

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES



*Office of Information Services
Chief Information Officer*

CMS Internet Architecture

*(Including Minimum
Platform Security Requirements)*



July 2003



Document Number:
CMS-CIO-STD-INT01

TABLE OF CONTENTS

1. FOREWORD.....	1
2. EXECUTIVE SUMMARY	2
3. BACKGROUND	3
4. CMS INTERNET ARCHITECTURE	4
4.A. CONNECTIVITY VIEW	5
4.B. PROTOCOL VIEW	6
4.C. PROCESSING VIEW	7
4.D. HARDWARE/SOFTWARE VIEW.....	8
5. SECURITY REQUIREMENTS ADDRESSED BY THIS ARCHITECTURE	9
5.A. GENERAL	9
5.B. GENERAL ARCHITECTURE: LAYERED SECURITY.....	9
5.C. GENERAL ARCHITECTURE: SEGMENTED SECURITY	11
5.D. FIREWALL CONFIGURATION - (“DENY EVERYTHING” MODEL)	12
5.E. FIREWALL ADMINISTRATION	14
5.F. SECURE SOCKETS LAYER (SSL).....	15
5.G. AUDIT LOGGING	16
5.H. INFORMATION HIDING.....	17
5.I. DOMAIN NAME SERVER (DNS).....	18
5.J. ADDITIONAL GUIDELINES FOR CONSIDERATION	19
5.K. OTHER	19

1. FOREWORD

This document provides an overview of the Centers for Medicare and Medicaid Services (CMS) Internet Platform Infrastructure Architecture and Minimum Platform Security.

This architecture addresses CMS application systems on the Internet from a platform infrastructure perspective. It establishes an environment that ensures availability, integrity, and confidentiality by protecting the platforms on which the data and applications reside. It also provides flexibility for applications development because the framework can be appropriately tailored to meet individual business needs.

This platform architecture is one of several of architectures and standards for Internet and other web-enabled applications. Others in the suite are CMS Web-Enabled Application Security Architecture, which focuses on security requirements that must be incorporated into CMS's Web based applications; CMS Enterprise Messaging Infrastructure, which describes the messaging and connectivity components for CMS's enterprise; and CMS Intrusion Detection Architecture and Design, which addresses intrusion detection and incident response requirements for infrastructure supporting Web based systems.

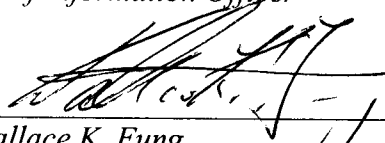
Based on industry and government architecture standards, this Architecture is considered an acceptable and secure structure. The Office of Information Services' (OIS) Deputy Director for Technology/Chief Technology Officer leads the development of this architecture with the support of all OIS components and input from other CMS Centers and Officers. In addition, an independent security services firm was retained to conduct a review of the Architecture as well as "table-top" penetration test to ensure the accuracy of the contents and the adequacy of the security standard. All comments and recommendations have been incorporated into this document.

This Architecture has been reviewed and accepted as a component of CMS's Enterprise Architecture and Standard in accordance with CMS's Information Technology governance process. It is a conceptual "to-be" architecture and serves as the blue print for the implementation of Internet-based systems for both in-house and contractor systems that support CMS business operations.



Tim Love
Director, Office of Information Services
Chief Information Officer

8/15/03
Date



Wallace K. Fung
Deputy Director for Technology and
Chief Technology Officer

8/15/03
Date

2. EXECUTIVE SUMMARY

The Architecture for the CMS Internet platform is a “three 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 will exist to support specialized network services such as Public Key Infrastructure (PKI), Domain Naming Services (DNS), etc.

The CMS Internet Architecture is crafted to support a single, unified interface with both our internal and external user/customer, as well as an operational approach to the various web applications developed and implemented by and/or for CMS. Various web applications hosted on the Internet platform will be able to access data in the data warehouse/data marts and a variety of operational databases, where and when appropriate, located within CMS and its contracted sites in the “Secure” region.

The databases accessed by web applications may be on operational database servers or may reside in the data warehouse or data marts. This essentially means that the innermost zone, the “Secure Region,” when implemented, will house database servers supported not only within CMS, but can include databases accessed across all CMS, securely linking CMS’ Fiscal Agents (FA), Fiscal Intermediaries (FIs) and the Carriers.

Access to the various databases at various physical sites will be facilitated by the use of a common message-oriented interface between the Internet platform’s application servers and the database servers at various sites.

3. BACKGROUND

This document presents the first of a series of efforts to address the architectural and related design and security issues related to the implementation of a standard CMS Internet platform in support of CMS' mission critical applications. This Internet Architecture was developed by staff from the Office of Information Services (OIS) based upon proven approaches used within the Government as well as the banking and financial industry to protect valued transactions and privacy data.

As a follow-up to this architecture effort, an overall Intrusion Detection System (IDS) capability for the Internet platform will be developed. This effort will include the development of an overall architecture and design for the implementation of an IDS for the Internet platform including scoping out the IDS hardware/software required for both Network based and Host based IDS capabilities and the associated Security Incident Handling capabilities required for the system. This effort will be reflected in a second document, CMS Internet Intrusion Detection System Architecture and Design Document. A third document, addressing Messaging and Connectivity, and a fourth addressing Application Architecture will also be developed.

