TARGET IT ARCHITECTURE

VOLUME 6

SECURITY ARCHITECTURE

VERSION 1

HCFA
Health Care Financing Administration

August 29, 2000

Health Care Financing Administration
7500 Security Boulevard
Baltimore, MD 21244

Executive Summary

In the course of only three decades, information technology (IT) has come to play an important, and often vital, role in almost all aspects of Health Care Financing Administration's (HCFA) mission. As a consequence, security has become an essential aspect of IT. In this context, IT security means:

- Confidentiality – prevention of the unauthorized disclosure of information;
- Integrity – prevention of the unauthorized modification of information; and
- Availability – prevention of the unauthorized withholding of information or resources.

This document describes the Security Architecture component of the HCFA Information Technology Architecture (ITA). Security underlies all of the other parts of the ITA. This document describes the high level HCFA policies for security, covering all aspects of security for all of HCFA's information assets. It is intended as a guideline for system developers, contractors, designers, implementers, managers, project officers, contract officers, senior executives, and staff to use as new information systems are conceived, designed, built, implemented, and maintained. Architecture is defined within the areas required by the Health Insurance Portability and Accountability Act (HIPAA) – mandatory and mission-critical regulatory guidance for HCFA. The HCFA Security Architecture is based on the Chief Information Officers (CIO) Council Federal Enterprise Architecture Framework (version 1.1, September 1999).

This document provides a summary of the current HCFA environment and Security Architecture and a more detailed, but conceptual description of the target Security Architecture. The keystone of the target HCFA Security Architecture is the use of Public Key Infrastructure (PKI). PKI is a technique that provides the encryption key management structure necessary to build applications secured by cryptography. For example, PKI-supported cryptography can be used to provide secure and private information exchange over a publicly accessible network.

This document does not present a step-by-step blueprint for implementing the target architecture. Rather, it presents the policies supporting the architecture, and explains the fundamental concepts of the Security Architecture that HCFA is building for the future, for readers with a wide range of security backgrounds.

Table of Contents

Table of Exhibits

1 Introduction

1.1 Scope

The Security Architecture provides guidance for protecting HCFA's business assets: systems, software, and information resources. To be effective, the Security Architecture must address the entirety of this enterprise. Security policies, procedures, management, and technologies will be applied in the appropriate measures to safeguard assets at each level of the enterprise. Any less comprehensive alternative will allow risks, weaknesses, and vulnerabilities to be overlooked, and, as a result, provide inadequate protection for the architecture as a whole. In this context, it is important to note that the information security architecture must address information in all its forms, not just electronic. Thus, the policies and protections will deal also with information as paper documents, and as verbal and fax transmissions.

1.2 Models

The HCFA Security Architecture is based on the Chief Information Officers' Council Federal Enterprise Architecture Framework (version 1.1, September 1999). As recommended by the Framework, it begins with "Level I (the view from 20,000 feet)" by specifying the architecture drivers in terms of HCFA-specific policies and design principles. With these drivers as a starting point, Levels II and III, including the current architecture and target architecture, are developed. Level IV, the "Zachman/Spewak Framework," is not developed. Instead, the architecture is defined against the areas that need to be addressed to comply with HIPAA. The result is a more concise and compliant statement of the current and target Security Architectures.

1.3 Document Use and Content

The responsibility for allocating resources and accepting business risks lies with HCFA management. The responsibility for carrying out procedures and implementing an effective system and controls lies with every employee and user, both staff and management. This architecture looks at security from the viewpoint of both groups. From each viewpoint, a common set of questions can be asked: What? How? Where? Who? When? and Why? A robust security posture results from ensuring that these questions have acceptable answers in each view.

In the house-building metaphor, the architect is primarily concerned with over-arching design needs, (e.g., how many people it must hold), while the electrician is concerned with detail, (e.g., what switch goes where). This document provides guidance at the architectural perspective or level. It describes the result but does not include detailed implementation plans. Thus, the HCFA senior executive charged with responsibility for a business system would be concerned with those security requirements described here, and with making decisions to ensure security for the system developers and users at the lower levels. But the security that results depends not only on management attention and involvement, but also on the active participation and involvement of developers, users and staff.

This volume is organized into the following six sections to provide an answer to security questions that must be addressed by the architecture:

1. Introduction: A statement of scope and overview of methodology.

2. Principles and Policies: An itemization and explanation of the architecture drivers.

3. Environment and Current Architecture: A brief summary of the “as-is” model and business requirements for security. The current architecture illustrates how the external entities link to the HCFA data center and describes the access requirements for the individual domains.

4. Target Architecture: The “to-be” model and business requirements for security. The Target Architecture illustrates the target boundaries and link to the HCFA data center and describes the access requirements.

5. Architecture Management and Process: A process for keeping the target architecture current and meaningful, and guidelines for promoting Security architectural compliance.

6. Summary: A summary of the document.

Complementing this volume are the HCFA Systems Security Plan Methodology and the HCFA Information Systems Security Policy, Standards and Guidelines Handbook, which elaborate on information contained in this document, and include additional detailed procedures and guidelines useful to the reader, including a comprehensive glossary of systems security terminology.

2 Policies, Principles, and Responsibilities

This section of the HCFA Security Architecture discusses the architectural drivers – terse statements of security principles and policies that form the basis for decisions on formulating the target Security Architecture. This section itemizes and explains those policies and principles. The HCFA security principles are derived from Government-wide security themes. The resulting security principles, in turn, drive the HCFA security policies. Exhibit 2-1 illustrates the relationships between the various information security drivers in the government. It also describes the IT security responsibilities of key HCFA staff and organizations.

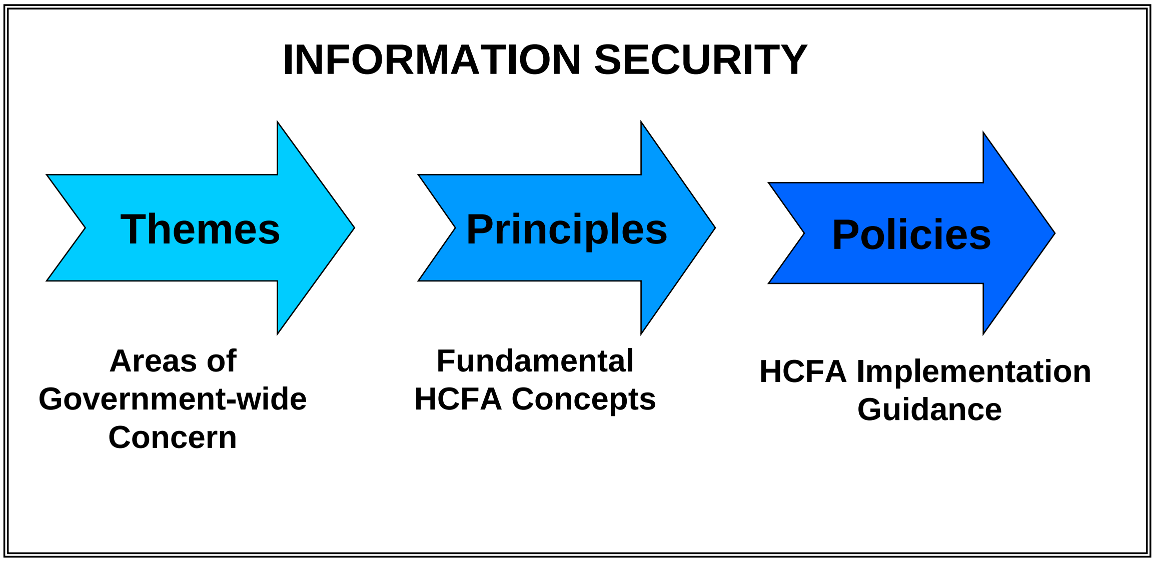

INFORMATION SECURITY
Themes
Principles
Policies
Areas of Government-wide Concern
Fundamental HCFA Concepts
HCFA Implementation Guidance

Exhibit 2-1 Information Security Architecture Drivers

2.1 HCFA Security Principles

Several underlying themes drive the development of HCFA's security principles. First, we must balance the need to restrict access to certain sensitive information with the need to increase public access for other types of information. Second is the Government's need to improve performance and results in the use of IT, including reducing information collection burdens on the public and improving information sharing and management. Finally, the Government must protect its critical IT infrastructure. These themes lead to HCFA's IT security principles.

> **HCFA Information Security Principle 1:** HCFA information assets must be protected from loss, corruption, or disclosure, and protection measures must be balanced against the operation cost imposed on the business, and must be appropriate to the threat and impact those assets face.
>
> **HCFA Information Security Principle 2:** As threats evolve, the security posture must be re-evaluated and protections adjusted appropriately.

HCFA Information Security Principle 3: The information owner determines the degree of acceptable risk; the level of protection must be appropriate to the risk and the value of the asset being protected.

HCFA Information Security Principle 4: Protective measures must not prevent necessary business from being carried out.

HCFA Information Security Principle 5: Security protections must be implemented in a layered, mutually reinforcing way. This can be accomplished by selecting an appropriate combination of technical controls; physical controls; administrative controls; training and awareness efforts; and auditing, logging, and incident response to mediate risk and minimize impact from security events.

HCFA Information Security Principle 6: Security controls need to be designed as products or processes integrated from the beginning of the software/systems development, rather than added as an afterthought. Security is but another aspect of quality. A system should do only what it is designed to do – no more, no less. Poor quality is a security risk.

HCFA Information Security Principle 7: Security mechanisms should balance the level of assurance with ease-of-use. The user should not be overly encumbered by security to the extent that productivity is seriously impacted or a strong motivation to work around security safeguards is generated.

