.

The CMS Internet architecture is a “3-Zone” architecture with each “zone” separated by firewalls to support web application systems. The first or outermost zone supports web servers only and is called the “Presentation Region” or “De-Militarized Zone (DMZ).” The second or middle zone supports only business logic for the applications and is called the ‘Application Region.” The third or innermost zone, called the “Secure Region” or “Protected Region,” contains the database servers used by the web applications. Additional network segments exist to support specialized network services such as Public Key Infrastructure (PKI), Domain Naming Services (DNS), etc.

The CMS 3-Zone architecture also supports a development environment that mirrors the production environment to provide developers and some higher-privileged testers and validators with the full functionality of the production environment.

3. SCOPE

This operational policy applies to remote access to all CMS infrastructure devices, systems, and databases within the CMS 3-Zone architecture, which are controlled and operated by CMS or its designated IT Infrastructure Implementation Agent(s) or Contractor(s) at all Central and Regional Office locations (includes CMS Single Site, Lord Baltimore, Building 7111, Enterprise Data Centers (EDCs), and other offsite facilities). Security devices, systems, and databases controlled and operated by other CMS contractors not previously designated are not covered by this policy.

One of the groups requiring access to the CMS 3-Zone Admin Segment are administrators and network maintainers of Tier 2 systems located in the CMS 3-Zone network. This group will require access to appropriate 3-Zone systems through the Medicare Data Communications Network (MDCN), CMS Intranet, and/or the Internet. The group will include CMS contractors and selected CMS staff that administer and maintain CMS 3-Zone systems or applications.

A second group requiring access to the CMS 3-Zone Development and Validation Segments are developers, some higher-privileged testers and validators, administrators, and network maintainers of Tier 2 systems and applications located in the CMS 3-Zone Development and Validation environment. This group will require access to appropriate 3-Zone Development and Validation systems and applications through the MDCN, CMS Intranet, and/or the Internet. The group will include CMS contractors and selected CMS staff that develop, test/validate, administer, and maintain CMS 3-Zone systems or applications.

This policy does not supersede any other applicable law or higher level agency directive, or existing labor management agreement in effect as of the effective date of this policy.

4. POLICY

All CMS staff and contractors that administer and/or maintain CMS production systems or applications in the 3-Zone infrastructure must access the appropriate systems/applications through the 3-Zone Admin Segments using CMS Virtual Private Network (VPN) services.

All developers that develop, administer, test/validate, and/or maintain systems or applications in the CMS 3-Zone Development and Validation infrastructure must access the appropriate systems/applications through the 3-Zone Development and Validation Segments using CMS VPN services.

All such CMS staff and contractors shall be appropriately identified and must adhere to all applicable DHHS and CMS Information Security and Privacy policies, standards, and procedures. In addition, based on recent security changes instituted by OMB, plus the impact of Homeland Security Presidential Directive 12 (HSPD-12), CMS staff and contractors shall adhere to those regulatory requirements contained in documents listed in the reference section below, which are not as yet covered in CMS policy, standards, or procedures.

CMS contractors shall supply their own laptops/desktops that are CMS-approved and configured per CMS configuration requirements. Contractor laptops/desktops must have appropriate systems protection, configuration, and hardware/software as described in the appropriate CMS VPN configuration documentation, which will include, but not be limited to, full disk encryptions, anti-spyware, patch management, and anti-virus software.

All CMS-assigned laptops/desktops issued to CMS staff that access systems/applications through the 3-Zone infrastructure shall be converted to imaged VPN laptops/desktops.

Contractors and CMS staff shall install CMS-provided VPN software and shall procure a CMS-approved smartcard and VPN software with appropriate license for each laptop connecting to the CMS 3-Zone Infrastructure Admin Segment and/or Development Segment. In addition, a card reader/keyboard shall be procured for each desktop that is to be connected to the CMS 3-Zone Admin or Development Segments.

Contractors and CMS staff shall adhere to appropriate configuration requirements provided in CMS VPN configuration documentation.

A contractor's laptop/desktop must be a VPN-dedicated laptop/desktop or one with a separate bootable partition used solely for VPN access. No other VPN products shall be used on the same laptop/bootable partition as the installed VPN product.

No laptop/desktop that is connected to the CMS infrastructure shall be directly connected to a contractor's corporate network or to the Internet at the same time.

5. ROLES AND RESPONSIBILITIES

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

5.A. CHIEF TECHNOLOGY OFFICER (CTO)

CMS CTO is responsible for:

- Oversight of the CMS VPN program for access to CMS infrastructure and sensitive information; and
- Approval of all OIS operational documentation in support of VPN use within CMS.

5.B. OFFICE OF INFORMATION SERVICES (OIS) / ENTERPRISE DATA CENTER GROUP (EDCG)

OIS/EDCG is responsible for:

- Implementation of VPN solutions within CMS;
- Oversight and management of day-to-day VPN operations within CMS;
- Development and implementation of operational procedures and documentation in support of VPN operations within CMS;
- Coordination with CMS Components regarding process and procedures for use of VPN within CMS;
- Development, maintenance, and operation of Local Registration Authority (LRA) procedures for identity proofing VPN requestors; and
- Approval or rejection of VPN requests.