As part of the process of developing this architecture, staff from the OIS area reviewed platform and security architectures put forth by several commercial banks in support of Internet initiatives for the Department of Treasury. While this architecture is not identical to any of those platforms (and they are not identical among themselves), the extensive design and security reviews done by the banks and by independent third-party security specialists are reflected to a significant extent in the architecture for the CMS Internet platform. This similarity in architecture is not done simply to 'be consistent' but rather is done to benefit from the thousands of person-hours of research, design, and review that went into the platforms put forth by the banks.

4. CMS INTERNET ARCHITECTURE

The CMS Internet Architecture at the highest level can best be presented in four ‘views’:

Connectivity View – Overview of major Internet platform systems and connectivity between various parts of the platform.

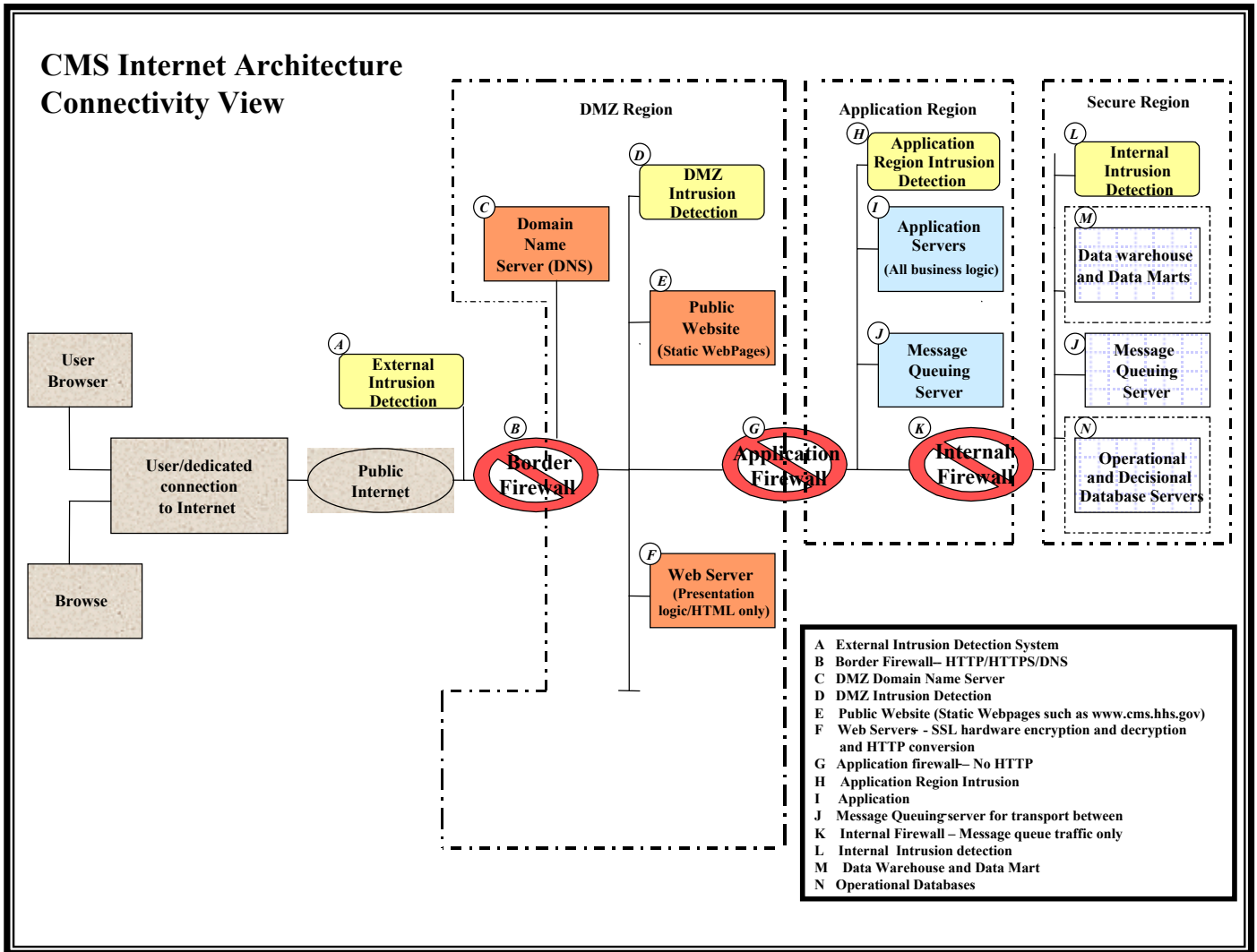
Protocol View – Overview of the protocols used in various regions of the CMS Internet platform.

Processing View – Overview of the types of processing that take place in each region of the CMS platform.