HCFA Information Security Principle 8: HCFA information policies and implementation shall fully comply with all Federal laws and regulations and shall be consistent with the policies and guidelines of the Department of Health and Human Services (DHHS).

2.2 Security Architecture Policies

HCFA's IT security policies are founded on and flow from the security principles listed in Section 2.1.

HCFA Information Security Policy 1: Every information asset, (i.e., every system, process, data set, or document), must have an owner. When information is in media which are isolated, such as physical documents or removable electronic media (e.g., floppy disks, removable disks, CDs), the owner is assumed to be the person authorized to hold that media; accountability follows the possession of the asset. For systems, processes, or data that are electronic in nature, in an interconnected environment, a written statement of ownership must document accountability. Such statements must be readily available for inspection.

HCFA Information Security Policy 2: Anyone accessing information using systems or processes must be authorized to do so. When access is limited, such as for accessing private or proprietary information, then the accessing party must be properly identified and authenticated prior to the access as being duly authorized for the access.

Public data may be accessed by anyone; everyone is authorized to see or copy public information. Thus, no authentication is required by policy. Authentication, to some degree, may be required for other purposes, such as auditing, if a risk or threat is perceived, in order to assure accountability. The degree of authentication required will be commensurate with the value of the asset and the nature and potential impact of the threat.

Accountability requires the explicit definition of roles, access authorization, and rights based upon those roles, and identification and authentication measures sufficient to support role-based access. Accountability implies further that records of access, so-called audit logs, be maintained and reviewed regularly to ensure that the controls function correctly and that only authorized parties access sensitive information or critical processes.

> **HCFA Information Security Policy 3**: Access to sensitive information, systems, or processes will be logged, and the owners (or their expressed designees) will periodically review the logs for anomalous entries. Logs will be subject to audit.

Accountability implies that assets have explicit boundaries, so that the asset and its owner can be defined.

> **HCFA Information Security Policy 4**: All information assets must have explicit boundaries, which define the domain of ownership and responsibility. Information flows across boundaries; the interfaces with other assets must be explicitly understood, defined, and documented. In particular, the trust relationships across interfaces must be detailed and accounted for in the design and implementation of access roles and rights across the interface(s).

> **HCFA Information Security Policy 5:** All sensitive assets must have a documented security plan that describes the asset and its boundaries. The security plan documents the current operation of the asset/system; evaluates and enumerates the risks and threats that the asset is vulnerable to; explains the security protections that mediate the risk to acceptable levels; describes the tests that validate that the protections work as intended; includes the documented results of those tests; and contains a certification by the asset owner that the protections are adequate and operate correctly. Security plans must follow the HCFA System Security Plan Methodology standard. Security plans must be submitted to the HCFA Senior System Security Advisor and accredited by the CIO prior to the asset being placed into use. HCFA business partners must also prepare Security plans and furnish a copy of the plan to HCFA. HCFA contracts for many services, including a variety of IT services; all contracts that require or allow the contractor access to HCFA information must require the contractor to comply fully with HCFA Security policies.

> **HCFA Information Security Policy 6:** Everyone, whether HCFA staff or contractor, must receive HCFA-approved information security training before being granted access to sensitive information assets.

HCFA Information Security Policy 7: HCFA Security policies apply equally to HCFA staff, HCFA contractors, users, and other partners.

HCFA Information Security Policy 8: Quality configuration management is essential. All mission critical systems must have configuration management in place and adhered to. One of the most significant security liabilities is inconsistency in configuration and policy application.

HCFA Information Security Policy 9: The HCFA security boundary is breached only at a very few specifically authorized gateways or control points. Unauthorized paths through the HCFA security boundary are not permitted.

If HCFA outsources a function, responsibility for security functions or activities will reside with a federal management official with accountability and responsibility for the security mission.

2.3 Security Responsibilities

Every HCFA employee and contractor has responsibility to protect HCFA’s information assets. Certain positions have specific responsibilities as delineated and explained in the paragraphs that follow. These tasks do not relieve the organizational components within which the positions are located to comply with system security requirements, including oversight of personnel assigned to the positions, since security is a management responsibility as well.

2.3.1 *Chief Information Officer (CIO)*

The CIO is responsible for HCFA’s information assets. The CIO shall:

1. Assure ownership is assigned for all HCFA IT resources.

2. Appoint a Senior System Security Advisor.

3. Establish and maintain the IT portfolio.

4. Develop HCFA-wide IT Security Architecture.

5. Ensure that an Information System Security Officer (ISSO) has been appointed for each component and a senior ISSO appointed for HCFA.

6. Ensure IT Security plans and accreditation documentation are prepared for all HCFA IT systems and that all corrective actions are completed.

7. Ensure that risk analysis is completed for all IT systems.

8. Ensure that contingency and disaster recovery plans are developed for all IT systems.

9. Ensure that a tracking system is established and maintained that includes the required controls and accreditation status for all IT systems.

10. Act as the central accreditation official of all HCFA Central Office and Regional Office sensitive IT systems, and ensure that all certification requirements have been met for each system prior to accreditation.

11. Ensure that each HCFA employee, contractor, staff member, or user of HCFA data or system has received appropriate security awareness training.

12. Establish and charter the IT Council as the agency-wide body charged with developing agency security policy.

2.3.2 *Senior System Security Advisor (SSSA)*

The SSSA monitors, evaluates, and reports, as required, to the CIO on the status of IT security within HCFA and the adequacy of the programs administered by the operating units. The SSSA's duties include:

1. Develop draft policies and submit to the IT Council for approval; and based on agency security policies, develop standards and guidelines for establishing, implementing, maintaining, and overseeing requirements for HCFA's IT security program.

2. Provide guidance and technical assistance, including analyzing, evaluating, and approving all HCFA internal IT System Security Plans and requirements for IT systems security.

3. Assure HCFA IT security oversight through compliance reviews of operating units and organizations, IT security verification reviews of individual systems, and by participating in DHHS program management oversight processes.

4. Maintain a tracking system and records concerning implementation of the required controls and accreditation status of all HCFA IT systems.

5. Act as the central point of contact for HCFA IT security-related incidents or violations.

6. Ensure compliance with Security policies including actively working with system design and implementation conflicts.

7. Arrange for IT security awareness training for the system staff, and monitor the user training programs to ensure that personnel receive security orientation before being allowed access to sensitive IT resources.

2.3.3 *System Owner/Managers*

All information resources (hardware, software, facilities, data, and telecommunications) will be assigned to an owner, designated in writing to the CIO. For example, the "owner" of the resources contained within a HCFA general support system (GSS), e.g., HCFAnet, may be the manager of that system or facility. Each system owner shall be responsible to:

1. Determine the sensitivity of the resources for which they are responsible.

2. Determine the appropriate level of security required consistent with federal laws, regulations, and directives.

3. Ensure a Systems Security Plan (SSP) is prepared for each GSS and major applications (MA) under their authority.

4. Be a certifying official and complete all required certification actions consistent with the SSP methodology.

5. Implement the SSP and monitor its effects.

6. Ensure that each automated data processing position (including contract positions) is properly designated in accordance with position sensitivity criteria, and receives appropriate investigative processing.

7. Ensure a systems security risk assessment is prepared for each system under their authority.

2.3.4 *Senior Information Systems Security Officer*

The Senior Information Systems Security Officer (Senior ISSO) is responsible for the following:

1. Evaluating and providing information about the HCFA AIS Security Program to management and personnel, and communicating HCFA AIS Security Program requirements and concerns.

2. Ensuring that SSPs are developed, reviewed, and implemented for the SSP process.

3. Ensuring that systems security risk assessments are developed, reviewed, and implemented for the SSP process.

4. Reporting information resources security incidents in accordance with the systems security incident reporting procedures developed and implemented by federal mandates, DHHS, and HCFA policies.

5. Mediating and resolving systems security issues that arise between two HCFA organizations, HCFA and other federal organizations, or HCFA and states and contractors.

6. Maintaining documentation used to establish systems security level designations for all SSPs with HCFA.

7. Assisting other ISSOs in developing local Information System Security for either in-place SSPs or for those under active development.

8. Researching state-of-the-art systems security technology and disseminating informational material in a timely fashion.

9. Assuring that ISSOs are appointed and trained.

10. Developing and implementing an AIS security training and orientation program in accordance with the requirements from the Computer Security Act of 1987.

2.3.5 Information System Security Officer (ISSO)

The ISSO for each component shall perform the following functions:

1. Advise the IT system owner on matters pertaining to IT systems security.

2. Develop, implement, and manage the execution of the IT system security program.

3. Prepare an IT System Security Plan in the HCFA Security Plan Methodology format for the IT system.

4. Conduct a risk analysis on the system when there are major changes to the system, or every three years, whichever is less. However all GSSs and MAs will be reviewed annually.

5. Ensure that system contingency and disaster recovery plans are developed, maintained in an up-to-date condition, and tested at least annually.

6. Establish and maintain liaison with any remote facilities or users served by the IT system, the operating unit ISSO, or if appropriate, the subordinate organization ISSO.

7. Monitor changes in hardware, software, telecommunications, facilities, and user requirements to ensure that security is not compromised or degraded.

8. Exercise system responsibility or direct activities for password management and control.

9. Ensure that positions requiring access to sensitive information or resources are identified, and that incumbents of these positions receive an appropriate level of

clearance before access is granted (see Volume 3 of ITA, for HCFA sensitivity levels).

