United States Department of
Health & Human Services

Enterprise Architecture
Program Management Office

HHS Enterprise Transition Strategy 2008

Version 1.0
February 2008

Approvals

The Health and Human Services (HHS) Transition Strategy describes gaps identified between current and future states of the organization, and plans and activities proposed or initiated by the Department and its Operating Divisions to fill those gaps. The Transition Strategy also provides HHS strategies and interim milestones for implementing planned measures to achieve progress towards its target vision.

Approved by:

Signature: /s/

John Teeter
Director, Office of Enterprise Architecture
HHS Chief Enterprise Architect

Date: February 28, 2008

Signature: /s/

Michael W. Carleton
Deputy Assistant Secretary for Information Technology
HHS Chief Information Officer

Date: February 28, 2008

Table of Contents

List of Exhibits

Document Change History

Version Number	Release Date	Summary of Changes
n/a	2/28/2007	Previous Transition Plans were produced in 2005, 2006 and 2007
0.5	1/17/2008	Transition contents revised to reflect segments
1.0	2/28/2008	Re-focus of milestones to next year and incorporation of FY2010 investments

1 Introduction

The Department of Health and Human Services (HHS) Office of Enterprise Architecture manages an Enterprise Architecture (EA) Program, under the leadership of the HHS Chief Enterprise Architect (CEA). The Office of Enterprise Architecture within the Office of the Chief Information Officer (OCIO) oversees many of the Department's core strategic planning and accountability functions, including information security, capital planning and investment control, information resources strategic planning, and of course, enterprise architecture. The HHS EA Program fulfills multiple Federal mandates related to planning and managing information technology (IT) investments and supporting organizational effectiveness at the Department, Staff Division (STAFFDIV), and Operating Division (OPDIV) levels, and with relevant government-wide initiatives.

Key legislative and management drivers for the HHS EA Program include the Information Technology Management Reform Act of 1996 (Clinger-Cohen), the E-Government Act of 2002, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Government Performance Results Act of 1993 (GPRA), and guidance from the Office of Management and Budget (OMB) including Circulars A-11, A-127, and A-130. In addition, the HHS EA Program ensures the Department's compliance with OMB's Federal Enterprise Architecture (FEA) and Federal Transition Framework (FTF), and responds to regular EA maturity assessments performed by the Government Accountability Office (GAO) and OMB.

1.1 Document Structure

This Transition Strategy is organized using the following structure:

Part 1 Introduction (this section) provides a general description of the purpose, scope and objectives, audience, approach, and methodology for the HHS Enterprise Transition Strategy.

Part 2 Transition Planning Drivers references strategic goals and objectives, internal and external mandates, Departmental commitments and obligations, and other drivers influencing the declaration, prioritization, sequencing, and execution of HHS initiatives.

Part 3 Major HHS Initiatives summarizes the major current or planned initiatives for HHS in 2008, especially those in support of goals and objectives articulated in the HHS Strategic Plan and HHS IRM Strategic Plan. This section addresses segments under development or completed during the previous planning year. Where appropriate, planning milestones and other relevant information is included from the FY2010 prospective IT investment portfolio.

Part 4 Transition Planning Milestones reviews progress against milestones specified during the 2007 transition planning process, and summarizes key transition performance milestones targeted for 2008-2010.

Appendix A HHS IT Investment Alignment summarizes HHS major and tactical IT investments proposed for inclusion in the FY2010 IT investment portfolio, showing the primary alignment of each investment to HHS segments.

Appendix B HHS Alignment to the FTF summarizes HHS IT investment alignment to each of the 18 mandatory Federal Transition Framework initiatives.

Appendix C HHS IT Investment Milestones provides quarterly milestones for HHS major and tactical investments proposed for inclusion in the FY2010 IT investment portfolio. Due to the length of this appendix, it is provided as a separate document to the Enterprise Transition Strategy.

Appendix D provides a listing and descriptions of acronyms and abbreviations using in the document.

Appendix E provides a listing of references used in the preparation of this document.

1.2 Purpose

The HHS Enterprise Transition Strategy is an annual checkpoint on the status and performance of activities and initiatives currently in progress that move the Department closer to its strategic vision. HHS produces and maintains a five-year Strategic Plan, in which HHS describes a long-term vision for the Department, establishes enterprise goals and objectives, and highlights areas of emphasis and proposes initiatives on which HHS will focus during the strategic planning timeline. The current HHS Strategic Plan covers the period from 2007 to 2012. The HHS Office of the Chief Information Officer is responsible for a similar five-year strategic plan focused on information resources management. The most recent version of the HHS IRM Strategic Plan also covers the 2007-2012 planning horizon. Both strategic plans are updated every three years. The Enterprise Transition Strategy incorporates progress measures for initiatives from both strategic plans.

The Enterprise Transition Strategy provides an annual status of accomplishments made in the previous year and anticipated progress to be made in the coming year. It reflects planned budgetary commitments as captured in the HHS IT portfolio and addresses mandated activities regardless of their actual funding status. In this way the Enterprise Transition Strategy can help HHS draw attention to obligations, strategic gaps, and other risk areas, and provide recommendations for mitigating any such risks. The Enterprise Transition Strategy is also an important tool to support accurate alignment of IT investments to business strategies and programs. This alignment will help HHS improve its programs' performance as measured by the Office of Management and Budget's Program Assessment and Rating Tool (PART).

1.3 Overview of this Document

This document, the HHS Enterprise Transition Strategy 2008, describes the strategy and sequencing to evolve from HHS' current baseline, representing fiscal year 2008, to achieve the strategic vision articulated in the current HHS Information Resources Management Strategic Plan 2007-2012 and HHS Strategic Plan 2007-2012. The Enterprise Transition Strategy has a shorter-term perspective than the strategic plans, generally covering a three-year span comprising the current fiscal year, the subsequent fiscal year (for which the proposed IT investment portfolio has already been approved), and the following fiscal year that is the focus of the current budget planning cycle. For the 2008 Transition Strategy, the planning horizon covers fiscal years 2008,

2009, and 2010. The transition from the baseline architecture to a target architecture consistent with the Department's vision is an iterative process.

The Transition Strategy focuses on transitional activities and performance milestones for initiatives that, when fully implemented, will become part of the target architecture for HHS. Initiatives and projects that have already achieved implementation – including investments in operations and maintenance or "steady-state" phases – are already part of the target architecture and are therefore not emphasized in the Enterprise Transition Strategy.

The HHS Enterprise Transition Strategy 2008 describes the major strategic and tactical drivers influencing the investments, initiatives, and activities on which HHS will focus in 2008-2010. Transition drivers include internal policies, plans, and initiatives as well as external mandates such as legislation, inter-agency agreements, and government-wide initiatives. The scope of this document includes significant HHS initiatives and programs, and plans and activities undertaken to align to or comply with cross-agency or other federal initiatives in which HHS participates.

Related documents that provide additional details of the HHS Enterprise Transition Strategy and the enterprise architecture's role in enterprise transition include:

- The HHS Strategic Plan 2007-2012
- The HHS Information Resources Management Strategic Plan 2007-2012
- The HHS Performance Management Plan
- The HHS EA Governance Plan
- The HHS EA Program Management Plan
- The HHS EA Program Communications Plan
- The HHS EA Framework

This plan complements related HHS policies and guidance, including:

- HHS OCIO Policy for IT Capital Planning and Investment Control
- HHS OCIO CPIC Procedures
- HHS OCIO IT Policy for Enterprise Architecture
- HHS Enterprise Performance Life Cycle
- HHS Information Security Program Policy

1.4 Audience

The intended audience for the Transition Strategy includes all HHS EA stakeholders, as well as those interested in the operational activities of the HHS EA Program. These stakeholders include:

- HHS Assistant Secretary for Resources and Technology (ASRT)
- HHS Chief Information Officer (OCIO)
- HHS Chief Enterprise Architect (CEA)
- HHS Information Technology Investment Review Board (ITIRB)

- HHS CIO Council
- HHS Enterprise Architecture Review Board (EARB)
- Program Staff and Contractors supporting the HHS Office of Enterprise Architecture
- HHS OPDIVs and staff involved Enterprise Architecture activities
- HHS OPDIV investment, business, and technical review boards
- HHS and OPDIV Capital Planning and Investment Control (CPIC) programs and staff
- HHS and OPDIV IT Program and Project Managers and staff, including contractors
- Business Owners of programs, investments, and business functional areas and processes
- OMB Line of Business programs and staff, including Federal Health Architecture (FHA), Human Resources LOB, Financial Management LOB, Grants Management LOB, Information Systems Security LOB, and IT Infrastructure Optimization LOB
- Federal Health Information Technology programs and staff, including the Office of the National Coordinator for Health IT
- Programs and staff of e-Government and Federal Transition Framework initiatives in which HHS participates or the products of which HHS is obligated to incorporate in its own planning and operations.

1.5 Transition Planning Approach

The enterprise architecture is a strategic resource that helps HHS plan, invest in, and implement information technology solutions to meet business needs and help manage the IT investment portfolio. It provides a mechanism for understanding and managing complexity and change. EA products identify the alignment of organizational business and management processes, data flows, and technology. They also enable identification of capability gaps and duplication. The role of the enterprise architecture within the broader cycle of strategic planning and execution is reflected in the initial "Architect" phase of the iterative performance improvement lifecycle described by OMB, as depicted in Figure 1 (Source: FEA Practice Guidance, December 2006).

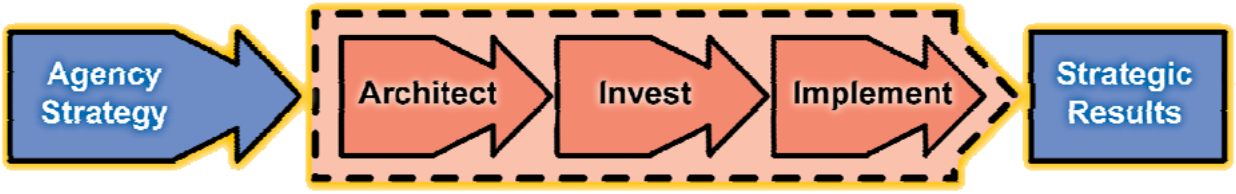


Figure 1: Performance Improvement Lifecycle

HHS is a large and diverse organization, with a broad mission and corresponding functional responsibilities at both the Department level and, especially, among the Operating Divisions. In order to identify mission-specific information resources management goals and objectives, the

IRM strategic planning process is structured around the nine business areas defined by the HHS Chief Enterprise Architect:

1. Access to Care
2. Health Care Administration
3. Health Care Delivery
4. Health Care Research and Practitioner Education
5. Human Services
6. Population Health Management and Consumer Safety
7. Information Resources Management
8. Management of Government Resources
9. Planning and Accountability

These business areas are used by HHS to help identify and coordinate work on common or shared business functions within and across the Department, Operating Divisions, and Staff Divisions, to group HHS IT investments, and to help apply appropriate stakeholders, subject matter experts, and other resources to strategic and transition planning activities. Since the publication of the most recent HHS Strategic Plan, these business areas also are used to facilitate program-to-investment alignment, as the business areas correspond closely to the strategic areas defined in the HHS Strategic Plan, as shown in Table 1, below.

Table 1: HHS Business Area Alignment with Strategic Planning Areas

Strategic Area (HHS Strategic Plan)	Business Areas (HHS OEA)
Health Care	Access to Care Health Care Administration Health Care Delivery
Public Health Promotion and Protection, Disease Prevention, and Emergency Preparedness	Population Health Management and Consumer Safety
Human Services	Human Services
Scientific Research and Development	Health Care Research and Practitioner Education
Responsible Stewardship and Effective Management	Information Resources Management Management of Government Resources Planning and Accountability

Each of the nine business areas is further decomposed into segments. Segments are discrete sets of business functions grouped according to similarities in mission, goals, objectives, and commonality of services and business processes. By focusing IRM strategic planning activities on segment-based perspectives, HHS is able both to capture and reflect mission-specific

priorities and to identify commonalities across segments and across the business areas in which the segments reside. This perspective helps ensure that strategic and tactical initiatives are planned and sequenced appropriately to focus appropriate efforts and resources on the areas of greatest impact for the enterprise. Individual initiative programs and investments maintain their own transition plans as part of program and project management, including establishing performance measures and milestones. In addition, HHS maintains Segment Transition Plans for each of the segments under development or for analysis after development. The HHS Enterprise Transition Strategy reflects a broader perspective covering all major initiatives, cross-segment priorities, and major milestones and commitments from cross-agency and government-wide initiatives.

1.6 Methodology

The HHS Enterprise Transition Strategy is produced and updated as a component of the annual strategic planning cycle. Beginning in 2006, the information resources management strategic planning process was modified to adopt a segment-based planning approach as a complement to enterprise-wide planning. The HHS Office of Enterprise Architecture convenes and facilitates a series of strategic and transition planning workshops with business and IT representation from all HHS Operating Divisions and many Staff Divisions. The scope of activities for each workshop includes a review of existing strategic goals and objectives from both the HHS Strategic Plan (i.e., the business strategy) and the HHS IRM Strategic Plan, a summary of current activities and IT investments, and a discussion of progress on initiatives against performance outcomes.

Both business-focused and IRM strategic planning follow a similar process for the development and update of the HHS strategic plans. At the broadest strategic level, planning process participants identify long-term goals, organized according to mission-oriented delineations of major activities across the Department and its Operating Divisions (OPDIVs). The goals articulate what the Department wants to achieve. A set of primary objectives is specified for each goal, to describe with more granularity what the Department will accomplish in pursuit of its goals. The planning process then focuses on the identification of discrete outcomes corresponding to different goals and objectives that, if realized, would demonstrate successful achievement of the goals and objectives. This hierarchy of goals, objectives, and outcomes provides the structure for the HHS Strategic Plan and the HHS IRM Strategic Plan.