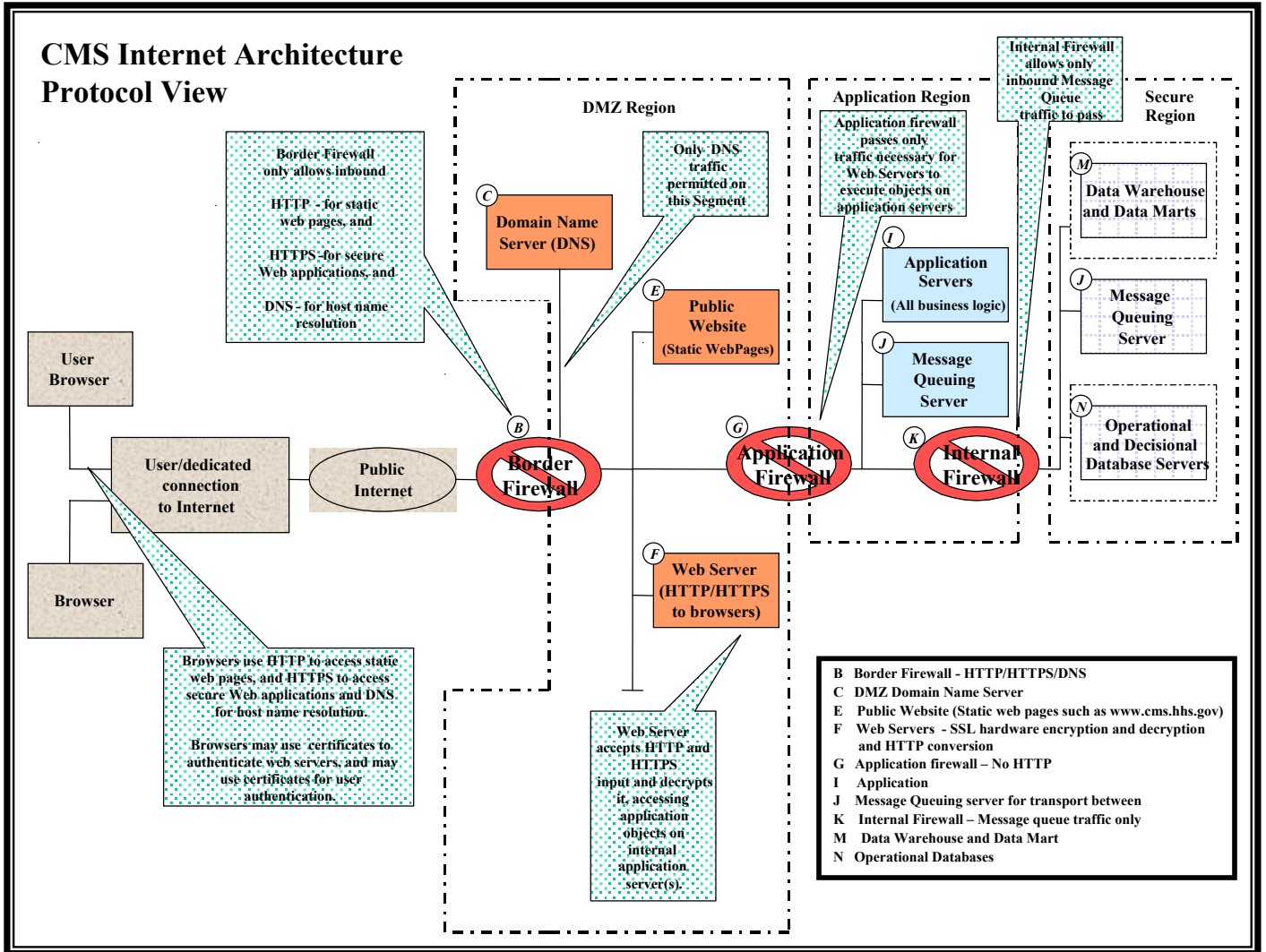
Hardware/Software View – Overview of the actual hardware/software platforms used in various regions of the CMS Internet platform.

Each view is shown below and is annotated appropriately to indicate the pertinent information for that view. After the four views, there is a CMS Internet Platform Security Policy section that provides details on the security architecture for the CMS Internet platform.