10. Investigate known or suspected security incidents or violations and prepare reports on them.

11. Ensure that the organization abides by software policies, and has the required virus detection and elimination software and procedures available to protect against these threats.

12. Audit all the systems within the organization for illegal software at least annually and maintain inventories of all software on each individual system to verify that only legal copies of software are being used.

13. Review IT-related procurement specifications for hardware, software, or services to ensure that they include adequate security requirements or specifications commensurate with the sensitivity of the system.

14. Conduct all activities required for the certification of the system, including preparing the certification and accreditation packages for final approval every year, or when major changes occur to the system, whichever is less.

2.3.6 Privacy and Security

The interaction of privacy and security results in a requirement to protect and secure from disclosure and unauthorized access those records that we maintain which are protected by the Privacy Act. Privacy and confidentiality are the driving forces behind security.

The Privacy act of 1974 can generally be characterized as an omnibus code of fair information practices, which attempts to regulate the collection, maintenance, use, and dissemination of personal information by Federal government agencies.

Broadly stated, the purpose of the Privacy Act is to balance the government’s need to maintain information about individuals with the rights of the individuals to be protected from unwarranted invasions of their privacy stemming from the collection, maintenance, use, and disclosure by Federal agencies of personal information about them. The Act focuses on four basic policy objectives:

1. To restrict disclosure of personally identifiable records maintained by agencies.

2. To grant individuals increased rights of access to agency records maintained on them.

3. To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.

4. To establish a code of fair information practices, which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

Any item, collection, or grouping of information about an individual that is maintained by an agency including, but not limited to, his education, financial transactions, medical history, and criminal or employment history, and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph, is considered a record under the Privacy Act. A group of any records under the control of any agency from which information is retrieved by the name of the individual, or by some identifying number, symbol, or other identifying particular assigned to the individual, is called a system of records.

2.3.7 Agency Responsibility

Each agency that maintains a system of records shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records, and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Moreover, with the exception of permissible disclosures authorized under the Privacy Act, no agency shall disclose any record contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

2.3.8 Privacy Officer (PO)

The Privacy Officer is the principal authority on maintenance and release of Privacy Act protected data from the Privacy Act SOR. The Privacy Officer's responsibilities include:

1. Interpreting Privacy Act requirements and rules.

2. Coordinating with all System Owners/Managers to ensure that they understand the Privacy Act requirements and their related responsibilities.

3. Reviewing requests and concurring with the need to establish a new Privacy Act SOR or to modify an existing Privacy Act SOR.

4. Assisting System Owners/Managers in preparing Privacy Act SORs in accordance with established procedures.

5. Ensuring that SORs comply with the Privacy Act.

3 Environment and Current Architecture

This section provides an overview of HCFA's information users, information resources, risks and threats, and the present Security Architecture. The discussion section presents an overview and summary of these topics.

3.1 Information Users

Users of HCFA information exist in many forms. A user can be a person or a system. Users of HCFA information include health care providers (hospitals and physicians); Contractor Organizations, such as Blue Cross Blue Shield (BCBS) organizations or other non-BCBS commercial insurance carriers; Health Management Organizations (HMOs); Preferred Provider Organizations (PPOs); patients (beneficiaries), researchers, and policy makers. Each user has unique access requirements and constraints.

For the purposes of this document, any organization that process Medicare claims and has a contractual agreement with HCFA will be referred to as a Medicare Contractor. Users of HCFA information exist at many diverse locations and have varying degrees of access authority.

External users include Medicare Managed Care Organizations, Medicare Integrity Program Contractors, State Medicaid Agencies, State Survey & Certification Agencies, Professional Review Organizations (PROs), and End State Renal Disease Networks. These users access HCFA information using a variety of access paths. Exhibit 3.1 illustrates several current types of users and indicates varying degrees of access privilege and information trust associated with these users.

At the present time, principal users of HCFA information include: HCFA Central Office, HCFA Regional Offices, High Assurance Remote Contractors (HARCs) or Trusted Contractors, Common Working File processing sites and users, Medicare Fee for Service Carriers and Fiscal Intermediaries, Medicare HMOs, State Medicaid Agencies, HCFA employees using Flexiplace, researchers, other Government Agencies [Treasury, Internal Revenue Service (IRS), General Accounting Office (GAO)], and the general public.

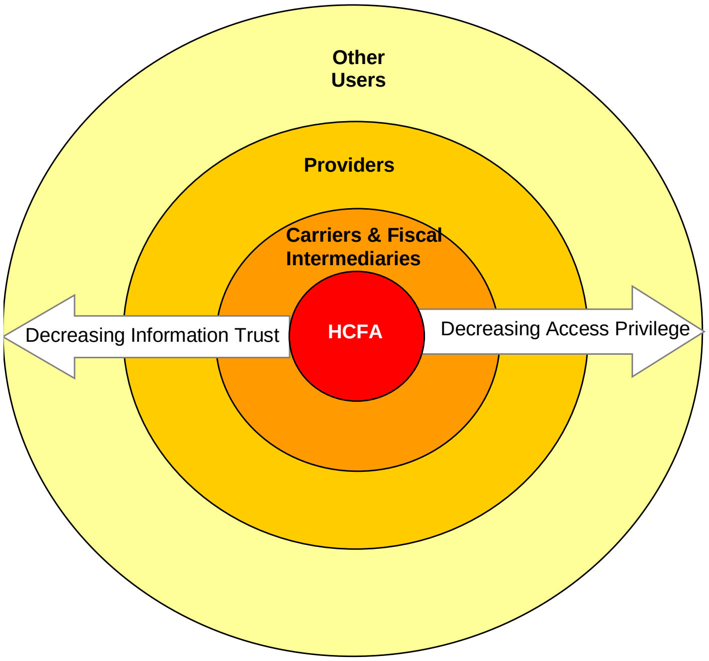

Other Users
Providers
Carriers & Fiscal Intermediaries
HCFA
Decreasing Information Trust
Decreasing Access Privilege

Exhibit 3-1 The Security Architecture Addresses the Constraints and Needs of Several Classes of Information Users

3.2 Information Resources

HCFA Information Resources are physically stored in many diverse locations: HCFA Central Office, HCFA Regional Offices, Medicare Fiscal Intermediaries, Medicare Carriers, Medicare Claims Processing Data Centers including CWF processing sites, researchers, state and professional organizations, and personal workstations. HCFA Information Resources exist in many forms including, but not limited to, data files, databases, and e-mails.

HCFA manages five principal types of information:

1. *Claims* information is the central means of conducting the business of paying fee-for-service healthcare claims. Claims are also used to help calculate rates for managed care plans. Privacy issues are the driving force behind protecting this most critical of HCFA's Information Resources. Validity and accuracy of this data also contribute sensitivity to the requirement to protect this information.

2. *Financial* information is critical to the fiscal health and management of the public trust. Validity and accuracy are primary drivers for the high level of protection necessitated by the management of financial information. Fraud protection and detection are also contributors to the sensitivity of this information. Safeguarding financial instruments (e.g., checks, EFTs, 1099 forms) is essential.

3. *Provider* information is essential to successful claims processing and payment. Secure, accurate provider information is also a requirement for financial reporting, including reporting to the IRS.

4. *Beneficiary* information protection is essential to maintaining the public trust. As with Claims information, beneficiary information contains an inherent privacy requirement. Protection of the integrity and availability of beneficiary information is critical to the Medicare and Medicaid Programs.

5. *Administrative* information is the aggregation, summarization, or other manipulation of other HCFA information. Administrative information may contain part or all of other HCFA information: Claims, Financial, Provider, Beneficiary.

3.3 Risks and Threats

The Security Architecture design mitigates specific risks and threats to the HCFA enterprise. Risks and threats are identified by examining technical, physical, administrative, and awareness limitations that would constrict HCFA from fulfilling the policies and principles identified in Section 2 and in Volume One, the IT Direction, of the HCFA IT Architecture. For example, risks and threats arise as a result of:

- Improper security practices on behalf of business asset users, such as poorly selecting passwords, sharing accounts, leaving workstations unsecured, or using default system parameters

- Attack from malicious hackers outside of the HCFA environment;

- Destructive viruses;

- Denial of service attacks;

- Attacks from discontented users within the HCFA domain; and

- Potential unauthorized access by ex-employees and former contractors.

Many threats and risks (internal and external, logical and physical) exist that may compromise the confidentiality, integrity, and availability of HCFA's Information Resources. Exhibit 3-2 illustrates a few potential threats and risks to some examples of HCFA's Information Resource as it exists today. HCFA’s IT Architecture provides a comprehensive discussion of this issue.

Information Resource	Threat or Risk	Type
Claims	Amount of claim is maliciously altered, personal confidentiality violated.	Integrity, Confidentiality Threat
Financial	Information altered, checks stolen or misplaced, funds allocated inappropriately.	Integrity, Availability Threat
Provider	Inappropriate viewing or dissemination of personal information.	Integrity, Availability Statement of importance of the data
Beneficiary	Inappropriate viewing or dissemination of personal information.	Confidentiality Threat
Administrative	Analysis data stolen, reported to the press, misrepresented. Integrity of HCFA systems challenged or questioned in the media.	Integrity Threat

Exhibit 3-2 Information Resource Threat or Risk Examples

3.4 Summary of Current Security Architecture and Business Requirements

The mission of HCFA is to assure health care security for beneficiaries. HCFA provides health insurance to over 78 million Americans, spending over $400 billion a year buying health care services for beneficiaries of Medicare, Medicaid, and the Children’s Health Insurance Program. In addition to providing health insurance, HCFA also performs a number of quality-focused activities including regulation of laboratory testing; surveys and certification of health care facilities (including nursing homes, home health agencies, intermediate care facilities for the mentally retarded, and hospitals); development of coverage policies; and quality-of-care improvement.