The annual review of HHS strategic planning documentation and the update of the Enterprise Transition Strategy identifies current and existing initiatives and investments approved for inclusion in the IT portfolio for the current planning year. This process also identifies additional objectives and outcomes that may not have been incorporated in the strategic plans. Participants analyze the existing initiative and investment information against the collective set of objectives and intended outcomes, to identify any gaps between the baseline and target that are not adequately addressed by existing plans. This gap analysis, performed for each of the nine HHS Business Areas, helps identify new or emerging themes in terms of required or desired capabilities that information resources can deliver. The existence of gaps in existing plans can also influence revision or re-prioritization of initiatives and planned investments, to encourage the most effective use of IRM resources.

Performance measures provide another important input to transition planning. All current or proposed IT investments specify performance measurement indicators used to evaluate the success of the initiatives funded by the investment and, in most cases, to measure interim progress of the initiatives during their life cycles. HHS has developed a performance management framework – applicable across all of the business areas – that provides guidance to investment owners as to appropriate types of measures that should be specified for their initiatives or projects. Using a common performance management framework across all IT investments helps HHS implement consistent performance-based evaluation of initiatives, and use the results of that evaluation to help determine transition strategy and adjust sequencing plans as necessary.

The HHS approach to performance management recognizes the difference inherent in relevant performance measures and milestones depending on the status and relative maturity of a program, project, or investment. Initiatives and activities identified in the Enterprise Transition Strategy have, for the most part, not yet achieved full implementation, completion or operational capability, so the milestones used to track the performance of these initiatives and activities are measures of implementation.[1] Once full implementation and operational capability is achieved, HHS emphasizes the use of operational or outcome-driven performance measures and milestones, which are the focus of the HHS Performance Management Plan.

The Enterprise Transition Strategy addresses strategic planning drivers both internal and external to HHS, and several different types of initiatives and activities:

- Current and proposed investments up to and including the fiscal year 2010 IT portfolio;
- Segments prioritized and initiated for architectural development;
- Program-based initiatives, spanning multiple investments and projects;
- Strategic themes and potential new initiatives from the strategic planning process;
- Health IT initiatives in which HHS is a partner, member, or participant;
- Cross-agency federal initiatives including the Federal Transition Framework and E-Gov.

A single HHS initiative or activity may correspond to more than one of the above drivers.

[1] The use of distinct kinds of measures and milestones to reflect implementation is consistent with federal guidance on performance management and the selection of appropriate performance measures, including NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems* and the Government Performance and Results Act of 1993 (GPRA).

2 Transition Planning Drivers

This section summarizes internally and externally produced drivers influencing HHS initiatives. The Enterprise Transition Strategy is in many ways derivative of the HHS Strategic Plan and HHS Information Resources Management Strategic Plan, as both of those planning documents describe long-term vision for HHS and the goals, objectives, and outcomes related to realizing that vision. Initiatives highlighted in the Enterprise Transition Strategy include those explicitly called out in strategic planning documents published by HHS.

2.1 HHS Strategic Goals and Objectives

The HHS Strategic Plan 2007-2012 declares four goals (strategic planning areas), and four objectives corresponding to each goal. All HHS mission-related initiatives, programs, and investments have among their business drivers one or more of these goals and objectives. Initiatives, programs, and investments outside the core mission areas may align to one or more of these goals and objectives, or to the broad-based strategic goal of Responsible Stewardship and Effective Management.

Table 2: HHS Strategic Goals and Objectives

Goal 1: Health Care Improve the safety, quality, affordability and accessibility of health care, including behavioral health care and long-term care.
Objective 1.1: Broaden health insurance and long-term care coverage.
Objective 1.2: Increase health care service availability and accessibility.
Objective 1.3: Improve health care quality, safety, cost and value.
Objective 1.4: Recruit, develop and retain a competent health care workforce.
Goal 2: Public Health Promotion and Protection, Disease Prevention, and Emergency Preparedness Prevent and control disease, injury, illness and disability across the lifespan, and protect the public from infectious, occupational, environmental and terrorist threats.
Objective 2.1: Prevent the spread of infectious diseases.
Objective 2.2: Protect the public against injuries and environmental threats.
Objective 2.3: Promote and encourage preventive health care, including mental health, lifelong healthy behaviors and recovery.
Objective 2.4: Prepare for and respond to natural and man-made disasters.
Goal 3: Human Services Promote the economic and social well-being of individuals, families and communities.
Objective 3.1: Promote the economic independence and social well-being of individuals and families across the lifespan.
Objective 3.2: Protect the safety and foster the well-being of children and youth.
Objective 3.3: Encourage the development of strong, healthy and supportive communities.
Objective 3.4: Address the needs, strengths and abilities of vulnerable populations.
Goal 4: Scientific Research and Development Advance scientific and biomedical research and development related to health and human services.
Objective 4.1: Strengthen the pool of qualified health and behavioral science researchers.
Objective 4.2: Increase basic scientific knowledge to improve human health and development.
Objective 4.3: Conduct and oversee applied research to improve health and well-being.
Objective 4.4: Communicate and transfer research results into clinical, public health and human service practice.

The HHS IRM Strategic Plan 2007-2012 also specifies a set of IRM-specific goals and corresponding objectives, in a format that mirrors that found in the HHS Strategic Plan.

Table 3: HHS IRM Strategic Goals and Objectives

Goal 1: Provide a secure and trusted IT environment.
Objective 1.1: Enhance confidentiality, integrity, and availability of IT resources.
Objective 1.2: Protect IT assets and resources from unauthorized access or misuse.
Objective 1.3: Enhance security awareness and role-based training department-wide, inclusive of privacy.
Objective 1.4: Ensure security is incorporated into the lifecycle of every IRM asset.
Goal 2: : Enhance the quality, availability, sharing, and delivery of HHS information and services to citizens, employees, businesses, and government
Objective 2.1 Provide an intuitive web-presence to quickly and reliably deliver information and customer services internally and externally.
Objective 2.2: Leverage web services to conduct business securely with customers and stakeholders.
Objective 2.3: Ensure the availability and dissemination of information in preparation of or in response to local and national emergencies, significant business disruptions, or disaster Interruption.
Objective 2.4: Establish COOP planning, testing, and training.
Objective 2.5: Provide technologies enabling both HHS internal stakeholders (e.g., employees, OPDIVs, STAFFDIVs) and external stakeholders (e.g., States, Municipalities, vendors) to work collaboratively and share knowledge.
Goal 3: Implement a robust, optimized, enterprise information technology infrastructure and common administrative systems that will foster innovation and collaboration.
Objective 3.1: Establish a basis to achieve further interoperability and communication among operating divisions through an enterprise approach.
Objective 3.2: Establish a capital asset replacement program.
Objective 3.3: Ensure an IT infrastructure foundation adequate to support new mandates and major initiatives.
Objective 3.4: Improve fee-for-service (FFS) models to ensure full cost recovery (annual, capital and refresh).
Objective 3.5: Evolve/mature contingency planning for IT infrastructure.
Objective 3.6: Maximize the value of technical investments.
Goal 4: Enable and improve the integration and quality of health and human services information.
Objective 4.1: Improve health outcomes by developing and using standard data, processes, and vocabularies.
Objective 4.2: Integrate critical cross-segment health and human services information across HHS, private industry, first responders, other health care providers and the public through implementation of the following steps: ⇨ Data Harmonization – Semantic Web Structure ⇨ Ontology Development and Adoption – Knowledge, Framework ⇨ Business/Administrative Data Sharing ⇨ Segment Data Integration ⇨ Public Health Data Governance ⇨ Data Quality
Objective 4.3: Develop and/or adopt public health ontologies.
Objective 4.4: Improve data quality through an effective governance architecture and data management/stewardship procedures.
Goal 5: Achieve Excellence in IRM/IT Governance and Management Practices Identified
Objective 5.1: Strengthen HHS enterprise-wide processes for collaborative IT strategic planning, capital planning, and investment control.

Objective 5.2: Apply sound standards-based lifecycle, project management and performance measurement processes to IT projects.
Objective 5.3: Develop and implement an IT human capital plan to guide the recruitment, retention, and skill development of staff.
Objective 5.4: Ensure dedicated funding steams for IS/IT management improvement and innovation.
Objective 5.5: Adopt comprehensive best practices-based IT management and governance.
Objective 5.6: Enhance the efficiency and effectiveness of competitive sourcing for IT services.
Goal 6: Implement SOA at HHS to promote interoperability
Objective 6.1: Develop HHS Enterprise SOA guidance outlining strategy, standards, and best practices.

2.2 HHS Strategic Planning Initiatives

Both the HHS Strategic Plan and HHS IRM Strategic Plan identify key information technology-related initiatives recommended for particular emphasis in helping the Department make progress towards realizing its strategic vision.

Information Technology Initiatives in the HHS Strategic Plan

1. Secure One HHS
2. Infrastructure Management
3. Health Information Technology
4. HHS Data Council
5. Confidentiality and Data Access Committee
6. Web Services
7. E-Government
8. Integrated Planning
9. Knowledge Management

Information Resources Management Initiatives in the HHS IRM Strategic Plan

1. E-Gov Initiatives
2. Federal Transition Framework Initiatives
3. Enterprise Architecture
4. Information Security
5. Optimization of IRM shared infrastructure
6. ITIM and Performance Management
7. Federated SOA infrastructure
8. Health Information Technology
9. Communications and Collaboration

The set of initiatives emphasized in the strategic plans is an input to transition planning in several contexts, including capital planning and investment control, budget preparation and investment prioritization, and the identification and prioritization of HHS enterprise segments to be documented and analyzed through segment architecture development. Three segment architecture development efforts initiated during the past year correspond to initiatives that appear in both the HHS Strategic Plan and the HHS IRM Strategic Plan: Information Security (reflected as Secure One HHS in the Strategic Plan and Information Security in the IRM Strategic Plan); IT Infrastructure Management (reflected as Infrastructure Management in the Strategic Plan and ITIM and Performance Management in the IRM Strategic Plan); and Enterprise Information Sharing Services (EISS) (related to Health IT in both plans). E-Gov initiatives remain a significant area of emphasis for HHS transition planning activities, as reflected in overall E-Gov initiative milestones summarized later in this document, and as also addressed by the IT Infrastructure Management segment (corresponding to the Infrastructure Optimization Initiative) and EISS (corresponding to the Information Sharing Environment initiative).

2.3 Major External Drivers

A summary of types of external drivers and specific instances is provided in Table 4.

Table 4: External Transition Planning Drivers

Type	Driver
Legislation	E-Government Act of 2002
	Federal Information Security Management Act of 2002 (FISMA)
	Information Technology Management Reform Act of 1996 (Clinger-Cohen)
	Paperwork Reduction Act of 1995 (PRA)
	Government Performance and Results Act of 1993 (GPRA)
	Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Executive Branch	President's Management Agenda (PMA)
	Homeland Security Presidential Directive 7 (HSPD-7)
	Homeland Security Presidential Directive 12 (HSPD-12)
	Homeland Security Presidential Directive 20 (HSPD-20)
Office of Management and Budget	Circular A-11
	Circular A-16
	Circular A-76
	Circular A-127
	Circular A-130
	Federal Transition Framework (FTF)

2.4 HHS Enterprise Architecture Principles

The HHS EA Program established a set of nine overarching principles that help provide a concise encapsulation of target-state outcomes consistent with the vision described in the HHS IRM Strategic Plan, "Comprehensive information management solutions are provided to match the critical needs of HHS and its stakeholders."

1. HHS is citizen-centered and business-driven, with services defined and delivered based on the needs of their consumers. (Customer Focused)

2. HHS is performance-driven, measuring success in terms of mission execution and continuous improvement towards meeting HHS Strategic Goals and Objectives. (Performance)

3. The HHS EA reflects a standards-based approach that promotes and facilitates technology standardization and reuse, interoperability, data sharing, and overall Departmental efficiency and effectiveness. (Standards)

4. HHS is citizen-centered and business-driven, with services defined and delivered based on the needs of their consumers. (Customer Focused)

5. HHS manages information and data as enterprise assets, ensuring integrity, confidentiality, and availability, at all levels of the department. (Information Assets)

6. HHS requires security and privacy practices to protect information assets from unauthorized use, disclosure, disruption, modification, or destruction. (Security/Privacy)

7. HHS integrates the planning, management, and governance of all HHS OPDIV enterprise architectures into a unified EA that is aligned with the Federal Enterprise Architecture (FEA). (Federated Architecture)

8. HHS streamlines business processes in alignment with Departmental and government-wide initiatives. (Efficiency)

9. HHS evaluates investments against business requirements and service needs, with a philosophy of first Reuse, then Buy, then Build. (Reuse)

3 Major HHS Initiatives

3.1 Transition Priorities

This section describes current and planned activities corresponding to several ongoing initiatives at HHS. The table below summarizes the current status of each initiative and highlights major progress milestones for 2009.