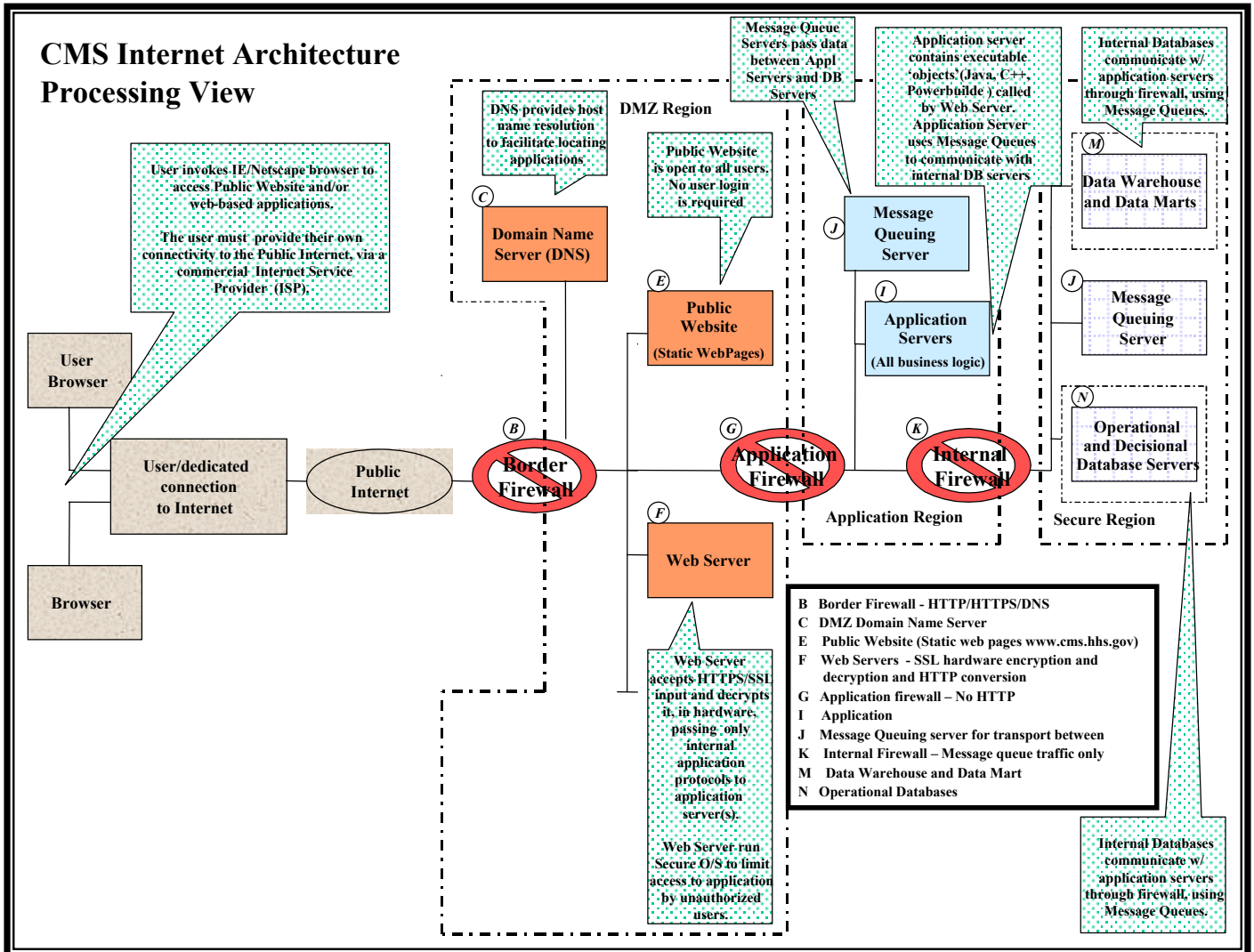
4.A. Connectivity View



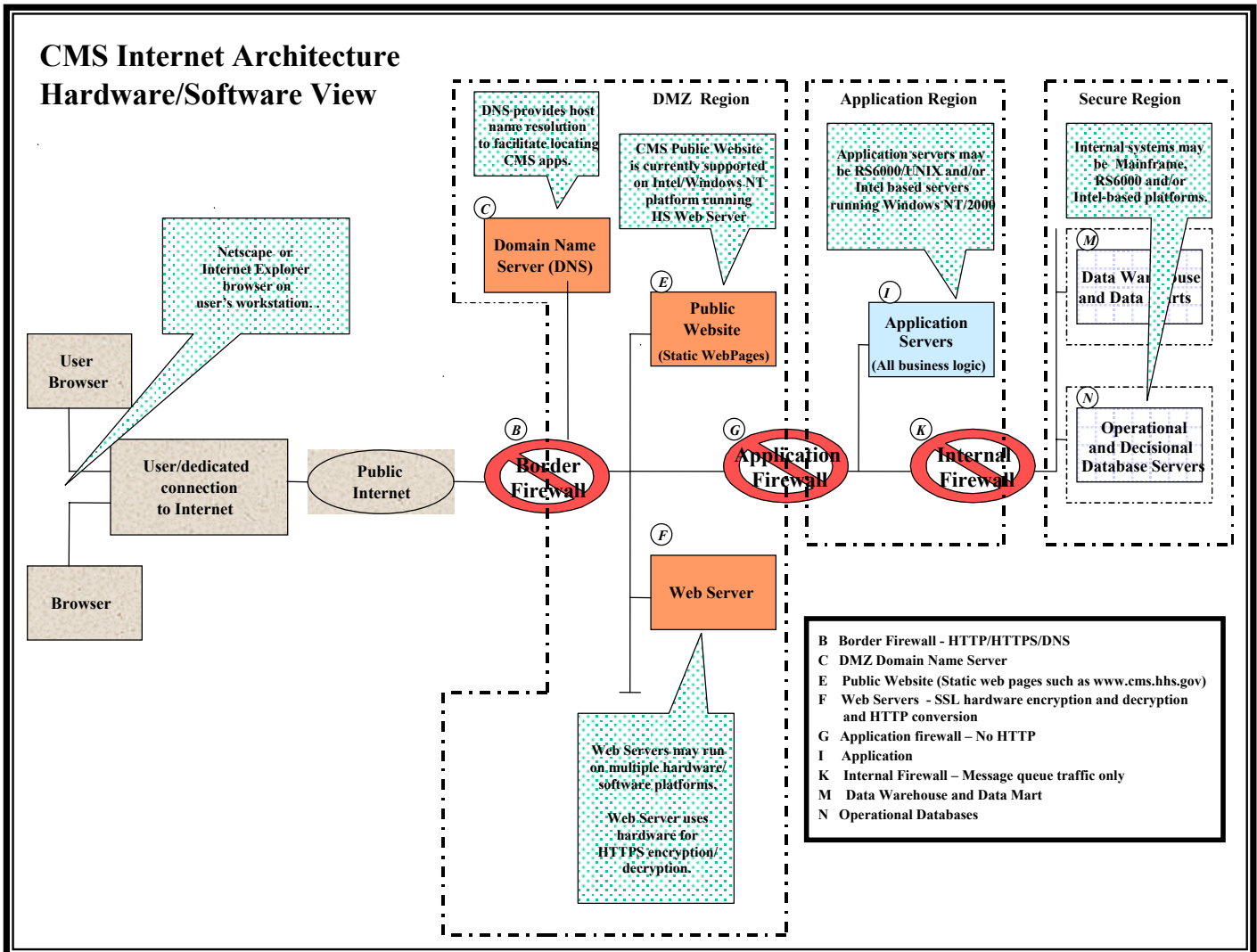
4.B. Protocol View



4.C. Processing View



4.D. Hardware/Software View



5. Security Requirements Addressed by this Architecture

This section of the document details security requirements addressed during the development of the Architecture. All requirements presented here are in addition to, and not in lieu of, all IT Security requirements of CMS.