In the course of assuring health care for eligible Americans, a tremendous amount of information is received, processed, and stored concerning beneficiaries, providers, and claims. HCFA is committed to ensuring that all necessary information is efficiently and effectively processed, and that this information is safeguarded from either intentional or unintentional corruption or misuse.

The current Security Architecture is documented in many existing HCFA sources, including the Chief Financial Officer Electronic Data Processing (CFO EDP) auditor reports and various internal audit report documents. An overview of the current Security Architecture is presented in Exhibit 3-3.

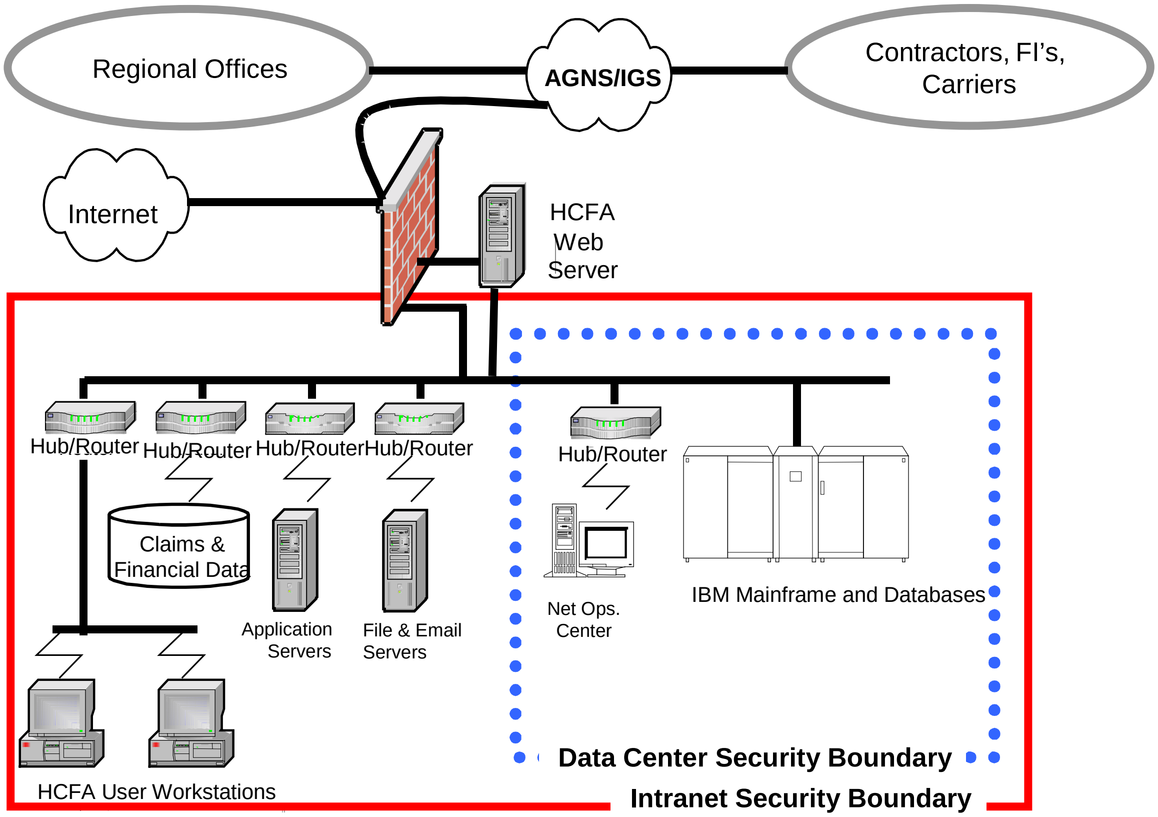


Exhibit 3-3 Conceptual Overview of HCFA's Current Security Architecture

4 Target Architecture

This document provides a conceptual description of the target Security Architecture. The target HCFA Security Architecture is defined within the context of six areas required by HIPAA. These areas include technical; physical; administrative and procedural protection; personnel training and awareness; event logging and auditing, and intrusion and incident response detection.

4.1 Technical Protection Measures

Technical protection measures are traditionally grouped into three high level categories: confidentiality, integrity, and availability. They are defined as follows:

- *Confidentiality* measures provide the mechanism to ensure that the privacy of information is maintained.

- *Integrity* measures enhance the reliability of information by guarding against unauthorized alteration.

- *Availability* measures seek to ensure that information assets are accessible to internal and external users when needed.

The keystone of the technical protection measures is the use of Public Key Infrastructure (PKI). PKI is a technique that enables users of a basically unsecured public network to exchange data securely and privately through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. This strong authentication mechanism, using certificates provided through the PKI process, is a mandatory prerequisite to both confidentiality and integrity.

4.1.1 *Public Key Infrastructure (PKI)*

Encryption is the underlying technology for many security controls. PKI is necessary to support encryption key management. Key management includes granting and revoking certificates that assign public keys to users and information resources. In the target architecture, public key cryptography is the underlying means for authenticating users, building information integrity, and protecting privacy.

The HCFA PKI architecture will build from the Federal PKI model (Proposed Federal PKI Architecture, W. E. Burr, 19 May 1998, NIST, TWG-98-29). It will include linkages back to the DHHS department level and Federal Bridge Certificate Authorities (CA) to enable HCFA applications to communicate securely, internally and externally, with trading partners.

A key component of the PKI architecture will be the HCFA X.500 enterprise directory. The directory will house certificates and serve as a coordination point for all other administrative and IT directories distributed across HCFA. Exhibit 4-1 presents the HCFA enterprise directory architecture.

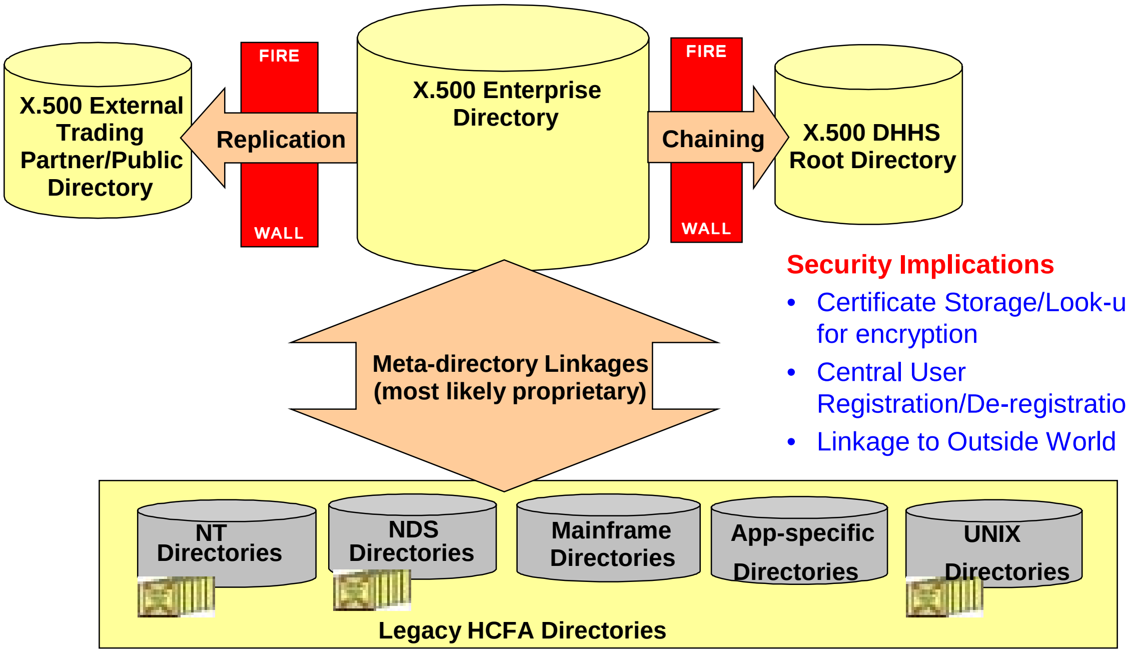

X.500 External Trading Partner/Public Directory
FIRE
WALL
Replication
X.500 Enterprise Directory
FIRE
WALL
Chaining
X.500 DHHS Root Directory
Security Implications
• Certificate Storage/Look-up for encryption
• Central User Registration/De-registration
• Linkage to Outside World
Meta-directory Linkages (most likely proprietary)
NT Directories
NDS Directories
Mainframe Directories
App-specific Directories
UNIX Directories
Legacy HCFA Directories

Exhibit 4-1 The Target HCFA Directory Architecture

The standard for access to the X.500 enterprise directory will be the Lightweight Directory Access Protocol (LDAP). Since LDAP only addresses the means to access directories, the selections of X.500 and LDAP are independent. By choosing X.500 and LDAP, HCFA will have a base-set of open standard protocols that are complementary, widely implemented, and supported by a wide-range of existing PKI and related security products.

There are five legacy directories in the HCFA enterprise: Microsoft Windows NT server directories, NetWare Directory Service (NDS) directories, IBM mainframe directories, application-specific directories (e.g., directories maintained by Human Resources or Facilities), and Unix directories. The proliferation of directories presents a security risk. The X.500 enterprise directory provides a single, authoritative source for all directory information on employees, contractors, and information resources. The legacy directories will be synchronized with the enterprise directory through “meta-directory linkages”. These linkages ensure that any changes to legacy directories are tracked in the enterprise directory.