Table 5: Transition Planning for HHS Initiatives

Initiative	Current Status	Milestones		
		2008	2009	2010
Telemedicine	Initiation delayed by full-year CR in 2007	Re-propose investment	Initiate project and pilot capability	Subject to result of pilot, expand project to HHS-owned health care facilities
Performance Measurement Tool	Defined performance management framework by HHS Business Area	Evaluate alternatives including existing tools and develop plan to implement solution	Revise performance measurement commitment requirements for programs and projects	Standardize performance measurement and monitoring
Business Intelligence Solution	Platform has been installed with new capabilities implemented.	Implement solution and develop reports for OCIO program perspectives	Expand data sources, scope, and use of reporting and analytics capabilities	Implement service offering for stakeholder-requested report creation and development
HHSIdentity	Contract awarded for solution implementation after successful pilot	Develop and implement solution	Complete phased roll-out of federated identity management, enrolling OPDIVs	Leverage HHSIdentity to support other security and system initiatives
HSPD-12	Currently issuing cards for physical access	Issue FIPS 201 compliant ID cards to employees and contractors	Maintain operational capability; extend use to logical access	Maintain operational capability
Data Architecture Work Group (DAWG) (part of HHS EA scope)	Data artifact standards developed; initiated enterprise data management plan	Implement data governance and stewardship; harmonize segment data models	Implement enterprise data models; develop health-related information sharing requirements	Facilitate implementation of HHS information sharing requirements and standards

Initiative	Current Status	Milestones		
		2008	2009	2010
Enterprise SOA	No centralized initiative; SOA analysis proposed, but not funded due to full-year CR in 2007	Initiate and develop SOA segment architecture with recommendations	Execute SOA transition priorities based on segment recommendations	Re-factor HHS business and IT capabilities as services

3.1.1 Telemedicine

From a Departmental perspective, the transition priorities for the OPDIV and HHS programs responsible for mission execution are reflected in the individual Segment Transition Plans for and in the HHS IT investment portfolio. One new initiative raised in the context of the HHS IRM strategic planning workshops is a distributed infrastructure and service model for the remote provision of medical advice and care. This concept is known as "telehealth" or "telemedicine."

In recent years, health care has migrated to a more proactive, preventative care delivery model compared with the reactive, episodic care delivery model utilized before. At the same time, the number of older people in the U.S. population has grown at a very rapid pace. Older age is accompanied by increased risk of certain diseases and disorders. Chronic diseases (e.g., arthritis, hypertension, heart disease, cancer, diabetes, stroke, etc.), memory impairment, and depressive symptoms affect a significant number of older people. Additionally, people with chronic medical conditions, medically underserved locations (i.e., rural and remote areas, including American Indian tribal areas), and disabled populations in urban areas have also increased. All these trends will continue generating a sustained demand for health care services.

Recent advances in technologies (e.g., broadband, wireless, physiological sensors, and electronic health records) offer an unprecedented opportunity to increase access to health care services and improve health care delivery using telemedicine. HHS has been a strong supporter of telemedicine in the past decade. Through its OPDIVs including HRSA, CMS, AHRQ, and IHS, HHS has provided substantial grants and funding to develop and establish telemedicine services to improve access to health care services and health care delivery in rural, remote, isolated, and urban communities across the nation. In a current report, "Evaluation Design of the Business Case of Health Technology in Long-Term Care (July 13, 2006)", HHS identified telemedicine as one of the eight health IT applications, tools, and functionalities that are relevant in nursing home and home health care environments.

Participants in previous strategic planning workshops recommended that telemedicine should be considered as a major HHS IRM initiative with a focus for the next several years on developing the infrastructure to support telemedicine. Current telemedicine efforts are primarily focused on delivering health care services and each individual service provider usually has its own IT environment. Sharing telemedicine IT resources and infrastructure among these providers is very limited. One proposal is that HHS should collaborate with internal and external stakeholders to build a national telemedicine infrastructure with regional service centers to coordinate, manage, and maintain such an infrastructure. Such a national IT infrastructure would enable health care providers to establish and deliver telemedicine services much faster, more uniformly and cost-

effectively, and facilitate collaboration among telemedicine services providers to improve the continuum and quality of services.

3.1.2 Information Resources Management

Building on the priorities and areas of emphasis in the most IRM Strategic Plan, stakeholders representing the Department, OS, and several OPDIVs identified IRM issues and requirements considered critical to their business areas and respective missions. The common themes of these requirements are shown in Table 6.

Table 6: Common IRM Themes Across Segments

Common IRM Themes
Data/information dissemination
Data quality (i.e., accuracy, authoritativeness, completeness, integration)
Provision of impact analyses (e.g. baseline analysis, trend analysis, etc.)
Disparities in HHS security controls and standards
Non-alignment of OPDIV and Segment goals and objectives
Questionable or inconsistent Segment performance measurement indicators
Data standardization/harmonization
Data modeling and meta-data standards
Decision support capabilities
Data sharing/collaboration
Adoption and coordination of service-oriented architecture (SOA)
Web portal (for education, training, single source of information, facilitating business processes)
Telemedicine and distributed enabling infrastructure
Use of best practices (e.g., ITIL) for information management
Use of software development best practices (e.g. CMMI)
Business intelligence capabilities (e.g., data mining)

These themes can in turn be grouped into eight actionable areas of need:

1. Improved data quality, declaration of authoritative sources for data, and data standardization. The general consensus was that the EA business area structure and IT investment-to-segment mapping would be useful in establishing data management priorities.
2. Improved decision support including business intelligence, impact analysis, and segment collaborative analysis should be investigated and developed.
3. Security should be more flexible to actual needs and existing and required roles, in particular with a clarification of roles and expectations among the Department's Secure One HHS program and the security programs of the OPDIVs and STAFFDIVs.

4. Performance measures and HHS alignment to strategic goals, objectives, and outcomes need to be improved, including Departmental guidance on relevant and recommended business area-specific performance measures.
5. With multiple independent efforts at different levels of scope and maturity implementing service-based approaches to IT services and system deployment, the Department should provide strategies, guidance, and standards for implementing a SOA.
6. Information dissemination (portals especially) should be improved and coordinated across the Department.
7. A specific need for developing telemedicine was brought up by Indian Health Service (IHS), but it was agreed that for other areas with difficult access (e.g., rural area) this would be an important initiative.
8. Best practices should be identified and sponsored department-wide. Information Technology Infrastructure Library (ITIL) and Capability Maturity Model Integration (CMMI) for IRM management and software development were mentioned specifically.

Based on the IRM mission, vision, goals and objectives, and the identified common IRM themes across segments, the following IRM priority areas have been identified. It is understood that these prioritized areas could change due to changes in HHS mission and vision, priorities, or emerging situations. This list of IRM priorities will be validated and updated in the next iteration of the Transition Strategy.

- E-Gov Initiatives
- Federated SOA infrastructure
- Federal Transition Framework initiatives
- HHS Enterprise Architecture
- Health Information Technology
- IRM consolidation and shared infrastructure
- IRM infrastructure and common services to support public health emergencies (e.g., Avian Flu pandemic, natural and man-made disasters)
- IRM investment performance management – HHS Performance Architecture
- IRM security and privacy provisions
- Technology strategies, and the adoption and insertion of key technologies and standards based on HHS IRM priorities and direction

3.1.3 OCIO Business Intelligence and Reporting

Last year HHS began an initiative to specify and provide consistent enterprise data aggregation, reporting, and analytics across multiple systems supporting programs within the Office of the Chief Information Officer. This initial work resulted in the formulation of a business case and

recommended product selection and implementation for a Business Intelligence solution. This BI solution is intended to maximize the investments made in the current systems by providing an integrated view of enterprise data with the goal of providing consistent, up-to-date and reliable data to end users to enable effective business decision-making support. BI solution offerings provide a way to automate consolidation, analysis, presentation, reporting, and compliance capabilities necessary to make enterprise data available for action and insight. This will improve data and information access and delivery as well as reporting and analysis capabilities at HHS. The current reporting environment across these various systems is inefficient and does not adequately address the overall reporting needs of the organization. This limits the range of data available for strategic planning and operational decision-making.

The long range direction and strategic objective of this initiative is to facilitate access to data and information to inform decisions made within the HHS OCIO. This project aligns with many goals established in the President's Management Agenda as well as the HHS Enterprise IRM Strategic Plan. The major milestones planned for this initiative include:

- Submission and approval of the business case to support investment in the BI solution; (completed)
- Conversion of the functional and technical requirements already gathering into a form that can support a request for information or request for proposal solicitation to vendors; (completed)
- Complete analysis of alternatives and market analysis to determine the most effective solution for HHS OCIO; (completed)
- Procurement, implementation, and deployment of the BI solution and its integration with existing information systems. (completed procurement, implementation, and deployment; integration with existing information systems still in progress)
- Deployment of a web-accessing reporting and analysis capability allowing users to generate and view reports without requiring access to the underlying information systems containing the data used in the reports. (completed)
- Identification, specification, and development of stakeholder-requested reports using data available within the integrated BI solution. (in progress)

3.1.4 Performance Measurement and Management

In the past year, HHS initiated the development of an enterprise performance management approach and the tools to support consistent performance measurement and performance-based management of investments and initiatives across HHS. The HHS performance architecture is the instantiation of the performance management framework within the HHS EA Repository. Individual initiatives and projects – independently or in the context of an EA segment – will determine appropriate performance measures following the guidance provided in the performance management framework, and will select performance indicators and target metrics that, if met, will effectively demonstrate success. The performance indicators selected for each program or project will be populated in the HHS EA Repository and aligned to the HHS performance management framework, and by extension to the FEA Performance Reference Model (PRM), allowing HHS to identify and report on which activities across the department are

intended to support specific goals and objectives, such as those in the HHS Strategic Plan, cross-agency initiatives, and the President's Management Agenda.

While the HHS EA Repository is an appropriate mechanism for capturing performance measures, it is not an optimal solution for recording individual metrics or performance measurement indicator observed values over time. HHS envisions deploying a streamlined performance measurement tool for the purpose of capturing measurement values over time, and facilitating performance monitoring and reporting of progress against measurement targets. One possible solution would be to leverage the toolset for the Business Intelligence solution. Another alternative would be to evaluate the suitability for use of the program performance reporting tool to be acquired by the HHS budget office. Major milestones for performance management at HHS include specification of functional and technical requirements for a performance measurement and reporting tool and, in parallel, formalizing performance measurement indicator requirements and guidance for HHS investment and initiatives, to improve the quality and consistency of the measurement indicators chosen.

3.1.5 Security

Data security and privacy protection are high priorities for HHS and all government agencies. The Department's strategy for improving protection of data assets addresses recently issued OMB mandates for encrypting data on laptops, as well as increasing the availability of encryption technology for use in protecting appropriate types of data across HHS. The Secure One HHS program evaluated, selected, and implemented a full-disk encryption solution for laptop computers, and emphasized a commitment to future interoperability with smart cards to be implemented as part of the Department's HSPD-12 program.

Department-level initiatives under Secure One HHS will seek to leverage externally mandated government security initiatives and requirements to enable more consistent and effective security controls across HHS. For example, as part of the OMB-mandated transition to Internet Protocol version 6 (IPv6) within government IRM infrastructure, the IP Security (IPSec) capability of the IPv6 protocol will become available for use to promote data confidentiality and integrity. The detailed network infrastructure analysis required to comply with IPv6 implementation milestones has provided information to HHS that will support improvements in network security. For example, integrity and confidentiality of data will be supported by instituting node authentication – possibly using network access control (NAC) – and greater degrees of internal network segmentation to effectively restrict access except to known devices. Starting with devices handling high sensitivity data as well as all servers, node authentication will ultimately be instituted throughout the remainder of the network. In addition, many of the technical measures to be implemented to support physical security and personal identity verification in compliance with HSPD-12 and FIPS 201 offer the potential for use to support better logical access and other information security measures. Core supporting services for HSPD-12, such as a public key infrastructure (PKI) enable strong authentication, digital signatures, and standardized identity management, authentication and authorization services. Successful management of these encryption capabilities will entail the development of policies and mechanisms for cryptographic key management and key recovery.

The HHSIdentity initiative, managed under the Office of the Chief Technology Officer, will integrate and implement key identity management and E-Authentication services across the Department in compliance with HSPD-12 and FIPS 201. These common security, identification, and authentication services will be integrated across the enterprise in support of enterprise initiatives such as Enterprise e-Mail, and will be leveraged by a variety of HHS systems and applications for authentication. This initiative will include the integration and implementation of key identified services including single sign-on, enterprise directory services, public key infrastructure, and, potentially, biometrics services to meet defined operational objectives and functional requirements.

Some of the specific areas to be addressed in meeting HSPD-12 requirements include use of smartcard technology to store digital certificates and enable strong authentication consistent with security control baseline requirements for high-sensitivity systems and government-wide guidance such as OMB Memorandum 06-16. The scope of the HHSIdentity initiative includes proofing of user identity in accordance with federal guidelines, centralized user provisioning, and technical implementation of secure encryption keys and digital signatures within a public key infrastructure (PKI). Appropriate policy will be developed to govern the implementation and use of these security technologies. Other policy and possible identification of additional technologies will be required for external personnel and others who will not be issued smart cards.

The significant number of security-related activities and mandates were contributing factors in the decision to prioritize information security as a segment architecture for development. The Secure One HHS program is also evaluating the security services provided and made available by other agencies through the Information Systems Security LOB; at the current time HHS has submitted a request for waiver in order to continue using existing FISMA tracking and reporting capabilities already in place, pending a more complete evaluation of alternatives.

3.1.6 Enterprise Data Management

HHS continues to oversee a Data Architecture Work Group (DAWG) under the Enterprise Architecture Review Board. The DAWG members represent the data architecture interests of all HHS Operating Divisions and the Department. Among the tasks assigned to the DAWG are the development and implementation of plans, processes, and activities to establish an enterprise data management program at HHS.

Major accomplishments in the past year include the creating of an enterprise-wide taxonomy of data subject areas, to be used within enterprise architecture and other programs to help identify, categorize, and normalize data entities in use across the Department. The group maintains a list of activities to be undertaken, including creation and formalization of data governance strategies for HHS, including data stewardship policies, procedures, roles, and responsibilities; development of policies and capabilities for enterprise data management, including data harmonization and normalization; enhancement of data quality; and specification of data protection standards covering both data privacy and information security.