5.A. General

These requirements shall be implemented consistent with the CMS Information Security Policy Standard and Guidelines Handbook and the CMS Information Security Acceptable Risks Safeguards.

5.A.1 Any operating system (UNIX, Windows NT, etc) must be configured in accordance with National Security Agency guidelines on server/operating system vulnerabilities and guidelines provided by the National Institute of Standards and Technology Special Publications, including but not limited to the Special Publications 800-7 and 800-43 as applicable.

5.A.2 All web servers must be configured in accordance with National Security Agency guidelines on secure web site configurations.

5.B. General Architecture: Layered Security

The Internet platform shall be comprised of three successive protected regions: (1) the DMZ/Presentation Region, (2) the Application Region, and (3) the Secure Region.

5.B.1 The DMZ/ Presentation Region contains the static web page public website and all web servers. The DMZ/Presentation Region servers shall contain presentation logic only (HTML) for the public website containing static web pages and Internet applications. No application/business/database logic/processing shall be executed on servers in the DMZ/Presentation Region.

5.B.2 The Application Region resides behind the DMZ/Presentation Region and contains web applications servers. The application servers in the Application Region shall execute all application/business logic for the web applications. Note, however, that the use of database-stored procedures that may reside on database servers in the Secure Region is permissible. No direct database interaction may be initiated via the application region. All queries will be handled via a messaging subsystem between the Application and Secure Regions.

5.B.3 The Secure Region resides behind the Application Region and contains all data sources including data warehouse and data marts as well as the operational databases for the applications. All interactions to and from the Application Region and the Secure Region must pass via a messaging system.

- 5.B.4** All of the regions shall be protected at a minimum by a layer of traffic filtering firewall security which must mediate all information flows without exception among the external networks/public Internet and the internal Internet platform. Additionally, all of the traffic shall be monitored via intrusion detection systems as defined by the Intrusion Detection System document in this series of documents.
- 5.B.5** Additional regions may reside behind the Secure Region.
- 5.B.6** The firewall security system used to protect the DMZ/Presentation Region must be complementary to that used to protect the Application Region and Secure Region; i.e., the firewall security system used for the Application Region and/or the Secure Region shall NOT be the same system as that used for the DM/Presentation Region. This requirement ensures that any unauthorized attempt to gain access to the Application Region and/or the Secure Region will have to break through two different firewall security systems. It is permissible to use the same firewall security system for the Application Region and the Secure Region as long as a different firewall system is used for the DMZ/Presentation Region.
- 5.B.7** The web server(s) in the DMZ/Presentation Region must support only HTML content. All support applications, business logic, databases, tables, and sensitive information for the CMS Internet web applications shall reside on dedicated servers in the Application Region and the Secure Region.
- 5.B.8** The web server(s) in the DMZ/Presentation Region must not store (on permanent database/disk storage) any data submitted by a client or any sensitive information passed to the client.
- 5.B.9** The DMZ/Presentation Region, and by extension the entire Internet platform, shall be protected by a border firewall, which provides a concentration of security services including, at a minimum, packet and protocol filtering, information hiding, and audit logging consistent with requirements of this document.
- 5.B.10** The Application Region and the Secure Region shall each also be protected by firewalls in front of the application and database servers. Those firewalls must provide a concentration of security services, including, at a minimum, packet and protocol filtering, information hiding, and audit logging consistent with the requirements of this document. The packet and protocol filtering on these firewalls must be complementary to that of the border firewall; i.e., no packet which is permitted through the border firewall based on its filtering rules shall be permitted through the Application Region or Secure Region firewalls (Internal firewall) based on their filtering rules.
- 5.B.11** All firewalls shall 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 rules of this document and the security policies established by CMS.

5.C. General Architecture: Segmented Security

- 5.C.1** All hardware and software used within the Internet platform shall be dedicated to processing only CMS Internet information and transactions.
- 5.C.2** All web applications, support applications, database applications, and firewalls shall be logically and physically separated onto dedicated servers. No additional business applications or other applications may reside on the dedicated servers.
- 5.C.3** Prior to acting on or transmitting the information submitted, all web servers and application servers which receive or process data obtained from clients shall check all data to ensure it has the appropriate format, size, and alpha-numeric construction and is within predetermined reasonableness parameters for the application or form concerned. The Internet platform must reject all sessions with malformed data and refer the information request to error handling or intrusion detection.
- 5.C.4** Common Gateway Interface (CGI) scripts, if used, shall be written in a manner that prevents users from obtaining command-level access to the Internet platform web server. Scripts must not allow user data to be passed to a server as a command string. Scripts must be capable of handling data exception conditions. Server Side Includes must be disabled for directories containing scripts.
- 5.C.5** The Internet platform public web site server and the Internet web pages shall prevent browsers and proxies from caching web pages with client forms, data, and other sensitive information.
- 5.C.6** Web servers, applications servers, other servers, firewalls, and routers shall disable all unnecessary features, Internet services, protocols, and applications not expressly required by Internet platform web module requirements. All compilers, editors, and other development tools must be removed from web servers, application servers, and other servers.
- 5.C.7** All Internet platform web servers shall be configured to prevent an administrative login from the Internet.
- 5.C.8** System administration for application servers and database servers may take place remotely from an internal network or dial up connection, but only if users are authenticated with hardware tokens and if communications are encrypted.
- 5.C.9** The following types of support applications shall be used to protect the integrity of the system:
- Intrusion detection - An intrusion detection program that continually monitors the entire Internet platform in real time.
 - Anti-virus - An anti-virus program that scans the entire Internet platform, both in real time and on a pre-determined schedule.