Use of the X.500 standard for the enterprise directory provides several key benefits. First, X.500 is a well-accepted industry standard that is implemented by many directory vendors’ products. Secondly, DHHS has standardized on X.500. This means that HCFA and DHHS will be able to use an advanced linking method, known as “knowledge links,” to allow selective sharing of directory information. Finally, X.500 supports a variety of other linking methods, including “replication.” Replication will allow HCFA to post sections of the enterprise directory accessible to external trading partners and the public. Exhibit 4-1 shows the use of firewalls to help re-enforce the directory boundaries between HCFA, DHHS, and the public.

The directory architecture plays an important role in the technical Security architecture. It supports the following security functions:

> Storage of Certificates: The Enterprise Directory houses X.509 digital certificates for HCFA employees, contractors, trading partners, and information resources. If, for example, HCFA employee Alice wishes to send an encrypted secure message to HCFA employee Bob, she must be able to look up Bob’s public encryption key. Bob’s key will be stored in a digital certificate in the Enterprise Directory. Although Exhibit 4-1 indicates that certificates may be stored in other (i.e., legacy) directories as well, the Enterprise Directory maintains the authoritative copy.
>
> Coordination of legacy directories content: The Enterprise Directory mitigates the security risk of incomplete or inconsistent access privilege storage in multiple legacy directories. The Enterprise Directory contains the “gold standard” for access privileges assigned to employees, contractors, and trading partners. Legacy directories will be synchronized to the Enterprise Directory.
>
> Secure communications with the outside world: Communicating securely with the outside world (e.g., DHHS, Blue Cross of Minnesota, or the general public) requires that the outside world be able to obtain public keys for HCFA and vice versa. The X.500 Enterprise Directory supports this function by providing knowledge links to DHHS and replicating data to others.

The target PKI architecture, illustrated in Exhibit 4-2, is integrated with the directory architecture. HCFA will arrange its own Registration Authority (RA) and CA. The RA is a person and a computing platform that confirms the identity of users or resources and approves the issuance of digital certificates that formally bind the user or resource to a public key. The CA manages certificates by sending them to the Enterprise Directory for posting, generating, and distributing Certificate Revocation Lists (CRLs) for certificates that are no longer valid.

Exhibit 4-2 shows a hierarchical trust relationship among the HCFA, DHHS, and Federal PKI Bridge CAs. This relationship will permit the HCFA CA to exchange certificates and CRLs with both entities to enable secure communications and digital signature with organizations that are known and trusted at the department level or at the Federal Government level.

There are four important categories of security-related functions supported by the PKI architecture: digital signature, strong authentication, public key enabled applications, and private virtual networks. These functions are described in Subsection 4.1.2.

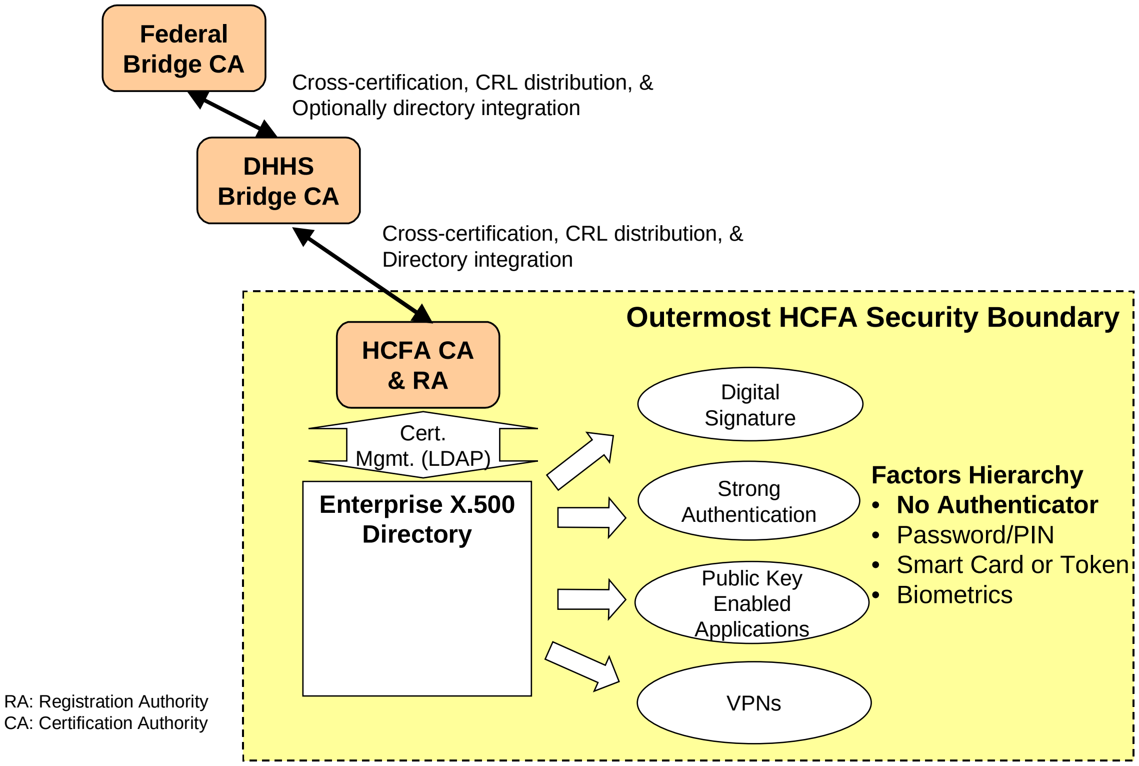

Federal Bridge CA
Cross-certification, CRL distribution, & Optionally directory integration
DHHS Bridge CA
Cross-certification, CRL distribution, & Directory integration
Outermost HCFA Security Boundary
HCFA CA & RA
Cert. Mgmt. (LDAP)
Enterprise X.500 Directory
Digital Signature
Strong Authentication
Public Key Enabled Applications
VPNs
Factors Hierarchy
No Authenticator
Password/PIN
Smart Card or Token
Biometrics
RA: Registration Authority
CA: Certification Authority

Exhibit 4-2 The Target HCFA PKI Architecture

4.1.2 *Confidentiality, Integrity, and Availability Services*

Technical protection measures are traditionally grouped into three high level categories: confidentiality, integrity, and availability. *Confidentiality* measures include encryption mechanisms (e.g., virtual private networks, end-to-end and link level encryption) to ensure that the privacy of information is maintained. *Integrity* measures enhance the reliability of information by guarding against unauthorized alteration. A key tool here is digital signature, also tied to the PKI initiative. The architecture will establish the goal of implementing digital signature technology both to reduce reliance on “wet-signed” paper documents, and to enhance the integrity of HCFA information assets. Strong authentication, using certificates provided through the PKI initiative, is a mandatory prerequisite to both confidentiality and integrity. *Availability* measures seek to ensure that information assets are accessible to internal and external users when needed, and guard against “denial of service” attacks. Availability protection measures such as planned redundancy will be used to mitigate availability risks created by the potential for system component failures. Protection measures such as firewalls and router filters will be used to mitigate availability risks created by denial of service attacks.

Volume 5 of the HCFA ITA identifies ten basic security services: 1) Physical Security; 2) Firewalls; 3) Intrusion Detection; 4) Access Control; 5) Authentication; 6) Privacy and Integrity (Encryption); 7) Electronic Signature/Non-repudiation; 8) Virus Protection; 9) Audit Trail Creation and Analysis; and 10) Database Security. These services are addressed from a technical measure perspective below and summarized in Exhibit 4-3.

Basic Service Areas*	AS-IS Technical Measure	TO-BE Technical Measure
Physical Security	Two level building security for Central Office and Data Center	Continued physical security; Integrated smart card access control
Firewalls	Use at connection to Internet	Use at Boundary Points
Intrusion Detection	Re-active Some limited monitoring	Automated monitoring of limited entry/exit points; Pro-active with integrated action plan
Access Control	Platform-specific access control lists	RBAC-based, centrally managed access
Authentication	User ID and password-based with limited smart card pilots	Private key-based with multi-factor identification
Privacy & Integrity (Encryption)	Application-specific, primarily DES-based	PKI-based key mgmt; FIPS 140-1 approved encryption; SSL
Electronic Signature/Non-repudiation	None	FIPS 140-1 Digital Signature; Escrow for encryption keys (not signing keys)
Virus Prevention	Workstation-based and server-based program	Workstation and server-based program; signed applications
Audit Trail Creation & Analysis	Logs generated on a platform-specific basis	Consistent log content, directive data reduction and analysis
Database Security	Proprietary, DBMS-specific; DAC	PKI-enabled; RBAC-integrated; DAC

*Reference ITA Volume 5, Section 5.5.8 Security

Exhibit 4-3 Summary of AS-IS and TO-BE Technical Protection Measures

Physical Security: HCFA currently implements two levels of building access control. Guards, who check for proper badges or other identification, monitor entry to HCFA building. Access to the data center is further restricted to authorized personnel. The Target Architecture retains this level of physical security, but adds the use of multi-factor (please refer to the paragraph on authentication below for a definition of “multi-factor”) access control based on private encryption keys to manage entry and exit. In the Target Architecture, employees and appropriate contractors will be issued smart cards or tokens that store a private key and other essential authentication information.

Firewalls: Currently, HCFA uses firewalls to establish a secure boundary between internal business assets and the public network. In the target architecture, HCFA will use firewalls more extensively to establish internal security boundaries. Exhibit 4-1 illustrated the use of firewalls to enforce the security boundaries within the Enterprise Directory Architecture. Exhibit 4-4 demonstrates the use of firewalls at boundaries between the data center administration, Intranet, and Extranet boundaries.