3.1.7 Enterprise Performance Life Cycle

The HHS Office of Enterprise Architecture continues to support the implementation and evolution of an investment-based life cycle (managed under the CPIC Program Office) defining 10 common phases from initiation through disposition. The Enterprise Performance Life Cycle (EPLC) integrates data collection and information reporting requirements across Capital Planning and Investment Control, Enterprise Architecture, Information Security, and Project Management functions. It defines exit criteria and a stage gate review process at the end of each phase of the life cycle to provide a framework in which individual projects supporting IT investments can be monitored and managed in a more consistent manner. Following the initial development of the EPLC, the implementation and oversight of the processes became the responsibility of the HHS CPIC Program.

During the past year, the HHS CPIC Program convened several information sessions and workshops related to the EPLC, to bring together representatives from the Department and the OPDIVs with responsibility for investment life cycle and IT portfolio management. Based on input, review, and feedback from these meetings, the EPLC has been revised and updated to reflect a true enterprise-wide perspective.

The upcoming milestones for the EPLC include the establishment of appropriate governance and policy directives addressing its intended use, the inclusion of adherence to the EPLC as a requirement in standard contract language used for acquisitions, training for project managers on the EPLC, and broader-scale implementation of the process.

3.1.8 Service-Oriented Architecture

SOA initiatives are leading a revolution in enterprise business and IRM integration. Many companies and government agencies are moving toward SOA projects, from limited scale efforts, to large strategic SOA rollouts at the enterprise level with supports from senior management in IRM and sometimes business executives. SOA as an IRM strategy has gained traction in the past year. SOA enables a business service layer on top of applications, which facilitates emphasis on business function support rather than hardware and software.

The core business value of SOA is in delivering business agility. Industry best practices have demonstrated that the business benefit of SOA is in service reconfiguration flexibility, with changes done in days by business people, not in weeks by technical specialists. This means that the business and technical architectures must be aligned, which is not the case in most organizations today. Expressing existing application architecture in SOA terms is not enough. Services must be business-oriented if they are to be orchestrated by business people. SOA helps to streamline IRM infrastructure, and helps to align IRM investments with business goals, optimizing IRM investments. The deployment of SOA in web service allows integration of business with current technologies.

SOA can be evolved based on existing systems and infrastructure rather than requiring a full-scale re-build. Organizations will achieve benefits from SOA by focusing their development effort around the creation of services with using both new and existing components and technologies, combined with the component-based approach to software engineering and the enabling SOA infrastructure. The benefits of SOA include:

- Business agility: SOA facilitates business process improvement. It provides business users with an ideal environment for monitoring business operations. Process modeling is reflected in the business services. Process manipulation and the change of process flow can be achieved by the use of BPM (Business Process Modeling) tools integrated into the SOA infrastructure.
- Reuse and leverage existing assets: A business service can be constructed as an aggregation of existing components, using a suitable SOA infrastructure and made available to the enterprise. Legacy systems can be encapsulated and accessed via web service interfaces.
- Common infrastructure as commodity: SOA infrastructure is becoming a commodity that can be implemented by the use of commercial-off-the shelf (COTS) products. By enforcing standards, its development and deployment can be consistent across an enterprise. Existing components, newly-developed components, and components purchased from vendors can be consolidated within a well-defined SOA infrastructure.
- Reduced development cost: The reuse of existing service and components will reduce software development time and cost.

HHS will conduct an analysis of SOA for HHS in the context of an architectural segment, to be developed during 2008 by the HHS EA Program. HHS will assess the extent to which it can in its target architecture leverage SOA technologies for delivery of common services across the Department to support both enterprise IRM initiatives as well as mission oriented IRM investment (systems and applications) across the Department. The Office of Enterprise Architecture intended to kick off a SOA initiative last year, but budget constraints associated with the full-year continuing resolution for fiscal 2007 deferred its initiation. Increased recent interest among ITIRB members has led to a commitment by the HHS EA Program to address SOA during the current fiscal year.

3.1.9 Internet Protocol Version 6 (IPv6) Implementation

In August of 2005, the Office of Management Budget (OMB) issued Memorandum 05-22 establishing the goal of transitioning all Federal government agency network backbones to support the next generation of the Internet Protocol Version 6 (IPv6) by June 30, 2008. Internet Protocol (IP) is the "language" and set of rules computers use to communicate over the Internet. The existing protocol supporting the Internet today – Internet Protocol Version 4 (IPv4) – provides the world with approximately 4 billion IP addresses, inherently limiting the number of devices that can be given a unique, globally routable address on the Internet. The emergence of IPv6, providing the world with a much greater number of available IP addresses and enhanced mobility features, is essential to the continued growth of the Internet and development of new applications leveraging mobile Internet connectivity. Although the IT community has come up with workarounds for this shortage in the IPv4 environment, IPv6 is the true long-term solution.

Agencies must prepare for the future of networking and Internet technology by transitioning their networks to support IPv6 addresses and data packets. The June 30, 2008 milestone, as required by OMB, applies only to making network backbones IPv6-capable. IPv6 does not actually have to be enabled (i.e., in an operational state) by June 30, 2008. However, network backbones must be capable of passing IPv6 traffic and supporting IPv6 addresses.

The IPv6 initiative at HHS follows the standard phases prescribed in the HHS Enterprise Performance Life Cycle (EPLC), including development of relevant EPLC artifacts delivered at the end of each phase. HHS maintains a distinct IPv6 Transition Plan, which lists historical progress and achievements against mandated IPv6 implementation milestones, major IPv6 initiative deliverables, and incremental performance milestones leading up to the June 30, 2008 completion deadline. The remaining IPv6 milestones are summarized below.

Table 7: IPv6 Milestones from IPv6 Transition Plan

Milestone Date	Activity	Artifacts
March 30, 2007	Demonstrate Readiness	Documented Current Network Infrastructure, Topology and impacted service providers; Identify any applications that will need to run over the Core IPv6 network; Identify IPv6 Address requirements
Apr. 30, 2007	IPv6 Address request	Submit IPv6 Address request to ARIN
May 31, 2007	Submit Design for IPv6 Core	Develop IPv6 Core architecture
June 29, 2007	Validate transition scenario	Validated core design
July 31, 2007	Develop a test plan for IPv6 compatibility / interoperability	Test plan
	Validate Service provider tansitions	Obtain validation from service providers of IPv6 compatibility
	Develop IPv6 Addressing Plan	Develop HHS wide schema for IPv6 addressing
	Procure Test equipment	Procurement equipment required to set up a test environment.
Aug. 31, 2007	Implement Test environment	Setup of Test equipment
Sept. 28, 2007	Develop Implementation, Security and Network Management Plan	Implementation Plan; Security Plan; Network Management Plan
Nov. 30, 2007	Equipment Upgrades\Replacement	Complete any upgrades\replacements required to implement IPv6 functionality
Jan 31, 2008	Complete validation of plans against Test environment	Results report of pilot testing
Feb. 29, 2008	Complete testing	Test results
June 30, 2008	Complete network backbone transition to IPv6	EPLC artifacts documenting the updated network infrastructure;Testing results submitted

3.2 Cross-agency Initiatives

All relevant government-wide and health sector initiatives are incorporated in the HHS enterprise architecture, to provide a centralized initiative alignment capability, to identify opportunities for reuse of internally and externally available services, and to help demonstrate compliance with mandatory guidance, regulations, and technical standards.

3.2.1 Federal Transition Framework

The most current version of the FTF Catalog lists 18 mandatory initiatives, each of which is applicable in some capacity to HHS. The table below summarizes the HHS transition planning perspective for each FTF initiative, characterizing the level of relevance, current status, and expected progress or milestones for 2009. As additional detail in support of FTF alignment, a listing of IT investments within the HHS IT portfolio aligned to each of the FTF initiatives appears in Appendix B.

Table 8: Transition Planning for FTF Initiatives

Initiative	HHS Relevance	Current Status	Planned Activities
Budget Formulation and Execution Line of Business	Potential Service Consumer	No enterprise initiative	Evaluate potential for reuse of FTF services as they are developed
Case Management Line of Business	Litigation and Regulatory Enforcement	No enterprise initiative	Evaluate potential use of FTF defined processes and services
Disaster Management	Mission Responsibility under Asst. Secretary for Preparedness and Response	ASPR efforts are focused on requirements of the Pandemic All-Hazards Preparedness Act	Execute plan developed under PAHPA
E-Authentication	Government-wide mandate	Evaluating within context of HHS PKI, HHSIdentity and HSPD-12 initiatives; implementing E-Authentication in grants.gov	Incorporate E-Authentication functional and technical requirements and standards in HHS solution architectures
E-Travel	Service Consumer	Completed HHS-wide deployment	No additional activities
Federal Health Architecture (FHA)	Managing Partner	Responding to Health IT system inventory and assessing the impact of compliance with recognized Heath IT standards	Apply architectural analysis to Health IT standards and interoperability requirements to plan compliance efforts
Financial Management Line of Business	Intent to be a Service Provider (SSP)	Deployed UFMS to all OPDIVs except CMS and NIH; HHS offering financial management services to external agencies	Migrate NIH NBS into UFMS; align UFMS processes and services to FMLOB
Geospatial Line of Business	Potential Service Consumer or Provider	Evaluating OPDIV-specific GIS systems and services for use within HHS	Integrate HHS GIS Public Health data to Geospatial One-Stop

Initiative	HHS Relevance	Current Status	Planned Activities
Geospatial One-Stop	Government-wide mandate	CDC and HRSA leading Health and Human Disease geodata.gov community	Integrate HHS GIS Public Health data to Geospatial One-Stop
Grants Management Line of Business	Co-Managing Partner; Intent to be a Service Provider (SSP)	ACF and NIH provide grants systems and services to external agencies; ACF's is part of the FTF	Increase internal and external use of HHS target grants management services
Grants.gov	Managing Partner	HHS grant opportunities are currently published on grants.gov; HHS developed guidance and interface specifications	Maintain 100% posting of HHS discretionary grants on grants.gov
HSPD-12	Government-wide mandate	Currently issuing cards to employees and contractors as ID expirations occur	Evaluate service and technology reuse potential for logical access and information security requirements
Human Resources Line of Business	Intent to be a Service Provider (SSP)	HHS offering human resources services to external agencies	Increase internal and external use of HHS target human resources management services
Information Sharing Environment (ISE)	Member of Information Sharing Council	Developing EISS segment architecture	Contribute to the development of a health information profile for ISE
Information Systems Security (ISS) Line of Business	Potential Service Consumer	HHS requested a waiver of requirement to use an external provider for FISMA reporting	Evaluate alternatives for ISS common processes and services
Integrated Acquisition Environment (IAE)	Government-wide mandate	Planned further system rationalization under HHS Consolidated Acquisition System (HCAS), with a target of one enterprise instance	Complete deployment and consolidation of HCAS; increase internal and external use of Strategic Acquisition Services
Internet Protocol Version 6 (IPv6)	Government-wide mandate	Meeting OMB milestones	Follow IPv6 transition plan (see section 3.1.9)

Initiative	HHS Relevance	Current Status	Planned Activities
IT Infrastructure Optimization Line of Business	Government-wide mandate	Initiated ITI segment architecture development to reflect activity in IPv6, Trusted Internet Connection, and ITI LOB HHS initiatives underway contract vehicles.	Align HHS to IOI specified business processes; Evaluate IOI services as they are developed

3.2.2 Health Information Technology

HHS has incorporated all technical standards adopted within the Health IT sector, including those approved through the Health Information Technology Standards Panel (HITSP) and recently formally recognized by the HHS Secretary. All of the individual technical standards specified by these initiatives are reflected in the HHS enterprise architecture and reported in consolidated form in the current version of the HHS Technical Standards Profile.

For Health IT standards, the major transitional activity focuses on implementing the standards that have been approved to date. HHS has designed and implemented the technical capability to associate Health IT standards with relevant data, systems, and processes across HHS. The next major milestone for these activities is to more fully capture the applicability of Health IT standards for HHS data, systems, and processes, and to provide reporting mechanisms that demonstrate accurate alignment to Health IT standards and, therefore, compliance with policies and mandates regarding the adoption of these standards. The quarterly HIT system inventory administered by FHA on behalf of ONC will help determine the impact associated with complying with the health IT standards formally recognized by the HHS Secretary in December 2007.

3.3 Segments

As noted above in section 2.2, as part of the HHS Enterprise Architecture Program's efforts to support and further progress on high-priority strategic initiatives, over the past year the OEA began and completed initial architecture development efforts for three segments. This section provides a summary of relevant information produced in each segment architecture development effort, with information drawn from the respective Segment Transition Plans.

3.3.1 Enterprise Information Sharing Services (EISS)

a) Overview

The Department's ability to deliver the best possible service relies not only on HHS' expertise but also on the expertise of other organizations, including Federal agencies, State, Local, and Tribal agencies, non-government organizations, commercial enterprises, etc. Achieving HHS' mission requires unprecedented cooperation; which also requires an unprecedented level of information sharing. Over the years, information sharing environments have grown organically, both within HHS as well as with its partners (e.g. Federal Agencies, State Agencies, non-

government entities, etc.). Indeed HHS currently supports information sharing through a variety of services provided by things like the cancer biomedical informatics grid (caBIG™), the Public Health Information Network (PHIN), and others. But HHS is responsible for more than Healthcare, there are after all Human Services as well; they too have information sharing needs and capabilities.

With the introduction of the Information Sharing sub-function within the Information and Technology Management LOB HHS realized the opportunity to achieve line-of-sight into this critical set area. HHS understands that over the years the organic growth created the potential, if not the reality, of overlapping and disjoint services.