- Application access controls - Access control programs that perform user authentication and assign user privileges for all applications.
- Application audit and logging - Audit and logging programs that track user actions for all applications.

5.C.10 The following types of security tools, at a minimum, shall be used to aid in the detection of vulnerabilities and to monitor the system:

- Network scanning programs such as SAINT, Internet Security Scanner (ISS), SomarSoft, and Ballista must be used to identify security related vulnerabilities in network programs.
- Security risk programs such as COPS, Kane Security Analyst, Tiger, ScanNT, and NAT must be used to obtain a "snapshot" of the systems potential weaknesses.
- Integrity assessment programs such as Tripwire must be used to identify unauthorized system changes and to detect attacks that have previously occurred.
- Vulnerability assessments shall be conducted as specified in the *CMS Acceptable Risk Safeguards*.

5.C.11 System administrators must maintain contact with the support application vendors to obtain software upgrades and security patches. Upon release of any new software, the system administrators must immediately obtain and test the new software and as soon as possible install it on the Internet platform web module.

5.C.12 System administrators must follow all established configuration management procedures and practices, as well as meet established requirements for testing new software prior to installation on the Internet platforms.

5.D. Firewall Configuration - ("Deny Everything" Model)

5.D.1 All firewalls shall be configured to deny all requests, protocols, services, destination ports, and destination IP addresses except as expressly permitted in support of Internet/web applications as specified by this policy document and approved via formal CMS review procedures for firewall configuration.

5.D.2 In the event of an outage of any sort, all firewalls must fail to a configuration that denies everything pending the re-enablement of services by the firewall administrator.

5.D.3 Upon start-up, all firewalls must not compromise their resources or internal data that is within the Internet platform.

5.D.4 All firewalls shall be configured to ignore or reject any probing and scanning tools directed at them. If a firewall rejects a probe or scan, the response to the client must not include any sensitive or valuable information from the Internet platform or

otherwise reveal anything about the business or application logic of the Internet platform.

- 5.D.5** Firewalls may permit audit logs, event logs, administrator notifications, and security alarms to pass through the Internet platform to system administration terminals.
- 5.D.6** The DMZ/Presentation Region firewall (border firewall) must filter traffic between external Internet hosts and the Internet platform.
- 5.D.7** The border firewall must be configured to allow on its external interface only HTTP connections on port 80, SSL connections on port 443, and DNS connections on port 53 to the Internet platform only. No other connections, services, or requests of any kind may be allowed from external hosts on the Internet into the DMZ/Presentation Region.
- 5.D.8** The border firewall must be configured with two internal interfaces, one reserved exclusively for the Internet platform Domain Name Server (DNS) and one to connect to the remaining devices on the DMZ/Presentation Region.
- 5.D.9** The border firewall shall reject all traffic at its external interface that appears to come from a network address internal to the Internet platform except for responses from the web servers and the DNS services. The web services and the DNS services should not initiate this traffic.
- 5.D.10** The border firewall shall reject all traffic on both its internal and external interfaces that appears to come from a local network, a broadcast network, a reserved network, or a loop back network.
- 5.D.11** The Application Region firewall (application firewall) must filter traffic between the Internet DMZ/Presentation Region and all application servers in the Application Region.
- 5.D.12** The Application firewall shall be configured to reject any inbound HTTP/HTTPS sessions from the DMZ Region to the Application Region. The only inbound sessions permitted to pass from the DMZ/Presentation Region through the Application Firewall to the Application Region will be those ports (other than HTTP/80 and HTTPS/443) specifically required for web servers in the DMZ Region to access application servers/objects in the Application Region.
- 5.D.13** The application firewall shall be configured to receive data on its external interface only from web servers in the DMZ/Presentation Region and to pass data through the external interface to web servers in the DMZ Region only.
- 5.D.14** The application firewall shall reject all traffic at its internal interface that appears to be initiated from a network address external to the Application Region.
- 5.D.15** The application firewall shall reject traffic on its external interface that appears to come from a network address internal to the Application Region.

- 5.D.16** The Secure Region firewall (internal firewall) shall filter traffic between the Application Region and all servers in the Secure Region.
- 5.D.17** The internal firewall shall be configured to reject any inbound HTTP/HTTPS sessions from the Application Region to the Secure Region. The only inbound sessions permitted to pass from the Application Region through the internal firewall to the Secure Region will be those ports specifically used by the message-queuing servers in the Application Region that handle the transport of all inbound information from the Application Region to the Secure Region.
- 5.D.18** The internal firewall shall be configured to receive data on its internal interface only from servers within the Secure Region and to pass data through its internal interface only from servers within the Secure Region.
- 5.D.19** The internal firewall shall be configured to receive data on its external interface only from messaging-queuing servers within the Application Region and to pass data through its external interface only to servers within the Application Region.
- 5.D.20** The internal firewall shall reject traffic on its internal interface that appears to come from a network address external to the Secure Region.
- 5.D.21** The internal firewall shall reject traffic on its external interface that does not originate from the message queuing servers within the Application Region.

5.E. Firewall Administration

- 5.E.1** Only authorized administrators may access firewalls.
- 5.E.2** Firewall accounts shall be limited to the authorized firewall administrator and a backup.
- 5.E.3** Firewall administrators and subsequent backup administrators are required to use individually unique access accounts.
- 5.E.4** All system administration for firewalls shall take place from a local console that is either directly connected to, or is part of, the firewall hardware. Remote access to the firewall servers from internal and external networks must be disallowed.
- 5.E.5** Traffic-filtering firewalls shall not reside on a general-purpose computer or server or make use of a general-purpose operating system. Firewalls must reside in special purpose, self-contained, non-reprogrammable hardware devices. Firewalls shall not contain any general-purpose storage capabilities (write once storage capabilities for recording audit logs are permissible) and shall not have the ability to execute arbitrary code or applications.
- 5.E.6** Firewalls must be configured to disable all features and options not expressly required including, but not limited to, network access, user shells, and the like.