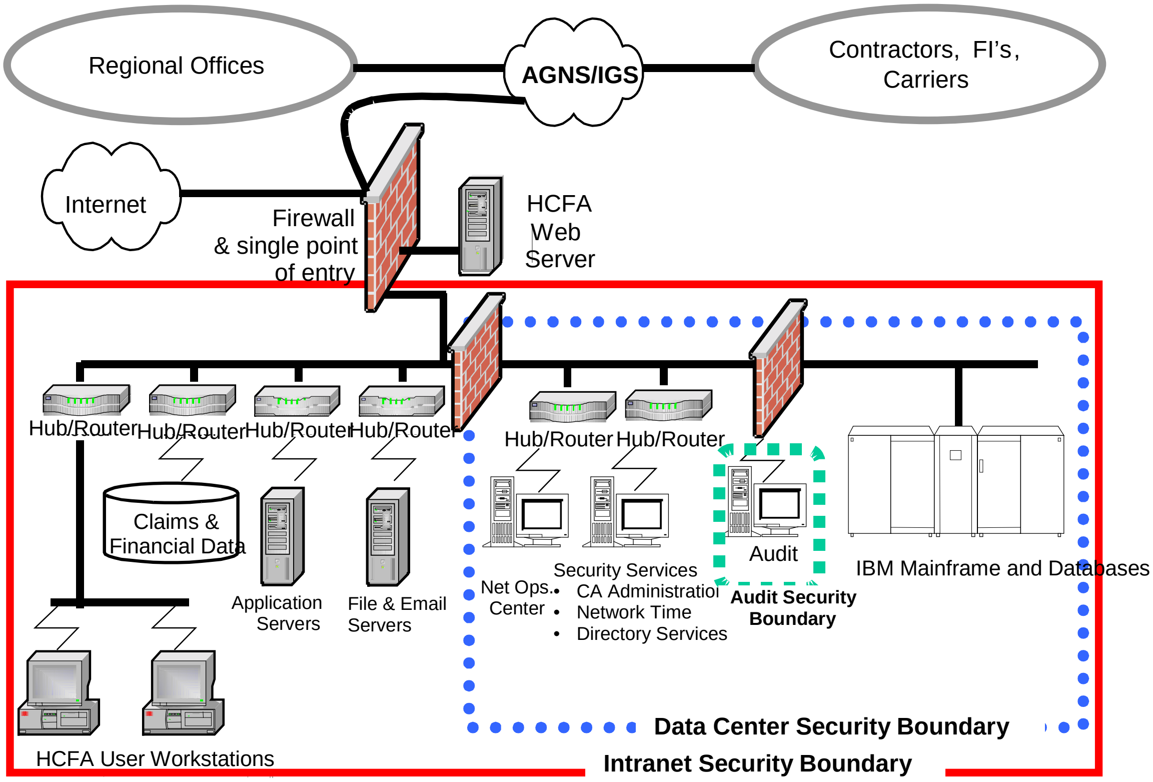


Exhibit 4-4 Logical Depiction of the Target Architecture

Intrusion Detection: Currently, intrusion detection is primarily a reactive function that responds as attacks are identified. In the target architecture, HCFA will use intrusion detection software to monitor network and host-based assets and employ a computer emergency response team to report and respond when incidents occur.

Authentication and Access Control: Although the mainframe computer currently provides the authoritative source for user account status, to a great extent, authentication and access control is based on the proprietary mechanisms that reside in HCFA's distributed computing platforms (e.g., Windows NT, Unix, and

Novell NetWare authentication and access control). HCFA currently employs userID and password as the principal authentication technology. The target architecture employs strong authentication, and centrally managed role-based access control (RBAC). At the core of this new approach, the fundamental authenticator will be the demonstration of a user’s knowledge of his/her private key. The authentication process will include multi-level factors. The factors hierarchy, illustrated in Exhibit 4-5, is classically: (1) something I know, (2) something I have, (3) something about me. As indicated in the exhibit, highly secure positions will require all three factors.

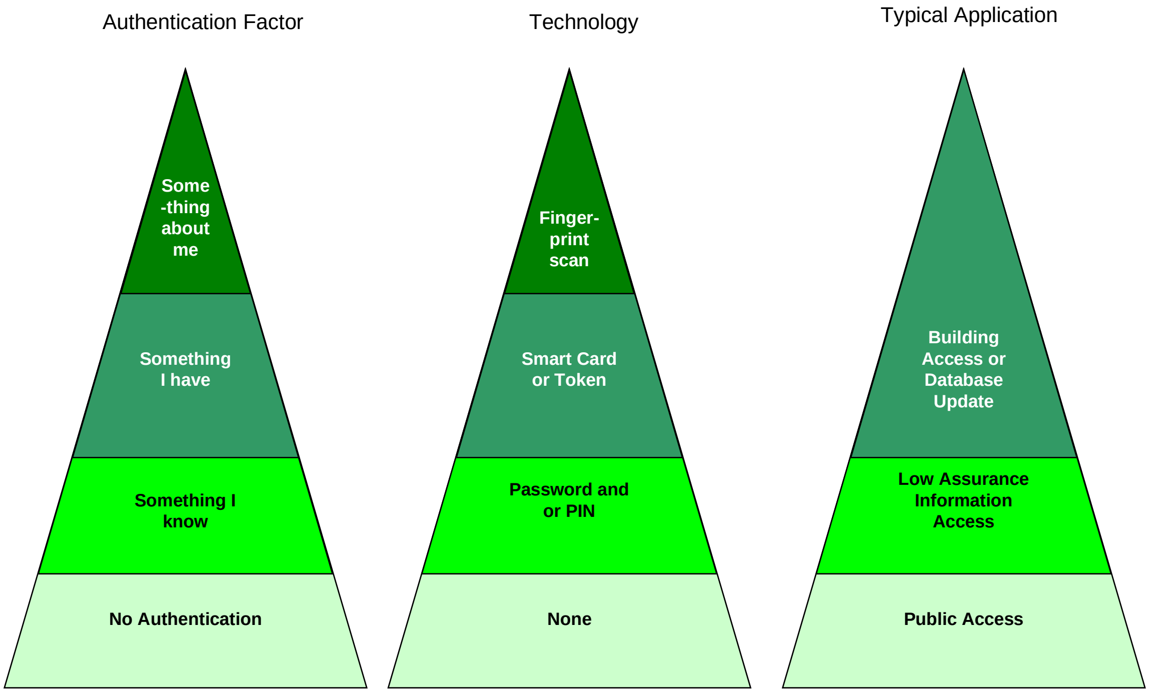


Exhibit 4-5 Authentication Factors Hierarchy

HCFA's RBAC strategy will map access privileges onto roles. Roles may include highly trusted positions, such as RACF system administrator, or more casual roles such as a Mid-Atlantic Host Common Working File Reviewer. Some roles will require access mappings at a very low level of granularity – down to the database record level. Exhibit 4-6 provides an example of high and low level granularity in role definition.

Role	Example System	
	CWF*	Some Public System**
System Administrator	Read, write, and modify all records.	Read all records.
HCFA Staff	Read records for all jurisdictions, write/modify records for area of responsibility.	Read all records.
Claims Processor	Read only records from jurisdiction Claims Processor represents.	Read all records.

*Fine-grained access control
**Coarse-grained access control

Exhibit 4-6 An Example of Role-based Access Control (RBAC) Granularity

Privacy and Integrity (Encryption): Depending upon the risk of inappropriate disclosure and cost for information protection, HCFA system designers, analysts, and managers will base their decision to encrypt and the encryption tactics on an application-by-application basis. In all cases, the exchange of authentication information and HIPAA/privacy act protected information will be encrypted in transit. The target architecture requires that all keys used for encryption be managed under the HCFA PKI. It also requires that encryption algorithms applied for the purposes of supporting privacy and integrity adhere to FIPS PUB 140-1.

Virtual Private Networks (VPNs) and Secure Socket Layer (SSL) are two technologies that HCFA will use to implement privacy and integrity. The target architecture will employ VPNs to establish secured sub-channels on an otherwise public, unsecured communications medium. The authentication and key exchange necessary to establish the secure sub-channels will be supported by the PKI. SSL is frequently used in electronic commerce to secure the communications path between a consumer and an e-merchant. The target architecture incorporates this well-proven protocol with some provisos. Namely, E-commerce’s use of SSL typically does not include authentication of the client, and HCFA will only use SSL in this manner when client authentication is not critical to the privacy and integrity of the transaction.

Electronic Signature/non-repudiation: Digital signature is an integrity function. To sign a document or other information resource digitally, the signatory encrypts a representation of the document with his/her private key. The PKI architecture is designed to help guarantee that only the signatory has knowledge of his/her private key. The HCFA Enterprise Directory stores the keys necessary to verify a digital signature, but only the signatory has knowledge of his/her private (signing) key. If the PKI is properly managed and the digital signature algorithm is strong, the signature cannot be repudiated; i.e. the signatory will not be able credibly to deny having digitally signed a document. The goal of the HCFA security technology architecture is to ensure non-repudiated digital signatures. All HCFA electronic signature algorithms will be FIPS PUB 140-1 compliant.

Virus Protection: HCFA has an aggressive program in place to maintain virus detection and removal software on both servers and workstations. The target architecture will maintain this program. In addition, the target includes digitally signed applications software executables to further reduce the threat of rogue software, Trojan horses, and viruses.