HHS therefore created the Enterprise Information Sharing Services (EISS) segment to provide a strong architecture that ensures comprehensive and secure information exchange between HHS and its partners. The purpose of the segment is to provide the architectural foundation for information sharing as a cohesive set of services across HHS; to rationalize and harmonize the many current services. EISS is an enterprise services segment focusing on technical infrastructure and services. It provides the architectural foundation for the systems and services necessary to support information sharing for HHS OPDIVs, STAFFDIVs, and partners.

b) Findings and Recommendations

Like many organizations, information sharing has grown organically at HHS. As the need presented itself, capabilities were added to the by the Business Area that required tem. In some cases (e.g. caBIG™, PHIN, etc.) information services took on a life of their own; nevertheless they remained closely aligned with the creating/sponsoring area. HHS now owns and operates a "network of networks"; however they are not interoperable. Even where common services exist; they have been implemented using different standards and technologies. Many of the findings are a direct result of the structural issues created by the unconstrained organic growth.

Table 9: HHS EISS Segment Findings Summary

No.	Finding	Description
F-1	No Comprehensive Information Sharing Mission	Responsibility for Information sharing environments (ISE's) at HHS is distributed among the Op Div's and Staff Div's within HHS. There is little coordination or sharing among the many initiatives. The ONC and FEA are focused on Health Information; ignoring the needs of the Human Services side of HHS mission
F-2	Information Sharing Inventory not completed	An inventory of HHS ISE's is not available. HHS cannot categorically state how many ISE's exist, nor how much is being spent on information exchange
F-3	Diffuse ISE Goals and Objectives	Responsibility for information sharing is delegated to the Op Div's and Staff Div's. The ISE goals and objectives, while similar, do no drive commonality or support re-use. ISE is not a primary objective in the HHS Strategic Plan 2007-2012
F-4	No Non-health Information Sharing Goal	Health information sharing remains, rightly so, a primary focus area for HHS. Non-health related information sharing has the same issues and problems.

F-5	**Too Many Stakeholders**	**The current ISE's stakeholder list is not manageable. It includes <all> Federal Agencies, State Agencies, Local Agencies, Tribal Agencies, Healthcare providers and organizations, etc. It is like this because ISE is mapped to the Core Mission and/or Business Service level in the BRM**
F-6	**No Common Architectural or Design Deliverables**	**Each ISE documents their segment at different levels of granularity and use different architectural deliverables. This make comparing them extremely tedious**
F-7	**Overlapping and Inconsistent Information Sharing Services**	**There are well over 100 use cases describing information sharing services in just three (3) documented ISE's. While there are similarities in services; it is difficult to ferret this out. There are no common service definitions among the many ISE's**
F-8	**ISE Systems Intermingled with other Sub-Functions**	**The current ISE's are heavily driven by business use cases. As a result, ISE's tend to be either tightly coupled with business services, or the support/development structures are intermingled.**
F-9	**Divergent Technologies**	**Though the TRM was out of scope during this iteration of the Segment Architecture, it was noted that the various organizations used significantly different technologies to provide the same services. It also appears that all of the technologies adhered to existing Health IT Standards.**
F-10	**Investment Information Not Readily Available**	**Within the HHS OCIO Exhibit 53 submission there were seven (7) obvious ISE investments. They were mapped to LOB 110 and Sub-Functions 248 and 249**
F-11	**Standards, Lots of Standards**	**There are numerous standards describing health information. It is not at all clear that the canonical forms exist outside the context of existing ISE's (i.e. what form will be exchanged between networks is not known)**
F-12	**Multiple Support Organizations**	**For each ISE there is a support organization complete with architects, engineers, project managers, testers, trainers, etc. From the FEA CRM, there are seven (7) Business Areas, 20 LOB'a and 60 Sub-Functions represented. That is a lot of duplication for a common set of services**

As many of the findings were structural in nature; it should come as no surprise that many of the recommendations are designed to solve the structural problems. Of primary concern is understanding the real scope of information sharing at HHS. Next is to rationalize/harmonize the various service definitions. Only then can HHS begin to address comprehensive implementation planning.

Table 10: HHS EISS Segment Recommendations Summary

No.	Recommendation	Finding(s) Addressed	Description

No.	Recommendation	Finding(s) Addressed	Description
SR-1	Establish Information Sharing Sub-Function 262 under the Information and Technology Management LOB	F-1 F-3 F-4 F-5 F-8 F10	Sub-Function 262, Information Sharing was recently created in the FEA CRM. All information sharing activities should be consolidated under this Sub-Function to provide the necessary investment visibility and governance foundation. The Stakeholders for Sub-Function 262 will be the CIO's of the participating Op Div's and Staff Div's. This will also allow ISE investments to be tracked.
SR-2	Complete a comprehensive HHS Information Sharing Survey	F-2	HHS organizations need to complete the Health Information Survey and create a separate instrument to assess the Non-Health Information Sharing inventory.
SR-3	Create and Fund an EISS Organization. Establish an ISE Council to provide oversight and governance	F-1 F-3 F-4 F-5 F-12	The EISS must be separated (logically, if not physically) from any specific Op Div or Staff Div if it is to provide Enterprise Services. All new services should be created by this organization. An ISE Council consisting of the HHS CIO's and a representative of the ONC should be created to provide governance.
SR-4	Architect a comprehensive ISE. Reconcile/harmonize the services and supporting technologies to be offered	F-6 F-7 F-9	Each instance of an information sharing environment should complete a high level Segment Architecture. At the direction of the ISE Council; designated architects/engineers should update this EISS Segment Architecture to reflect the mandatory common service definitions and supporting technologies.
SR-5	Decouple Data Interchange Standards from EISS	F-12	While EISS must be able to effectively transform information as it moves through it's infrastructure; EISS is not responsible for establishing the canonical form of the information exchange package. EISS only requires that the canonical form exist with a set of rules for performing the transformation. EISS can specify the technology base to provide the transformation.

3.3.2 Information Technology Infrastructure (ITI)

a) Overview

Twenty-three (23) U.S. Federal civilian and military Departments/Agencies are participating in the IT Infrastructure Initiative (ITI) Line of Business (LoB) which aims to realize four long-term outcome goals:

1. Interoperability of functions across agencies and programs
2. Collaboration within and across agencies, sectors, and government levels
3. Reductions in total cost of commodity IT infrastructure and return of savings to agency missions

4. Improved governance of IT infrastructure investment in support of agency mission and government-wide goals

The government's business case seeks to save between 16% and 27% annually on its aggregate $21 B+ IT infrastructure budget, or between $18B-$29B over ten years, based on a five-year technology refresh cycle.

Key to delivering such results is the development of an analytical foundation to establish the means to assess performance in three IT infrastructure areas, as defined by the ITILoB:

- End User Systems and Support
- Mainframe and Server Services and Support
- Telecommunications Systems and Support

The ITI segment will optimize IT infrastructure and services, IT administration, management and oversight functions common to all Operating Division (OPDIVs). This segment facilitates a HHS optimized and cost-effective IT infrastructure enabling core agency missions and OPDIVs customer-centric services. This includes all categories of IT investment that are employed in the process of IT management and oversight. It also includes the traditional view of infrastructure such as networks and shared services. This segment shared infrastructure includes such things as help desks and support processes, common services and the infrastructure needed to deliver shared and federated services. The ITI segment also incorporates planning for Departmental enterprise initiatives that are intended to provide core or essential IT services in support of all HHS Staff Divisions (STAFFDIVs) and OPDIVs. These are fundamental elements in supporting the Secretary's goal of managing HHS on an enterprise basis. This consolidated and shared approach requires a highly organized, coordinated, and disciplined effort. Thus, the scope of the ITI segment is focused on the following initiatives:

1. Information Technology Infrastructure Line of Business (ITILoB) – an analysis of this initiative established to achieve an optimized, cost-effective, government-wide information technology infrastructure, while providing reliability and security in service, will determine what the HHS target environment should look like upon completion of this initiative in three phases:
    - Phase 1 - End User Systems and Support (EUSS)
    - Phase 2 - Telecommunications Systems and Support (TSS)
    - Phase 3 - Mainframes and Servers Services and Support (MSSS)
2. Trusted Internet Connection (TIC) – an analysis of IT assets that currently align to this initiative; and determination what the HHS target environment should look like upon completion of this initiative.
3. Internet Protocol Version 6 (IPv6) – an analysis of the current IPv6 transition plan to determine the current environment within HHS for supporting IPv6; and what specific changes will be needed within HHS to support the transition. This analysis will focus on:

- An assessment and update of communications components
- Upgrade of appropriate operating systems and TCP/IP software products providing network services to support the migration from IPv4 to IPv6
- Transition of WAN/Internet service providers/connections to IPv6 enabled and addressed WAN connections
- Re-IP addressing appropriate servers, clients, and telecommunications components to employ IPv6 addresses

4. Desktop Standardization – an analysis of the HHS Federal Desktop Core Configuration (FDCC) Standard for Windows. In collaboration with its OPDIVs, HHS adapted the standard provided by the National Institute of Standards and Technology (NIST) and made appropriate adjustments to best suit the HHS Environment.
5. Security Alignment – while this Segment Summary is not specifically focused on security, it will show how the current environment of IT improvement initiatives aligns to the current security approach of HHS; and will make recommendations on changes to the target HHS security approach, if needed, once the initiatives are completed.

b) Findings and Recommendations

HHS Office of the Chief Information Officer (OCIO) will be following the ITILoB recommended ITI Optimization implementation approach; however, the HHS OCIO has encouraged OPDIV CIOs (or their designated representatives) to adapt a transformation strategy that satisfies their individual needs while meeting HHS OCIO's expectations:

- Collect data or representative data samples from distinct and logical organizational groupings by participating agencies using the Gartner workbook and data collection tool. Where organizational sub-groupings are identified, these units will be rolled up into an OPDIV representation.
- Use the data or data samples plotted against the industry average.
- Set annual improvement targets in both cost efficiency and service levels to address the established metrics.
- Set quarterly targets for refining the OPDIV data as necessary to reflect implementation of optimization decisions, and plan to report to OMB on progress.
- Measure performance against the metric for each IT infrastructure area, by assessing improvements in the cost efficiency and service level components to show progress toward the target.
- Include all critical partners (*e.g.*, Enterprise Architecture (EA), Capital Planning and Investment Control (CPIC), Security, Human Resources, Budget/Finance, and Acquisition) as part of the ITILoB optimization planning process to ensure that implementation strategies are coordinated with on-going EA Infrastructure and Security Segment development activities, security initiatives (*e.g.*, Trusted Internet Connections),

and to ensure that future acquisition strategies and terms facilitate optimization and ITILoB reporting.

- Based on the previously delivered HHSNet Architecture, deploy and implement the network backbone for the IPv6 upgrades. There are three facilities that will need to be transitioned, Humphrey, Parklawn and Atlanta. The intended architecture deployment will be dual-stack. The specific architecture design for each segment will be based on requirements and cost-benefit analysis. The connection between HHSNet and individual OPDIV backbones may apply a gateway approach.

- Determine risk factors in providing high availability internet connectivity by identifying internal and external threats in support of TIC. Also, when reducing the number of internet connections, the physical link connecting HHS to the Internet Service Provider (ISP) can be a single point of failure.

- NIST recommended the setting of 'Enabled:Disable' is understood to be potentially problematic for some OPDIVs and was modified within the HHS FDCC Standard to provide additional flexibly. Also, many CMS business applications use ActiveX controls and FDA does not use Windows Firewall.

- NIST recommended HHS to enforce an universal enforcement of maintaining password history and the length and age of passwords.

The following is a summarized overview report of benchmarking and performance measurement findings, results and analysis related to the first of three IT infrastructure areas: End User Systems and Support (EUSS) within the IT Segment. Once the data collection for each participating OPDIV was completed and reported, an evaluation of the macro-level was conducted. The high-level results are as follows:

- Six major Infrastructure Investments across HHS
    - OS ASAM IT Service Center – Unique Project Identifier (UPI)
    - CDC Information Technology Infrastructure – UPI
    - CMS IT Infrastructure – UPI
    - FDA Consolidated Infrastructure – UPI
    - IHS Infrastructure, Office Automation, & Telecommunications (I/OA/T) – UPI
    - NIH IT Infrastructure – UPI
- Total EUSS spending in excess of $200 million
- Total Cost per User is within but near the top of the industry range
    - The Client and Peripherals Support component of this total cost is 7% below the top of the industry range
    - The IT Help Desk component is 10% below the bottom of the industry range
- The Total Cost per Device is close to the mid-point of the industry range
- Client & Peripherals service levels for four (4) of six (6) OPDIVs exceeded the Client & Peripherals service levels

  - FDA and NIH reported service restoration percentages below target
- While HHS's 1.24 devices per user is close to the industry average of 1.1, the OPDIVs vary in this regard from 0.81 devices per user at HIS, to 1.78 at FDA

After the data collection for each participating OPDIV was analyzed, its results were benchmarked, performance measurements were identified and the following are the recommendations from this analysis related to the first of three IT infrastructure areas: End User Systems and Support (EUSS) within the ITI Segment. The following are recommendations based on the data collected:

- Critical Areas for Improvement
  - Leverage economies of scale
  - Invest in IT asset management and reporting tools
  - Beware feast or famine environments
- Resulting Recommendations
  - Standardize tools at help desks
  - Enable cross-agency sourcing
  - Centralize small environment support
  - Centralize help desks at large agencies
  - Monitor outsourcing
  - Improve service level and metric reporting
- Successful Approaches
  - Optimization requires investment
  - Outsourcing governance requires sustainment
  - Centralization of support services is best (where sensible)
  - Continuous improvement program dedication pays off
- Practices to Avoid
  - Lowest cost provider
  - Static, long-term outsourcing contracts
  - Independent, autonomous IT organizations

3.3.3 IT Security

a) Overview

The Department of Health and Human Services (HHS) is a high profile target for hackers and others with malicious intent seeking sensitive medical information, homeland security first responder information, intellectual property, and financial and budgetary data. Like many other organizations, HHS is also challenged with the drop in productivity and loss of intellectual capital that occurs when viruses, worms, and other information technology (IT) security threats enter HHS' mission-critical systems.