5.E.7 Firewall administrators shall maintain contact with the firewall vendors to obtain software upgrades and security patches. Upon release of any new software, the firewall administrators must immediately obtain and test the new software and as soon as possible install it on the Internet platform.

5.E.8 All firewalls shall provide the following functions at a minimum and must restrict the ability to perform them to an authorized administrator:

- Start-up and shutdown.
- Create, delete, modify, and view information-flow security policy rules that permit or deny information flows.
- Create, delete, modify, and view administrator profiles.
- Modify and set the threshold for the number of permitted authentication attempt failures.
- Modify and configure logging parameters, including the definition of auditable events, audit log size limitations, and audit log retention policy.
- Restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures.
- Enable and disable external hosts from communicating with the firewall.
- Modify and set the time and date.
- Archive, create, delete, and empty the audit trail.
- Backup of administrator profiles, information flow security policy rules, and audit log data where the backup capability shall be supported by automated tools.
- Recover to the state following the last backup.
- Disable remote administration from internal and external networks.

5.F. Secure Sockets Layer (SSL)

5.F.1 Web pages/web applications running on the Internet platform shall be designated as either 'public' or 'secure.'

5.F.2 Static web page content, such as the publications and general information available on the CMS Public website, will typically be designated as 'public' information. Web applications that contain non-public information shall be designated as 'secure' applications.

5.F.3 Public web pages/applications designated as 'public' do not require the use of SSL except for encrypting any information relating to user authentication/login that could be used to compromise User ID/password/authentication information.

5.F.4 Web pages/applications that are designated as ‘secure’ must use SSL Version 3 128-bit key encryption to protect Internet traffic subject to the following:

- The only unprotected HTTP content made available via the CMS Internet platform for a secure web application/page may be an initial homepage that immediately redirects clients to an SSL Version 3 connection. Otherwise, all other connections and all other traffic to the CMS Internet platform from external hosts on the Internet must be protected using the SSL Version 3 protocol implemented in accordance with the following:
 - The web server application shall be configured to allow only SSL Version 3 with server authentication and the full record layer with message authentication and encryption.
 - The web server application shall be configured to disallow SSL Version 2.
 - The web server application shall be configured to disallow resumed sessions.
 - The web server application shall be configured to disallow all export-weakened cipher suites with the exception of a session established with an initial SSL protected page to which the client may be redirected from the blank unprotected homepage.
 - The web server application shall use a Federal Information Processing Standard (FIPS) approved pseudo random number generator (PRNG) algorithm to generate cryptographic keys. (See Appendix 3 of FIPS PUB 186-1 and Appendix C of ANSI X9.17.)
 - All cryptographic modules used in the SSL session for key generation and cryptographic calculations shall be selected from the NIST FIPS 140-1 and FIPS 140-2 vendor list.
 - The web server shall be reviewed by an independent third-party to ensure that Version 2 rollback is not possible when Version 2 sessions are disallowed. Depending on the web server application, this may require an examination of source code.
 - Public key certificates for the web server shall be issued by the Government.
- The Internet platform shall “time out” SSL and application sessions and require users to logon to the system again if no activity occurs for 10 minutes during a user session.

5.G. Audit Logging

5.G.1 At a minimum, all firewalls shall produce audit records for each of the following events:

- Start-up and shutdown of the audit functions.
- Modifications to the users that are authorized firewall administrators.

- All use of the user identification mechanism, including the user identity provided.
- All use of the authentication mechanism.
- The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g., disabling of a terminal) taken and the subsequent restoration by the authorized administrator of the users' capability to authenticate.
- All decisions on requests for information flow
- Changes to the time.

5.G.2 The audit records on the decisions for all requests for information flow shall contain, at a minimum, packet type source and destination addresses, source and destination ports, frequency, user identifier, and session duration.

5.G.3 The audit records for all audited events shall be stamped with dependable date and time when recorded.

5.G.4 The firewalls shall maintain a log of all attempts to use disallowed services, protocols, and information flows.

5.G.5 The firewalls shall maintain a log of all attempts to spoof internal hosts and all attempts to access any internal host other than the web server.

5.G.6 The firewalls shall maintain a log of all attempts to probe or scan them.

5.G.7 All firewalls shall have automated alarms and automated activity thresholds that alert firewall administrators to all suspicious activity, report all security relevant events, and trigger corrective actions as appropriate in accordance with firewall security policies.

5.G.8 All audit logs shall be protected from unauthorized deletion. All firewalls and other hosts that maintain audit data must be able to prevent modifications to audit logs.

5.G.9 All logging activities done via the firewalls shall be published in raw format in GMT time.

5.H. Information Hiding

5.H.1 All host names and network IP addresses behind the border firewall shall be masked to Internet hosts external to the Internet platform.

5.H.2 All in-bound Internet traffic shall be intercepted and processed by the border firewall.

5.H.3 All out-bound Internet traffic shall be processed through the border firewall.

5.H.4 Firewalls shall ensure that residual information from a previous information flow or internal firewall data is not revealed or transmitted in any way. Resources must be overwritten or cleared before being made available for use again.