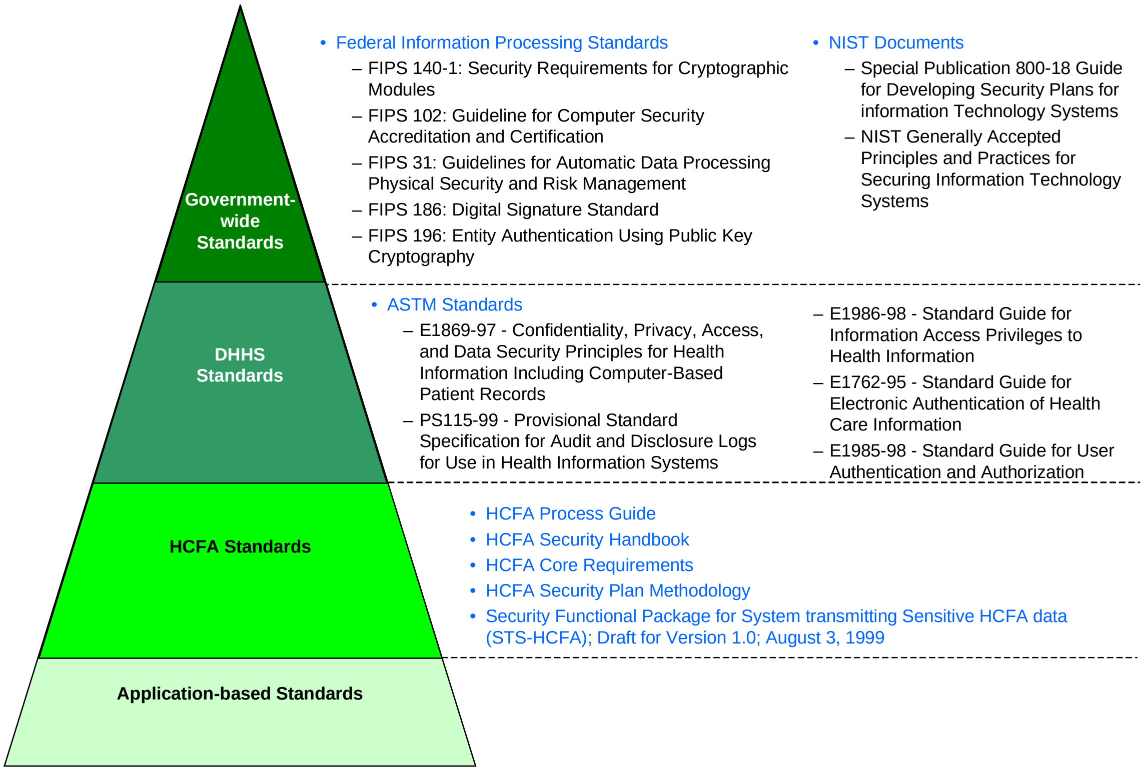
Audit Trail Creation and Analysis: All HCFA information systems will create audit logs following the guidance specified in Section 4.5 of this document. The target architecture requires a tunable audit and logging analysis. The analysis should provide sufficient filtering facilities to reduce large volumes of log data to useful information. In addition, the analysis should allow auditing and logging to be varied in intensity in response to ambient security threat conditions and targeted analyses.

Database Security: Currently, HCFA mission-critical business applications and databases use proprietary authentication mechanisms (generally userID/password-based) and often do not provide secure connectivity. Under the target architecture, database authentication and access control will be public key enabled and role-based. This means that a user will employ a multi-factor authentication procedure based on knowledge of his/her private key to obtain access to a database. Once authentication is complete, access, sometimes down to the record level, will be granted or denied based on the user’s roles and associated privileges. Database security will be implemented on a discretionary access control (DAC) basis.

4.1.3 *Standards*

There is a hierarchy of standards, ranging from most general to most specific, to which all systems under the Security target architecture must adhere. Exhibit 4-7 illustrates that hierarchy and populates it by citing the applicable standards documents.

In general, HCFA will base the target Security Architecture technical measures on FIPS PUB 140-1 standards to the greatest practical extent. The key standards in this area are X.500 directories: X.509 certificates: RSA, DSA, and ECDSA for public key cryptography; and DES and Triple DES (soon to be replaced by AES) for symmetric (i.e., secret key) encryption.



- Federal Information Processing Standards
  - FIPS 140-1: Security Requirements for Cryptographic Modules
  - FIPS 102: Guideline for Computer Security Accreditation and Certification
  - FIPS 31: Guidelines for Automatic Data Processing Physical Security and Risk Management
  - FIPS 186: Digital Signature Standard
  - FIPS 196: Entity Authentication Using Public Key Cryptography
- NIST Documents
  - Special Publication 800-18 Guide for Developing Security Plans for information Technology Systems
  - NIST Generally Accepted Principles and Practices for Securing Information Technology Systems

- ASTM Standards
  - E1869-97 - Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records
  - PS115-99 - Provisional Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
  - E1986-98 - Standard Guide for Information Access Privileges to Health Information
  - E1762-95 - Standard Guide for Electronic Authentication of Health Care Information
  - E1985-98 - Standard Guide for User Authentication and Authorization

- HCFA Process Guide
- HCFA Security Handbook
- HCFA Core Requirements
- HCFA Security Plan Methodology
- Security Functional Package for System transmitting Sensitive HCFA data (STS-HCFA); Draft for Version 1.0; August 3, 1999

Exhibit 4-7 Standards and Guidance

4.2 Physical Protection, Contingency Planning, and Disaster Recovery

Each HCFA information asset should have plans for physical protection and a disaster recovery plan. Preparation of these plans is the responsibility of the manager of the asset. This section summarizes some of the issues that should be addressed when dealing with physical access, environmental issues, contingency planning, and disaster recovery. It is not the intent of this document to include a Physical Security Plan. The following sections delineate some elements that should be addressed by the Physical Security Plan.

4.2.1 *Physical Protection*

HCFA will have a documented plan for the physical control of information assets. The plan will include the data center, assets located within HCFA office space, and removable assets, e.g., laptops and documents.

The physical protection plan should address such issues as:

- Physical access control including emergency egress.
- Visitor control.
- Temperature and humidity monitoring and control.

- Protection from loss of power, including the availability of an uninterruptible power supply (UPS) and emergency lighting.
- Automatic smoke and heat detectors, and a fire fighting policy.

4.2.2 *Business Continuity and Contingency Planning (BCCP)*

Every effort must be made to avoid disruption of critical applications processed by automated data files and AIS facilities, HCFA must also be able to minimize, and be prepared to recover from, any disruption that does occur. A BCCP must be prepared in writing for all HCFA systems and databases, including those provided by contractors, that fulfill mission critical business functions, whether they be a facility, network, major application, or stand-alone workstation. BCCP's are documented as part of the organization's overall AIS Security Program.

Managers of HCFA's critical information assets must identify the potential consequences of undesirable events and the safeguards needed to counter act their effects. Safeguards included in the BCCP must be selected based on whether they are needed to maintain a minimum level of operation for the affected systems. Guidelines for development of the BCCP are found in the HCFA Information System Security Policy Standards and Guidelines Handbook.

Systems users conduct a risk assessment to gather quantitative data to assist them in making the above determinations. The results of the risk assessment assist the user by indicating:

- Critical applications and workloads
- Maximum tolerable delay for the processing of each deferred activity.
- Maximum permissible outage for each application and workload.

Backup and recovery procedures will be prepared for each information system. These procedures should address:

- Frequency of backups to prevent unacceptable loss of information should equipment failure or other processing interruptions occur.
- Testing and demonstration of the ability to restore information.
- Retention duration of archive copies of backup.
- Frequency of checkpoint triggered saves of transactions throughout the daily processing period so that an appropriate restart, given the criticality of the data, volume of transactions, and size of data in each transaction, can be achieved.
- Frequency of a full system backup of both data and software.

- Availability of an offsite storage facility and its security.

Managers of HCFA's critical information assets must prepare disaster recovery plans for the assets under their control. Disaster recovery and business continuity planning inherently requires continuous review and update of activities, assigned roles, and responsibilities. The plans will be distributed to the required participants, who will be measured and evaluated based upon their performance in a staged test of a hypothetical scenario. BCCP’s must be part of the SSP, either referential or as an appendix.

Depending of the nature of the system involved, these plans should address:

- Availability of a hot site at which the recovery team is able to load system software and the most critical applications and data needed for the organization to meet its most pressing obligations to the public.

- The immediate required actions, to move operations to an alternate processing data center, and resume normal processing operations. The plan will outline in detail the procurement of processing equipment, the description and location of all equipment at the alternate site, the security of the alternate site, and the security procedures required in processing at the alternate site.

During the year, a random section of the plan will be selected for an unannounced incremental test of that section. Annually, a document will be prepared describing the results of the test, and comparing that to the expected results, noting areas where the plan is no longer adequate due to changing circumstances.

4.3 Administrative Security, Personnel Security, and Procedure

Administrative processes must support good security practices and integrate with the architecture. HCFA will develop and document administrative security procedures to address:

- A virus protection strategy that addresses prevention, detection, containment, elimination, and recovery from virus contamination.

- Procedures for software development and maintenance, including emergency maintenance, will include sufficient version control and authorization of updates, to ensure that only management-approved changes are placed into the production environment.