Secure One HHS was established to strengthen the IT security posture across all HHS Operating Divisions (OPDIVs) while reducing reporting burdens for compliance with federal mandates. The creation of this security program, which spans the HHS IT community,

Headquarters (HQ), and the OPDIVs, is an important step in protecting HHS' ability to provide mission-critical services and maintain the public's trust and confidence in the quality of HHS services and business operations.

In response to an evolving IT environment where HHS is increasingly dependent on information systems to accomplish mission critical services, HHS established an enterprise-wide IT security program, Secure One HHS, to meet legislative requirements and mitigate risk. Secure One HHS consists of the following four functions: Enterprise Security, Outreach, Governance, and Finance and Budget.

The IT Security Segment builds upon the foundation laid by Secure One HHS in order to develop stronger governance processes that provide the necessary security services and oversight to the OPDIVs.

b) Findings and Recommendations

The IT Security Segment Transition Plan is a critical component of an effective transformation activity. It describes the overall plan for the program to achieve its target state within a specified timeframe thus enabling HHS to achieve its target. It clearly links proposed HHS investments to that target state. Also, the Secure One HHS Segment Transition Plan helps to define logical dependencies between transition activities (programs and projects) and helps to define the relative priority of those activities for investment purposes.

In brief, the findings cans be classified into a few main categories:

1. Communication issues – where the communication mechanisms between HHS and OPDIVs require improvements
2. Delegation of authority issues – where the decision-tree for certain types of security-related decisions require clarification and/or formalization
3. Process automation issues – where processes (e.g., the compliance measurement audits) are carried out manually rather than in an automated fashion
4. Process variance issues – where security controls are implemented with slight differences among the various OPDIVs

The recommendations developed in response to the findings focus on increasing the automation and integration of existing processes among the IT Security Segment itself and between the OPDIVs. These recommendations call for leveraging the existing data requests and aggregation tools and techniques in order to develop strong governance processes that provide the necessary security services to the OPDIVs, and place emphasis on good governance procedures to guide the IT Security Segment development.

Table 11: IT Security Segment Findings Summary

No.	Finding	Description

No.	Finding	Description
F-1	Incident Management Gaps	Current incident management process communications flow mostly from the OPDIVs to the Department. Incidents are reported by the various OPDIV Incident Response Teams (IRTs) to the Secure One Team. These reports are utilized for increased situational awareness at the HHS level. Secure One HHS does not provide similar, albeit filtered, reports to the OPDIVs.
F-2	Vulnerability Management Communication Flow	Current vulnerability management process communications flow mostly from the Department to the OPDIVs. Vulnerabilities of supported OPDIVs are reported by the Department to the OPDIV. Little insight into remediation and existing vulnerabilities within larger OPDIVs.
F-3	Vulnerability Management Authority	The Vulnerability Management team does not currently have the authority to require the OPDIVs to fix discovered vulnerabilities.
F-4	Limited Automated Compliance Ability	The Secure One HHS Governance team has limited ability to measure compliance with technical security policies and controls. While some OPDIV capabilities exist for automated measuring of policies and controls, the majority of measures are audited manually at the Department level.
F-5	Limited Security Training Availability	The current Security Awareness Training is adequate, but not flexible enough for the changeable nature of security issues. The Secure One team does not provide standard or specialized role based training.
F-6	Narrow Customer Focus	While audit and oversight roles have broader interactions, the implementation of policies, standards, and controls have had limited interaction with Project Management and Systems Development stakeholders.
F-7	Varying Interpretation of Security Controls	Security Stakeholders within each OPDIV have differing levels of control within their respective organization, making standardized responses to security issues extremely difficult.
F-8	Varying Compliance Alignment	HHS bases its implementation of security controls on federal guidance as much as possible, however its broad mission and diverse make-up of customers and partners makes some controls difficult to implement.
F-9	Limited Security Intelligence	HHS has limited visibility into the overall security posture and limited insight into how external threats, agents, personnel view the HHS network and might try to breach the HHS network. Likewise, there still remains some unwillingness to share internal weaknesses to understand the communal risk OPDIVs share by being interconnecting.
F-10	Varying Governance of IT Security Segment	HHS level policy to date has been general and focused on establishing a minimum baseline of acceptable behavior. This has resulted in varying responses at the OPDIV level. Overall the various approaches align with OPDIV missions, however response to specific policy statements vary in coverage.
F-11	Limited interactions with Enterprise Architecture	Secure One HHS staff has limited interaction with the Enterprise Architecture team.
F-12	HHS CERT Staffing Required	In order to properly staff the HHS CERT, the proper staff requirements will need to be identified and a decision made on source and funding. Prior to fulfilling this requirement the entire makeup of the HHS CERT needs to be defined, publicized, and approved.

No.	Finding	Description
F-13	Limited Security Toolset Visibility	HHS visibility into tools and solutions utilized within the various OPDIVs differs. Generally, OPDIVs with more resources are more likely to propose Enterprise solutions to the Department. This tends to bring focus to large COTS implementations that may not fit all environments. Increasing the awareness of the security solutions in place at all OPDIVs will facilitate prioritization of solution needs.
F-14	Proposed IT Infrastructure Security still conceptual	The *HHS OCIO Security Architecture Whitepaper proposes* a number of specific industry best practices relating to • Establishing zone-based IT infrastructures; • Implementing Least Privilege\Functionality and Separation of Duties; • Securing User and Administrative accounts; and • Secure Web Browsing. Many of these recommendations are still high level and need to be refined in light of operational realities.
F-15	Proposed Secure Systems Architecture still conceptual	The *HHS OCIO Security Architecture Whitepaper* utilizes CMS's Internet Architecture as a model of providing secure access to data. The whitepaper also proposes a number of long term goals relating to endpoint assurance, identity management, cryptography, and authentication that are not possible in the current HHS environment.
F-16	Proposed Security Management Infrastructure still conceptual	The *HHS OCIO Security Architecture Whitepaper* proposes a number of best practices relating to: • Vulnerability and Configuration Management; • Active Directory Change Management; • Continuous Monitoring (Detection); • Automated Logging and Security Information and Event Management; and • Other operational security practices. Many of these recommendations are still high level and need to be refined in light of operational realities.

Based on the findings, there were 16 resulting high-level recommendations designed to address the findings and to achieve the future vision for the Secure One HHS Segment. Summary descriptions of the sixteen recommendations are provided in Table 12.

Table 12: IT Security Segment Recommendations Summary

No.	Recommendation	Finding(s) Addressed	Description
R-1	Establish a consistent reporting mechanism to provide OPDIVs awareness of the Department's view of HHS risk level. Establish an HHS CERT to focus and coordinate security efforts across the department	F-1, F-2, F-9	Secure One HHS plans to develop reports that provide high-level summaries of reported incidents in each OPDIV as a method to provide situational awareness. Reports must be sufficiently anonymous so that OPDIV-specific data is not transported between OPDIVs. HHS CERT will also assist in providing situational awareness data to OPDIVs.
R-2	Establish an HHS CERT to focus and coordinate security efforts across the department	F-1, F-2, F-9	HHS CERT will also assist in providing situational awareness data to OPDIVs. It will also coordinate IM and VM processes to more effectively leverage risk data against current system inventories.
R-3	Implement a vulnerability management policy	F-3	Policy must be established that provides the proper authority to security teams at the HHS and OPDIV level to require critical vulnerabilities be addressed in a timely manner.
R-4	Modify contract language to ensure all service contracts reference compliance with HHS Security policies.	F-3	Modify contract language to ensure all service contracts provide sufficient clarity both for contractors and for the government, and reference compliance with HHS Security policies.
R-5	Increase the use of automation to audit policy compliance	F-4	Secure One HHS will implement a number of tools that will automatically report on compliance with HHS policies, including OMB mandates such as FDCC.
R-6	Identify an appropriate training LOB provider	F-5	Enable the Program to address security training and awareness more broadly than just meeting baseline FISMA requirements. Improve security competencies of the HHS workforce and enhance agency-wide security performance.
R-7	Coordinate with existing teams within the OPDIV that focus on project management and system development	F-6	Secure One HHS Security Architecture processes need to expand its focus from the current security customers to address the needs of project managers and system developers.
R-8	Increase coordination with HHS Enterprise Architecture team	F-6	The Enterprise Architecture team is leading a number of efforts that can assist in coordinating and identifying new stakeholders.
R-9	Break out Communications processes to provide better focus	F-7, F-9	As the methods of communications increased from email to other personal and technical avenues the communications team required more resources and better align and manage the various tasks and requirements place upon it by both Departmental, internal, and OPDIV customers. The original communications role has been elevated to include all outreach activities, including focused group devoted to web-based communications, web-based portal, other communications, and training. This effort will also be instrumental in establishing better coordination of incidents and vulnerabilities via the planned HHS CERT.

No.	Recommendation	Finding(s) Addressed	Description
R-10	Develop a collaboration portal	F-7, F-9	Where the Secure One HHS intranet site is an excellent place for reference of historical and static programmatic information, a web-based portal for the sharing of documents is instrumental to facilitating communications with other HHS stakeholders and more quickly coordinating the development and implementation of policy and technology.
R-11	Long-term plan for migration to secure architectures where appropriate	F-8	HHS bases its implementation of security controls on federal guidance as much as possible, however its broad mission and diverse make-up of customers and partners makes some controls impossible to implement Current HHS approach to policy is to implement only policies that can be implemented by the OPDIVs and managed by the Department. Inconsistencies are the result of applying realistic timeframes and solutions in support of the various HHS and OPDIV missions. In the longer term, the Department is working to develop overarching standards for securing the IT infrastructure, implementing a security management infrastructure, and establishing standard for secure systems architecture.
R-12	CIO Council to establish the accountable authority	F-9	CIO Council to establish the accountable authority
R-13	Develop more targeted policies and standards	F-10	Look to develop more specific policy targeted to at specific technical weaknesses in OPDIV implementations and/or to clarify required elements in HHS Policy.
R-14	Increase coordination between Enterprise Security and Governance processes	F-10,F-11	This is in place as of the end of 2007, but is still maturing. The differing skill sets of the technical security experts and policy experts coordinate well. Technical experts are able to identify weaknesses in current policy implementations through the review of historical incidents and vulnerabilities and identify tools and capabilities that for automating compliance. The governance team is able to respond quickly with directed policies or standards and prioritize compliance solutions against GAO, PMA, and FISMA requirements.
R-15	Establish Working Groups to refine *HHS OCIO Security Architecture Whitepaper* recommendations	F-14, F-15, F-16, F-13	Working groups will provide the best use of resources for developing secure solutions that best fit the current operating environment and have immediate buy-in from the implementing stakeholders.

No.	Recommendation	Finding(s) Addressed	Description
R-16	Develop staffing plan for HHS CERT	F-12	HHS should leverage resources at NIST and Carnegie Mellon for establishing a CERT. Part of this process is define personnel roles and skill sets required to fulfill the situational awareness and technical communications coordination roles.

3.3.4 Public Health Informatics

a) Overview

The Centers for Disease Control and Prevention's (CDC) National Center for Public Health Informatics (NCPHI) is charged with the unique responsibility of providing critical, complex and dynamic informatics and IT systems and services to public health. In seeking to accomplish these challenging yet critical efforts, NCPHI leadership must address resource limitations, shifting demands and priorities, heightened oversight and the unpredictable needs of emergency response, all of which increasingly challenge the Center's success. To support and enhance the Center's ability to deliver programmatic results within this context, the Director of NCPHI requested and approved the NCPHI Architecture Project on September 21, 2007.

In order to achieve the objectives of NCPHI leadership, the NCPHI Architecture Project will require multiple phases with distinct scope and activities. Phase 1 of the NCPHI Architecture Project was conducted from September 2007 to January 2008. Phase 1 includes documentation of the current NCPHI Architecture, a proposal for the foundation of the future (or target) NCPHI Architecture, and a strategy for the development of a transition plan (or roadmap) that will guide the movement of the NCPHI Architecture from its current state to the target state. Phase 2 of the NCPHI Architecture Project which would begin in March 2008 will complete the documentation of the target NCPHI Architecture and complete the documentation of the transition plan. The transition plan will provide the roadmap, at the system level, for the evolution of the NCPHI Architecture into its future state or target architecture. Phase 3 of the NCPHI Architecture Project will consist of a series of projects that will implement the transition plan.

The architecture has been structured into segments which align with CDC's business functions as determined by CDC's Office of Strategy and Innovation (OSI) and documented in CDC's HealthImpact.Net system (HI.Net). These high-level business functions also align with the high-level activities of public health which are, in turn, supported by the informatics and infrastructure of the Public Health Information Network (PHIN). The division of the architecture into segments allows the same team to architect and analyze systems which support closely related business functions

As part of Phase 1, the NCPHI Architecture project team worked with various system owners, stewards and related resources to document the current architecture of NCPHI's systems. Information was collected utilizing surveys and interviews. Once collected, the project team analyzed the systems information to observe the strengths and weakness of the current architecture. This document is the interim report presenting the current state architecture review and its related activities.