5.1. Domain Name Server (DNS)

5.1.1 If an ISP operates a DNS server for the Internet platform, written assurance is required to guarantee that adequate countermeasures have been taken to prevent DNS cache poisoning and other DNS vulnerabilities including, but not limited to, denial of service attacks. Otherwise, the DNS server must be located in the DMZ Region in accordance with the following.

5.1.2 The border firewall will be configured to filter traffic between external Internet hosts and a DNS server, in addition to the Internet platform server.

5.1.3 The border firewall must be configured with an additional network interface card representing a separate network segment dedicated to the DNS server. Thus, the border firewall would have an external interface to the Internet, an internal interface to the DMZ Region server(s), and a third interface to the DNS server (the 'DNS Interface'). No other machines (other than intrusion detection systems) may be connected to the dedicated DNS network segment.

5.1.4 The border firewall shall be configured to allow on its external interface DNS message connections on port 53 to the DNS server. No other connections, services, or requests of any kind may be allowed from external hosts on the Internet or internal hosts in the Application Region or Secure Region to the DNS server.

5.1.5 The border firewall shall be configured to receive data on its 'DNS Interface' only from the DNS server and to pass data through its 'DNS Interface' only to the DNS server.

5.1.6 The DNS server shall be configured to service DNS messages only. No other applications may reside on the DNS server. The DNS servers shall be configured to disable all other services, features, and options not explicitly required to handle DNS messages including but not limited to network access, user shells, and the like.

5.1.7 All system administration for the DNS server shall take place from a local console that is either directly connected to or part of the DNS server hardware. Remote access to the DNS server from internal and external networks must be disallowed.

5.1.8 The DNS server shall be dedicated to servicing the domain name of the CMS Internet platform only.

5.1.9 The CMS DNS server shall deny zone transfer requests to unauthenticated hosts.

5.J. Additional Guidelines for Consideration

The items below are not mandatory but are guidelines for consideration for implementation where practical and where they will not have a significant adverse impact on the capability for the Internet platform to provide reliable service to all its users.

- 5.J.1** The Internet platform shall either (a) temporarily block, for up to 60 minutes, any IP addresses from which users submit invalid login attempts 10 successive times or (b) temporarily block, for up to 60 minutes, any IP address from which users submit invalid login attempts 10 times during a 60 minute period. This applies regardless of whether any of the 10 attempts comes during different SSL sessions.

Note that in the case of users accessing the Internet platform via a ‘proxy’ server care must be taken to ensure that temporarily blocking users from specific IP addresses does not have a significant adverse impact on additional authorized connection to the Internet platform through the same ‘proxy’ server.

- 5.J.2** The Internet platform shall either (a) temporarily block, for up to 60 minutes, any account against which users submit invalid passwords 10 successive times or (b) temporarily block, for up to 60 minutes, any account against which users submit 10 invalid passwords during a 60 minute period. This applies regardless of whether any of the 10 attempts comes from different IP addressees or during different SSL sessions.

- 5.J.3** When responding to an invalid user login attempt or when temporarily blocking accounts or IP addresses, the system shall provide the user with the same generic rejection message without revealing anything about the business or application logic which led to the action regardless of the reason for the rejection or the technique used to enforce the action.

- 5.J.4** Notwithstanding any other provision in this section, the threshold amounts (e.g., 10 attempts) and time periods (e.g., 10 minutes) identified in this section shall be readily and independently configurable so that amounts and periods may be individually increased or decreased.

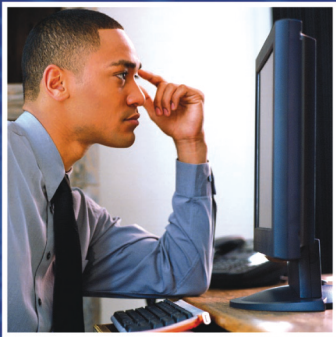
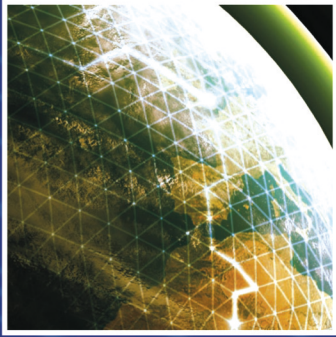
- 5.J.5** To ensure that damaging intrusions and intentional acts of unauthorized access can be effectively prosecuted, warning banners should be implemented as a minimum for all systems that interface with the public.

5.K. Other

- 5.K.1** Vulnerability Assessments - An independent third party with subject matter expertise must perform a penetration analysis. Major assessments should take place twice annually for the test/development platform and twice annually for the production platform. Less comprehensive assessments; i.e., mini or rapid assessments, should be performed on a regularly scheduled basis. An assessment should also occur when

significant changes are made to the platform; i.e., new applications are rolled-out, new servers are deployed, etc.

- 5.K.2** Incident Logging – A separate incident log shall be maintained to record all attacks, system failures, bugs, application problems, and other security related problems.
- 5.K.3** Configuration Documentation – A comprehensive record of all current and past configuration settings shall be maintained for all hardware and software including operating systems, applications, and firewalls, and be kept off-line at all times.
- 5.K.4** Operating Procedures - A comprehensive record of operating procedures for all applications within the Internet platform, including firewalls shall, be maintained and kept off-line at all times.
- 5.K.5** Cryptographic Authentication - User authentication tables, functions, and processes shall be built in a manner that permits future migration from knowledge-based authentication and access controls (PIN and password) to cryptographic authentication (public key authentication or digital signature).



Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244-1850

www.cms.hhs.gov
www.medicare.gov