- System Security Plans will be developed for all new and existing applications that are in compliance with:

  - National Institute of Standards & Technology (NIST) Special Publication 800-18 “Guide for Developing Security Plans for Information Technology Systems”

  - OMB Circular A-130

  - Management of Federal Information resources," Appendix III
  - "Security of Federal Automated Information Resources"
  - Public Law 100-235, "Computer Security Act of 1987"
  - Federal Information System Controls Audit Manual

- Role-based access controls and management policy that define individual or group role definitions within domains. Inclusion within the role defines which users are authorized to access which asset and in what capacity.

- Background checks and clearance processes as they apply to Government employees, contractors, and trading partners who would have permission to access sensitive information or physical assets.

- Segregation of duties within the entire security management process.

- A process to ensure that responses to security breaches reported by HCFA users are well documented and available for review.

4.4 Training and Awareness

Many of the classic attacks on information systems start with "social engineering." Social engineering is a euphemism that recognizes those individuals, or more specifically, the poor security practices of individuals, are frequently the weakest link in the security assurance chain. The HCFA security training and awareness program seeks to strengthen this link by both informing users of the proper use of security mechanisms, and by increasing understanding of the threats to business assets and the ways to mitigate the risks.

HCFA's Information System Security Initiative provides for a comprehensive IT Security Training and Awareness Plan. Because administrative procedures are crucial to all of the other protection measures, training will be tailored to all levels of the user community. The training will be computer-based or tele-learning, to afford the maximum opportunity to participate regardless of geographic location. Participation in and successful completion of training, and the actual retention of the content, will be measured and monitored to ensure compliance.

HCFA security training will have a tiered structure consisting of: 1) pre-packaged training programs, and 2) customized HCFA security training. All personnel will be trained appropriately regarding their roles in HCFA security policy. Security awareness training will include both general and role-specific training. Refresher training will be provided to all HCFA and contractor staff annually.

4.5 Logging and Auditing

Security should be proactive. A number of proactive actions should be part of the security plan for each information system. In the areas of logging, auditing, and intrusion protection, security plans should attend to:

- Layered defense. These mechanisms serve to measure security performance, and may serve as indicators that additional protections are needed.

- Auditing of all accesses to sensitive/critical information and physical assets. The ability to monitor for potential security incidents will be limited to a small staff in support of HCFA's separation of duty policy.

- Role-based control of all execution of programs and utility programs that grant a higher level of access than is normally available to a user, whether directly or indirectly.

- Audit logs that record, in a centralized repository, logon and logoff; instances where a role is authorized access or denied access; the individual acting in that role; the sensitivity level of the data or other asset accessed; what type of access was performed or attempted (e.g., whether the nature of the requested action was to create, read, update, execute a program, or delete); and where appropriate what specific fields or finely granular data type name and description the access attempt involved.

- Audit logs that also record the date and time of each event's occurrence, and a unique program identifier of each program, which is the ultimate authorizing entity where there is no individual acting in that role, and where that program is logically (in what security domain) or physically located.

- Computer systems employed in the logging function that safeguard their programming code from unauthorized modification.

- Auditing and monitoring reporting processes should provide useful data for decision makers, not just reams of detailed data that need further processing to be made meaningful.

- Independent reviewers to perform monitoring of the sufficiency of documented controls and the extent of compliance with stated physical access controls and environmental controls, security audit trail logging, and intrusion detection procedures.

- Recording all actions, using the emergency maintenance accounts, in the audit log. A predetermined, accountable individual or automated process will determine the validity of each action.

- Retention period of logs.

- Semi-autonomous software agents to detect intrusion attempts regarding networks and systems, and take mitigating action, react, and adapt without supervision. The software agents could be empowered to turn off services, close ports, adjust firewalls, replace agents with fresh agents, use alternate means of communication, or send out probes to locate and assess the attacker.

4.6 Incident Detection and Response Capability

It is both theoretically and practically impossible to devise a flawless Security Architecture. Therefore, an incident detection and response capability is a critical part of maintaining a high level of information assurance and asset protection. Computer systems and communication networks are subject to a variety of sophisticated threats, many of which have emerged only during the past decade with the enormous growth in the use of computer workstations, local area networks (LANs), and the internet. Although, prevention must be the main line of defense, when a systems security incident occurs there must be on-call experts who can quickly control and contain sophisticated intrusions, limit damage, eliminate the problem, and restore normal operations.

Intrusion detection consists of the real-time identification of unauthorized use, misuse, and abuse of computer assets by both internal network user and external hackers. Intrusion detection is a challenging task because of the proliferation of network connectivity, heterogeneous computer environments, mixed operating systems, various communication protocols and a significant assortment of popular and proprietary applications.

Incident detection will be accomplished in the target architecture with the use of automated detection software tools, both network and host-based. Network intrusion detection utilizes traffic analysis to compare session data against a known database of popular operating system and application attack signatures.

Host-based detection analyzes operating system and application system logs and events to compare systems events against a database of known security violations and custom policies. Both detection methods react by logging files or sessions, alerting the administrator, possible termination of the session/activity, and allow for hardening of a firewall. The combination of network and host-based intrusion detection software provides significant attack protection and policy enforcement.

Intrusion response consists of the real-time decisions and actions taken to minimize incident-related effects on the activity’s assets and to mitigate residual security risk based on available evidence from the incident. The HCFA Computer Emergency Response Team (CERT) will be chartered by the Chief Information Officer and is responsible for real-time detection and response of potential security incidents. The CERT responsibilities will be restricted to a dedicated staff in support of HCFA’s separation of duty policy.

The CERT will be:

1. Continually aware of pending virus threats and prepared with countermeasures;

2. Proactive in identifying potential intrusions and ready to counter threats to information assets;

3. Responsible for communicating existing threats and response procedures to users and managers throughout the enterprise;

4. Responsible for Department of Health and Human Services reporting requirements; and

5. The coordination point for incident responses that require participation of organizations scattered throughout HCFA to respond effectively.

5 Architecture Management and Governance

The procedures for maintaining and enforcing the IT Architecture are addressed in Volume 7 of the ITA The Security Architecture. This section details how maintenance and governance will be integrated into the ITA process and discusses some of the features unique to IT security. The IT Architecture management and governance process is particularly important for security because:

- One of the basic security design principles, stated in Section 2 of this document, is that HCFA will design security into systems, rather than retrofit it as an afterthought. As a result, architecture compliance must be integrated into the IT Investment Management Technical Review Process.

- Both security technology and threats are changing rapidly. In order to remain effective and relevant, the HCFA Security Architecture must continually evolve.

The following subsections address maintenance and compliance processes as they fit into the broader ITA governance framework.

5.1 Architecture Maintenance

The stimulus for changes to the Security Architecture may arise from four sources: 1) a new information system is upgraded or developed; 2) a change in regulation occurs; 3) a change in technology occurs; or 4) a new threat arises. The ITA Security Architecture Committee is a critical component in maintaining the architecture.

The Security Architecture Committee, one of five committees supporting the IT Council, will track environmental changes to determine when it is necessary to submit a Security Architecture change proposal and evaluate and facilitate change requests that are sourced from other parts of the HCFA community. New policies, once approved by the IT Council and the CIO, will become part of the security of the ITA.

Exhibit 5-1 identifies some of the emerging technologies and standards that will be candidates for incorporation into the Security Architecture in the near future.

Emerging Technology	Description	Importance to HCFA Security Architecture	Projected Timeframe for Emergence
IP Version 6	The update to the current Internet Protocol (IP version 4).	Offers link level integrity and privacy. Key to VPNs and prevention of spoofing attacks. Currently not in wide use.	5 years.
Common criteria	An international scale for ranking the assurance level of an information system.	Provides a measure of system assurance level. Not widely implemented and few evaluation labs.	2 years
FIPS 140-2	Update of the current standard (includes lists of encryption).	A draft on the verge of approval.	1 year.
AES	The replacement for DES as the national standard symmetric key encryption algorithm.	Replacement for DES—leading candidates are fast and secure. Final evaluation is in progress at NIST; decision expected Summer 2000.	1 year for decision on AES protocol; 5+ years for full adoption.
Public Key Enabled Kerberos	Non-proprietary protocol for secure, single sign-on network authentication.	Mature (in secret key implementation) open source protocol. Native network authentication for Windows 2000.	2 to 3 years for public enabled Kerberos variant.

Exhibit 5-1 Emerging Technologies – Candidates for Inclusion in HCFA Security Architecture

5.2 Architecture Compliance

Compliance with Security Architecture will be embedded in the IT investment review process and the System Development Processes. HCFA will use investment review and a proactive implementation program to evolve from the current to the target Security Architecture.

6 Summary

The HCFA information Security Architecture has been prepared with several thoughts in mind. HCFA information Security Architecture must:

- Protect HCFA's information assets;
- Be straightforward and easy to understand for staff at all levels;
- Not interfere with, or prevent HCFA from conducting its business; and
- Comply with all Federal laws, regulations, standards, and guidelines.

The reader of this document has been introduced to HCFA's information security principles and policies, and HCFA's current and target Security Architectures. The target architecture will:

- Improve the security of HCFA's information assets;
- Provide a consistent information security environment throughout HCFA;
- Clearly delineate security responsibilities; and
- Provide a guideline for implementation of security precautions for HCFA's IT systems.

IT security technology evolves at a rapid pace. HCFA's Security Architecture must similarly evolve and be kept current to ensure the protection of HCFA's information assets.

> *This document does not stand-alone. It is an integral part of HCFA's overall IT Architecture. Implementing the Security Architecture will require additional documents as well, such as the HCFA System Security Plan Methodology, the HCFA Information Security Policy, Standards and Guidelines Handbook, and specific detailed procedures for technical aspects of the target Security Architecture.*