Based upon work completed in Phase 1, the project team made a number of findings and observations about each architectural segment

b) Findings and Recommendations

- NCPHI systems typically have been developed and managed independently and without coordination at the Center level, making it difficult to support a consistent vision and architecture.
- CDC has a culture built upon separate and independent approaches that does not encourage teamwork and collaboration among programs.
- NCPHI to date has been functioning as a software development organization for its partners without taking on the best practices of a good software development organization.
- NCPHI is responsible for systems in almost every segment of the CDC and Public Health Core Mission Areas. The potential interoperation of systems across these mission areas must be addressed to provide complete and seamless support of critical public health activities. For example, STARRS is a laboratory system that collects patient IDs but not other patient information, while BioSense could collect Patient ID in addition to other case information. In this way The information from STARRS and BioSense can be easily merged to meet public health requirements (e.g., epidemiological analysis).
- Some of NCPHI's information systems lack broad stakeholder and user involvement**.** Accordingly, the scope, requirements and solutions are defined almost entirely by the individual business and technical stewards, and CDC program staff.
- State, local, and territorial public health partners are compelled to use multiple NCPHI systems and have multiple relationships with different groups within NCPHI for each system (e.g., PHINMS and VADS have separate User Groups/ Communities of Practice).
- Many NCPHI systems are not using shared services appropriate to their requirements.
- Enterprise Architecture analysis and comprehensive business process analysis are typically not conducted prior to system development; nor is there currently a central governance, review, and portfolio management process within NCPHI.
- Some of NCPHI's systems share infrastructure level services such as messaging, transport and security, but do not share application level functions such as visualization and analysis algorithms.
- The CDC Unified Process was strongly encouraged for use in all NCPHI systems in July, 2006. However, projects initiated earlier than July, 2006 have not consistently utilized the CDC Unified Process as the project management standard, resulting in inconsistent system documentation and system review.
- NCPHI does not have an established set of best practices for software development life cycle methodologies; a common code repository; or other mechanisms for code reuse

between its systems and programs. This results in duplicated efforts where commonly required services, practices and utility functions are created for each system implementation at NCPHI.

- The reported number of servers in the disaster recovery site appears to be very low for the number of production and development servers in CDC sites (23:418). A strategy should be explored to address the funding and operational needs for continuity of operations.
- NCPHI has heavily utilized a number of non-open standards technology platforms including many Microsoft software products.
- Due to EA team efforts, CDC recently (Summer 2007) published a policy for the usage of open source software when possible. Prior to the approval and publication of the policy, use of open source software was prohibited by OCISO and ITSO.
- CDC program funding models are not structured for collaborative development and the development and use of shared services.

Considerations for the Future

- A key issue for all of CDC is that there are not distinct organizations for research, development, and operation and therefore does not follow industry best practices such as the Information Technology Infrastructure Library (ITIL) and Control Objectives for Information and Related Technology (CobiT).
- The planning, analysis, design and development of systems need to be guided by the broader enterprise archtecture context. Thus the NCPHI EA team must be a participant in all NCPHI systems development projects in the systems development lifecycle, as specified in the CDC Unified Process (CDC UP).
- NCPHI should conduct Enterprise Architecture analysis and comprehensive business process analysis prior to system development and adopt a central governance, review, and portfolio management process within NCPHI.
- Need to create governance for services. The lack of users for STARRS is an example of the building of services without governance or discoverability of those services.
- NCPHI should more effectively leverage available COTS/GOTS/Open Source products when possible.
- Instead of focusing on software development, NCPHI should be leading the collaborative development of interoperable service components.
- NCPHI should advance biomedical informatics science and lead its adoption by CDC and the public health community.
- NCPHI should discuss a development methodology that fosters reusable code, COTS products and Open Source Solutions when applicable. Because NCPHI currently has heavy utilization of non open source products, moving toward open source products

should be evaluated not just on cost, but alson on the value of public health partner collaboration.

- Several NCPHI systems are doing forms generation in different ways, these should be reviewed for standardization.
- ITSO provides backup/failover, hardware recovery, and server capacity planning; however, for applications that may run in the MTDC or DSS, they do not take responsibility for the typical systems management disciplines of change control, performance monitoring, configuration management, etc. NCPHI and other CC/NCs have to pick up those responsibilities, currently within the groups that do application development. Processes and cultural models that will foster successful system development should be evaluated.

3.4 IT Investment Alignment to Segments

As part of continued efforts to integration EA and CPIC program activities and incorporate architectural analysis in investment planning, the HHS EA Program initiated a new information request for IT investments proposed for the FY2010 HHS IT investment portfolio to be aligned to a primary segment, selected from a common list of HHS segments. The results of this investment-to-segment alignment are presented at Appendix A, which is included as a separate document due to the size of the report.

4 Transition Planning Milestones

The purpose of this section is to establish milestones related to significant individual initiatives and segment-related findings and recommendations listed in this Transition Strategy, to provide a basis for assessing transition progress against those milestones on an annual basis.

4.1 Summary of 2008 Milestones

As described in the previous sections of this document, the HHS Transition Strategy includes short and medium-term planning milestones covering the fiscal years 2008-2010. This section summarizes the milestones corresponding to segment architecture development activities recently completed at HHS. These milestones are derived from the findings and recommendations listed in the Segment Transition Plan for each completed segment.

Table 13: Transitional Milestones for 2008

Driver	Initiative	Milestones for 2008
Federal Transition Framework	Budget Formulation and Execution Line of Business	Evaluate FTF initiative elements as they are developed to determine potential for use by HHS
	Case Management Line of Business	Evaluate FTF initiative elements as they are developed to determine potential for use by HHS
	Disaster Management	Align HHS emergency preparedness and response processes, systems, data, and services with FTF initiative elements
	E-Authentication	Integrate E-Authentication services for grants.gov authentication; develop plan for enabling web-based HHS applications to use E-Authentication services
	E-Travel	Complete migration of all HHS OPDIVs to exclusive use of GovTrip service
	Federal Health Architecture (FHA)	Populate FTF catalog elements for the FHA initiative to reflect full scope of FHA activities and work products
	Financial Management Line of Business	Align UFMS processes and services to FTF initiative elements; expand use of HHS-offered financial management services to external agencies
	Geospatial Line of Business	Integrate HHS-maintained GIS Public Health data to Geospatial One-Stop
	Geospatial One-Stop	Integrate HHS-maintained GIS Public Health data to Geospatial One-Stop
	Grants Management Line of Business	Align ACF GATES processes to FTF initiative elements; increase internal and external use of HHS grants management services

Driver	Initiative	Milestones for 2008
	Grants.gov	Achieve 100% target for posting discretionary HHS grants to grants.gov
	HSPD-12	Issue FIPS 201 compliant ID cards to employees and contractors
	Human Resources Line of Business	Align EHRP processes and services to FTF initiative elements; expand use of HHS-offered HR services to external agencies
	Information Sharing Environment (ISE)	Evaluate FTF initiative elements as they are finalized to determine potential for use by HHS; contribute health alert and emergency preparedness and response data to ISE
	Information Systems Security (ISS) Line of Business	Develop plan for incorporating security services provided by another agency
	Integrated Acquisition Environment (IAE)	Evaluate FTF initiative elements as they are developed to determine potential for use by HHS; deploy HHS Consolidated Acquisition System
	Internet Protocol Version 6 (IPv6)	Continue implementation and migration activities according to mandated timeline; complete acquisition of IP addresses
	IT Infrastructure Optimization Line of Business	Evaluate FTF initiative elements as they are developed; align ITSC processes and services to FTF initiative
Health Information Technology	Health IT Standards Panel (HITSP)	Implement approved HITSP standards for appropriate uses within HHS; demonstrate compliance with standards
Strategic Planning Process	Telemedicine	Define initiative in preparation for formal proposal
	Performance Measurement Tool	Specify requirements and evaluate alternatives for solution
	Business Intelligence Solution	Implement solution and develop reports for decision support
	HHSIdentity	Implement solution chosen after pilot
	Enterprise Data Management	Establish plan for Data Architecture Work Group to execute prioritized initial data management activities
	Service-Oriented Architecture	Conduct SOA segment architecture development

4.2 E-Gov Milestones

HHS maintains a tracking inventory of milestones for all E-Gov initiatives. Within the context of the Enterprise Transition Strategy, the milestones presented here in Table 14 cover the historical

timeframe over the preceding year since the 2007 version of the Enterprise Transition Strategy was released, and the forward-looking timeframe over the next four quarters.

Table 14: HHS E-Gov Milestones

Initiative	Milestone	Date	Complete?
GovBenefits.gov	Execute all necessary inter-agency agreements (MOU,IAA, etc.) and complete funding transfers as required per agreement	Q2 2007	Yes
USA Services	Complete the USA Services "Government-wide Assessment of Citizen Service Activities" for all relevant citizen activities.	Q2 2007	Yes
E-Rulemaking	Begin Phase II implementation for Federal Docket Management System	Q2 2007	Yes
	Federal Docket Management System Configuration: All OPDIVs	Q4 2007	Yes
	Agency Kick-off Meeting: All OPDIVs	Q4 2007	Yes
	Convert paper-based docket processing to electronic processing using FDMS – train and implement all OPDIVS except FDA and CMS	Q4 2007	Yes
	Migrate agency rulemaking public comment systems to E-Rulemaking solution	Q4 2007	Yes
	Retire existing agency e-comment forms	Q4 2007	Yes
	Establish process within the agency for posting all agency rulemaking public comment announcements to E-Rulemaking solution	Q4 2007	Yes
	Execute all necessary inter-agency agreements (MOU,IAA, etc.) and complete funding transfers as required per agreement	Q2 2007	Yes
	Complete Testing and Evaluation of CMS and FDA Final Configuration	Q1 2008	Yes
	Train FDA and CMS	Q1 2008	Yes
	Shut down existing electronic agency rulemaking docket systems	Q2 2008	Yes
	Implement FDA and CMS	Q2 2008	
	Shut down existing agency rulemaking public comment systems	Q2 2008	
Federal Asset Sales	Inventory all systems that currently support personal property disposal and identify the systems that may be shut down	Q2 2007	Yes
	MOU or interagency agreements with selected sale centers, consistent with migration schedule	Q3 2007	Yes
	Consolidate/migrate personal property sales process to FAS Sales Centers	Q4 2007	Yes

Initiative	Milestone	Date	Complete?
	Provide required real property data on assets available for sale per the ESC approved process	Q4 2007	Yes
	Per agency's personal property migration certification, participate with the ESC/FAS PMO in the development of the temporary waiver process and complete draft version of agency waiver request	Q1 2008	Yes
	Shut down systems supporting the agency's existing personal property sales processes that are redundant to the initiative solution	Q1 2008	
	Complete request for waiver per temporary waiver process	Q2 2008	
	Provide required sales data and metrics on completed sales per ESC approved process	Q1 2008	Yes
Business Gateway	Execute all necessary inter-agency agreements (MOU,IAA, etc.) and complete funding transfers as required per agreement	Q2 2007	Yes
E-Vital	HHS Submit Draft regulation (NPRM) to OMB by 10/19/2007	Q1 2008	
	Post draft regulations in Federal Register	Q2 2008	
	Post final regulations in Federal Register	Q1 2009	
Grants.gov	Post all competitive discretionary grant application packages on Grants.gov to match posted opportunities in the current quarter, excluding any valid exemptions approved by OMB.	Q3 2007	Yes
	Develop the Outreach Plan for informing Grant Community	Q3 2007	
	Pilot Apply with Grants.gov users in the Grants.gov test environment	Q3 2007	
	Submit migration strategy and plan for implementing E-Authentication and migrating to HHS Authentication provider	Q4 2007	Yes
	Implement platform independent infrastructure using Adobe Solutions by May 1, 2007.	Q4 2007	Yes
	Post all competitive discretionary grant application packages on Grants.gov to match posted opportunities in the current quarter, excluding any valid exemptions approved by OMB.	Q4 2007	Yes
	Post all competitive discretionary grant application packages on Grants.gov to match posted opportunities in the current quarter, excluding any valid exemptions approved by OMB.	Q1 2008	Yes
	Implement Citrix Solution to address Mac issue	Q1 2008	Yes

Initiative	Milestone	Date	Complete?
	Develop project plan in conjunction with E-Authentication PMO to achieve production implementation of E-Authentication multiple CSPs to the Grants.gov Apply functionality for application submissions	Q1 2008	Yes
	Analyze the FY 2007 agency exemption requests for posting accompanying packages on Grants.gov and provide draft findings to OMB	Q1 2008	Yes
	Post all competitive discretionary grant application packages on Grants.gov to match posted opportunities in the current quarter, excluding any valid exemptions approved by OMB.	Q2 2008	
	Submit final analysis results with proposed exemption mitigation strategies to OMB and the GEB	Q2 2008	
	Implement OMB and GEM approved migration strategy	Q3 2008	
E-Training	Migrate old system to new system (E-Training Learning Management System service provider)	Q3 2007	Yes
	Migrate FDA to new Learning Management System	Q3 2007	Yes
	Consolidate training licenses and redundant courseware for FDA	Q3 2007	Yes
	Migrate NIH and IHS to new Learning Management System	Q4 2007	Yes
	Consolidate training licenses and redundant courseware for NIH	Q4 2007	Yes
	For those agencies adopting the EHRI eOPF, complete backfile conversion of personnel files	Q4 2007	Yes
	Decommission legacy LMS's except FDA and CDC systems	Q1 2008	Yes
	Decommission legacy LMS's at FDA and CDC	Q2 2008	
Enterprise Human Resources Integration (EHRI)	For those agencies adopting the EHRI eOPF, complete agency migration to eOPF	Q4 2007	Yes
	Develop plan for agency to migrate workforce planning and analysis reports to WASS/CIVFORS/BI environment	Q4 2007	Yes
	Provide Training Data File to EHRI	Q1 2008	