5.C. CMS IT Infrastructure Implementation Agent or Contractor

The CMS IT Infrastructure Implementation Agent or Contractor is responsible for:

- Developing and maintaining all procedure, configuration, support, and user documentation regarding CMS VPN access;
- Ensuring that all CMS-assigned laptops/desktops utilized by CMS staff are appropriately converted to imaged VPN laptops/desktops;
- Providing a VPN installation package with configuration instructions to CMS contractors;
- Providing VPN operations documentation to CMS staff and contractors;
- Providing an automated system for registering requestors, tracking approvals, and notification of requestors, approvers, LRAs, Government Task Leaders (GTLs), POCs, and appropriate contractor support staff; and
- Operating, maintaining, and controlling a Certificate Authority for CMS, to include the control, issuance and recovery of smartcards.

5.D. CMS COMPONENTS

CMS Components are responsible for:

- Identifying contractors and CMS staff that operate and maintain CMS systems or applications located in the CMS 3-Zone Infrastructure;
- Ensuring that VPN requests for identified contractors are appropriately processed and approved in accordance with CMS VPN procedures;

- Providing smartcards procured by contractors to the CMS IT Infrastructure Implementation Agent or Contractor for processing and subsequently issuing them to the appropriate requestor;
- Procure CMS smartcards and card readers through the CMS IT infrastructure catalog for CMS staff supporting 3-Zone Production and Development and Validation systems and applications; and
- Providing OIS/EDCG with a list of CMS Component POCs responsible for contracts that are involved with operation and maintenance of CMS systems or applications located in the CMS 3-Zone Infrastructure.

5.E. CMS STAFF AND CONTRACTORS

CMS Staff and Contractors are responsible for:

- Adhering to the requirements of this operational policy and all other applicable Government, DHHS, and CMS Information Security and Privacy policies, standards, and procedures;
- Installing and appropriately configuring all hardware and software (e.g., VPN client, anti-virus, anti-spyware, and encryption software) on laptops/desktops as required by CMS;
- Providing all CMS standard smartcards, software licenses, and smartcards/readers in accordance with CMS VPN procedures and configuration documentation;
- Configuring assigned laptop and VPN hardware (except smartcards) and software in accordance with the *Installation Guide for CMS SafeNet VPN Client for Windows XP*;
- Maintaining the system, security, and VPN software and configurations to prescribed CMS VPN standards and procedures, insuring that anti-virus, anti-spyware, and encryption software are updated regularly and compatible with CMS VPN systems.
- Applying for, securing, and maintaining a CMS-issued smartcard and PKI certificate per CMS documentation;
- Ensuring action is taken to notify the CMS Component when someone no longer requires VPN access, and recovering the laptop and smartcard; and
- Obtaining support directly from the CMS IT Infrastructure Implementation Agent or Contractor regarding connectivity issues and VPN client operation, maintenance, and compatibility with other software packages.

6. APPLICABLE LAWS/GUIDANCE

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

- OMB Circular A-130, Management of Federal Information Resources, November 30, 2000

- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006
- OMB Memorandum M-07-11, Implementation of Commonly Accepted Security Configuration for Windows Operating Systems, March 22, 2007
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
- NIST FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
- Homeland Security Presidential Directive-12, Office of the White House, August 27, 2004
- DHHS Information Security Program Policy, December 15, 2004
- CMS Policy for the Information Security Program, CMS-CIO-POL-SEC02, November 15, 2007
- CMS Policy for Privacy Act Implementation & Breach Notification, CMS-CIO-POL-PRIV01-01, July 23, 2007
- CMS Information Security Acceptable Risk Safeguards (ARS), Version 3.0, September 19, 2007

7. INFORMATION AND ASSISTANCE

Contact the Director of the Enterprise Data Center Group (EDCG) within the Office of Information Services (OIS) for further information regarding this operational policy.

8. EFFECTIVE DATE/IMPLEMENTATION

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

9. APPROVED

/s/

Julie C. Boughn
CMS Chief Information Officer and
Director, Office of Information Services

1/9/2008

Date of Issuance

10. ATTACHMENTS

The following documents augment this operational policy:

- Installation Guide for CMS SafeNet VPN Client for Windows XP

GLOSSARY

Local Registration Authority (LRA)

An operational entity that registers a user into the primary Registration Authority (RA). The LRA is responsible for identity proofing, enrolling, and removing requesters.

Public Key Infrastructure (PKI)

In cryptography, PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique for each CA. This is carried out by software at a CA, possibly under human supervision, together with other coordinated software at distributed locations. For each user, the user identity, the public key, their binding, validity conditions and other attributes are made unforgeable in public key certificates issued by the CA.

Tier 2 System

Mid-level, server-based system and appropriated network components that includes UNIX-based servers, Microsoft Windows-based servers, and/or Linux-based servers.

Virtual Private Network (VPN)

A system that allows strong authentication and encryption between a remote client and a gateway into an organization infrastructure.

3-Zone Admin Segment(s)

Network administrative segment(s) that are designed to provide private, secure communications for systems connected to the segment(s) to allow systems/DBA administrators or application administrators to perform technical services on the systems or applications for which they are responsible. The segment(s) are separate from the public infrastructure.