Initiative	Milestone	Date	Complete?
	Submit to OPM and OMB, a plan for agency to reach compliance for: 5% or less deficiency submissions for all security investigation requests; Agency submission of security investigations to OPM within 14 days or less using e-QIP; actual submission of security investigations within 5% of workload projections	Q2 2008	
	Provide training data feeds to EHRI each month for the entire agency per OPM Training; Reporting Requirements, 5 CFR Part 410, Vol. 71, No.95, dated May 17, 2006) for the entire agency (including all subcomponents of the organization and training cost data.)	Q3 2008	
	Provide technically compliant training data feeds to EHRI each month for the entire agency (including all subcomponents of the organization and training cost data.)	Q4 2008	
	Ensure the WASS/CIVFORS/BI tools are adequate for the CHCO to produce 5 year workforce agency plan and analysis using supporting output or data reports produced by WASS/CIVFORS/BI environment	Q4 2008	
E-Clearance	Submit to OPM and OMB, a plan for agency full submission/input of all security clearance information in CVS and use of CVS for the cross-agency verification and transfer of all security clearances by Q1 FY09.	Q2 2008	
	Submit to OPM and OMB, a plan for Agency to utilize e-QIP to process 95% of Agency's initial and re-investigations for SF 85-P (Public Trust investigations)	Q3 2008	
	Submit to OPM and OMB, a plan for Agency to utilize e-QIP to process 95% of Agency's initial and re-investigations for SF-85 investigations	Q4 2008	
	Agency compliance in the submission of no less than 95% of the SF-86 (National Security) investigations in e-QIP	Q4 2008	
	Agency full compliance in the submission of all security investigations into CVS.	Q1 2009	
	Agency compliance in the submission of no less than 95% of the SF-85 investigations in e-QIP	Q1 2009	
	Agency compliance in the submission of no less than 95% of the SF-85-P (Public Trust) investigations in e-QIP	Q1 2009	
E-Travel	Modify HHS ETS Task Order to support the implementation tasks and schedule and fund the NIH requirements by March 31, 2007.	Q3 2007	Yes

Initiative	Milestone	Date	Complete?
	Continue deployment in accordance with the updated MOU	Q3 2007	Yes
	Work design/development tasks with NGMS	Q4 2007	Yes
	Conduct kick-off meeting, integration and BPR workshops with the vendor and agree to project plan with NGMS	Q4 2007	Yes
	Complete development/testing with NGMS	Q1 2008	
	Start testing with NGMS	Q1 2008	
	Begin NIH deployment	Q1 2008	
	Complete testing and move forward	Q2 2008	
	Process all agency travel vouchers through ETS vendor	Q3 2008	
	Provide date of decommissioning of legacy system	Q3 2008	
	Train and complete deployment	Q3 2008	
E-Authentication	Determine approach for implementing E-Authentication for Grants.gov	Q3 2007	Yes
	Evaluate grant package posting service deployment by September 1, 2007.	Q4 2007	Yes
	All MOU identified systems perform live E-Authentication transactions	Q4 2007	
	Sign an MOU for integration of the E-Authentication service into: (1) the CMS Identity Management Utility, add at least 1 application behind the Utility (2) the FDA Identity Management Utility, add at least 1 application behind the Utility (3) the extension of E-Authentication functionality to at least 3 more applications behind the Center for Disease Control's Secure Data Network Identity Management Utility.	Q4 2007	Yes
	Develop project plan (by September 1) in conjunction with E-Authentication PMO to enable the application to accept SAML credentials from appropriate CSPs (e.g. the on demand CSP and other CSPs with credentials that end users may already have) into the production implementation of the Apply functionality for Grants.gov application submissions.	Q1 2008	Yes
	Complete project plan for implementing E-Authentication service on MOU identified systems by January 31	Q1 2008	Yes
	Pilot Apply with Grants.gov users in the Grants.gov test environment	Q2 2008	
Grants Management LoB	Execute signed Memorandum of Understanding (MOU) with Consortia Lead or submit appeal (including Fit /Gap analysis).	Q1 2008	Yes

Initiative	Milestone	Date	Complete?
	Develop an Implementation Strategy Plan that defines the agency's plan for implementing the GMLOB objectives.	Q2 2008	
Federal Health Architecture LoB	Revision and delivery of the FHA Program Plan reflecting Q3 activities approved by FHA Program Manager and ONC.	Q3 2007	Yes
	FHA Leadership Council Member Identification	Q3 2007	Yes
	Federal Health IT Investment Planning Guide and Educational Session (2)	Q3 2007	Yes
	Identify the appropriate resources to serve as FHA Leadership Council members.	Q3 2007	Yes
	Development and delivery of standards educational forums to agency members identified by the FHA Leadership Council Point of Contact	Q4 2007	Yes
	Completion of Food Safety Import architecture products and obtaining segment owners approval prior to submission into the Federal Transition Framework.	Q4 2007	Yes
	Development of the HIT investment planning guide and facilitation of related cross-agency collaboration and education.	Q4 2007	Yes
	Development of the Federal health Information reporting guide and facilitation of related cross-agency collaboration and education.	Q4 2007	Yes
	FHA's FY07 FTF Submission (includes: obtaining guidance/approval from FHA partners on products, priorities, time frame, and negotiating with OMB for out of cycle submission as needed).	Q4 2007	Yes
	FHA FY07 Program Plan Quarterly Updates	Q4 2007	Yes
	Standards Educational Forums	Q4 2007	Yes
	FHA Federal Transition Framework (FTF) Submission	Q4 2007	Yes
	Food Safety Import Architecture Products	Q4 2007	Yes
	Interoperability Specification Gap Analysis Report (Cycle 2)	Q4 2007	Yes
	Revision and delivery of the FHA Program Plan reflecting Q3 activities approved by FHA Program Manager and ONC	Q4 2007	Yes
	Development and submission of the agency IS IT Results Report	Q4 2007	Yes
	Development and submission of Gap Analysis Report	Q4 2007	Yes
	Complete Educational Forum Survey	Q2 2008	
	Complete Educational Forum Survey	Q3 2008	
	Complete Educational Forum Survey	Q4 2008	

Initiative	Milestone	Date	Complete?
	Creation of a Federal Reporting Guide	Q2 2008	
	NHIN-C Trial Conducted	Q3 2008	
	Publish FHA content to the FTF Catalog	Q4 2008	
Geospatial LoB	Submit populated performance reporting template for each of the A-16 datasets, following GeoLoB guidance, by 05/25/07.	Q3 2007	Yes
	Provide updated agency report on geospatial investments using the guidelines and template developed by the Geo LoB Task Force	Q3 2007	Yes
IT Infrastructure LoB	Submit a Department/Agency 5 year plan to optimize the End User Systems and Support area of IT infrastructure that is aligned with the ITI LOB Exhibit 300 Business Case (FY09)	Q2 2008	
Information Systems Security LoB	Work with the Information Systems Security Line of Business initiative to use security awareness and reporting services and develop a timeline with reasonable milestones for full implementation.	Q3 2007	
Disaster Assist Improvement Plan	Complete all Q2 activities for your agency included in the DAIP Implementation Plan.	Q2 2008	
	Complete all Q3 activities for your agency included in the DAIP Implementation Plan.	Q3 2008	
	Complete all Q4 activities for your agency included in the DAIP Implementation Plan.	Q4 2008	

4.3 Segment Transition Milestones

4.3.1 Enterprise Information Sharing Services

Sequencing for this segment is designed to (a) acquire a good inventory of existing ISE's, (b) standardize the level of documentation (e.g. create segment architectures), (c) create a common set of service definitions, and finally (d) begin the implementation planning and submit investment requests to move EISS forward.

Table 15: HHS EISS Segment Sequencing Recommendations

No.	Recommendation	Finding(s) Addressed	Investment Type	Dependencies	Priority	Timing
R-1	**Establish Information Sharing Sub-Function 262 under the Information and Technology Management LOB**	**F-1 F-3 F-4 F-5 F10**	**N/A**	**EISS PHIN FHA caBIG™**	**Very High should be first**	**Q2 FY08**

No.	Recommendation	Finding(s) Addressed	Investment Type	Dependencies	Priority	Timing
R-2	**Complete Health Information Survey**	**F2**	**Ongoing**	**All potential ISE's**	**Very High Must be completed in Q2 FY08**	**Q2 FY08**
R-3	**Create and Complete a Non-Health Information Survey**	**F2**	**O&M**	**N/A**	**High Must be completed in Q2 FY08**	**Q2 FY08**
R-4	**Create High Level Segment Architectures for Each Information Sharing Environment**	**F-6**	**New?**	**After R2**	**Very High Complete Q4 FY08**	**Q4 FY08**
R-5	**Isolate ISE Investments**	**F-8 F-10**	**N/A**	**After R2**	**Very High**	**Q3 FY08**
R-6	**Create and Fund an EISS Organization**	**F-12**	**New**	**After R5**	**High**	**Q4 FY08**
R-7	**Establish an ISE Council**	**F-1 F-3 F-4 F-5**	**O&M**	**With R6**	**High**	**Q3 FY08**
R-8	**Conduct High Level Implementation Planning for EISS**	**F-7 F-9 F-12**	**O&M**	**After R7**	**High**	**Q3 FY08**
R-9	**Establish an EISS Enterprise Architecture Framework**	**F-6 F-7 F-6**	**New**	**R-2 R-3 R-4 R-6**	**High**	**Q1 FY09**
R-10	**Update EISS Segment Architecture: Reconcile the Services Offered by the Many ISE's**	**F-7**	**New**	**Concurrent with R-9**	**Medium**	**Q1 FY09**
R-11	**Select Common Technology Base for EISS**	**F-9**	**New**	**After R-9**	**Low**	**Q2 FY09**
R-12	**Decouple Data Interchange Standards from EISS**	**F-12**	**Ongoing**		**Medium**	

4.3.2 Information Technology Infrastructure

In accordance with ITILoB requirements and working within HHS' existing federated IT infrastructure management model, HHS OCIO is requiring OPDIV CIOs (or their designated representatives) to develop and document OPDIV plans, using the GSA 5-Year Plan template, for optimizing their commodity IT Infrastructure and ultimately reducing infrastructure costs while maintaining quality of service. Specifically, OPDIV CIOs (or their designated representatives) are expected to:

- Develop a 5-Year Optimization Plan, using the GSA Template and following the guidance in this document, and submit it to HHS OCIO to be incorporated into an HHS Department-wide ITILoB 5-Year Optimization Plan submission

- Implement the strategies outlined in their individual 5-Year Optimization plans and report the results to HHS OCIO quarterly and annually, according to a HHS OCIO process that will be the subject of future guidance.

As part of this first ITI 5-Year Optimization Plan submission, OPDIVs are required to present plans for the End User System and Support Infrastructure Area. OPDIV plans to optimize Telecommunications Systems and Support and Mainframe and Server Services and Support infrastructure areas are optional in this submission and will not be required until those phases of the ITILOB are completed. At the present time, the remainder of this section addresses sequencing activities associated with the End User System and Support activities contained within the OPDIVs ITILoB 5-Year Optimization Plan.

The following table presents HHS OCIO's schedule for managing the development of a consolidated HHS Department-level ITILoB 5-Year Optimization Plan Submission. Following this table is a list of the HHS CIO's expectations associated with the schedule contained within the table.

Table 16: HHS OCIO ITILoB 5-Year Optimization Plan Development Schedule

	Task	Start	Finish
1	HHS/OPDIVs Review OPDIV EUSS Data to Verify Accuracy and Document Assumptions	12/20/07	1/11/08
2	HHS OCIO Develops and Issues 5-Year Optimization Plan Guidance	12/20/07	1/30/08
3	OPDIVs Develop 5-Year Optimization Plans	1/30/08	2/27/08
4	HHS OCIO Reviews/Comments on OPDIV 5-Year Optimization Plans	2/28/08	3/6/08
5	HHS OCIO Develops Draft Consolidated 5-Year Optimization Plan	3/7/08	3/21/08
6	Critical Partners Review/Comment on Draft Consolidated 5-Year Optimization Plan	3/24/08	3/26/08
7	HHS OCIO Finalizes 5-Year Optimization Plan based on comments	3/27/08	3/31/08

8	HHS OCIO Submits 5-Year Optimization Plan to GSA (EUSS only)	3/31/08	3/31/08

For the overall planned activities and their priorities to align the new IT Commodity Infrastructure Investment with the ITILoB services and systems, Table 17 below presents a detailed schedule with specific tasks activities and due dates.

Table 17: Consolidated It Commodity Infrastructure Exhibit 300 Task Schedule

Task	Due Date
HHS distributes Phase 1 Infrastructure E-300 Guidance and Process Description to OPDIVs	01/25/2008
HHS prepares and submits a Consolidated ITI LoB Infrastructure E-300 Remediation Plan to OMB	02/04/2008
OPDIVs establish new IT investments for their organizations and create OPDIV Consolidated IT Commodity Infrastructure Exhibit 300s.	02/19/2008
HHS prepares and distributes Phase 2 Consolidated IT Commodity Infrastructure Exhibit 300 Guidance to OPDIVs.	02/22/2008
OPDIVs prepare Part I, Sections A, B, and C of OPDIV Consolidated IT Commodity Infrastructure Exhibit 300.	03/10/2008
OPDIVs prepare remaining Parts and Sections of the Draft OPDIV Consolidated IT Commodity Infrastructure Exhibit 300 per HHS Phase 2 Guidance.	04/04/2008
HHS reviews/comments on OPDIV Draft Consolidated IT Commodity Infrastructure Exhibit 300.	04/25/2008
HHS develops HHS Draft Consolidated IT Commodity Infrastructure Exhibit 300.	05/27/2008
OPDIVs review/comment on draft HHS Consolidated IT Commodity Infrastructure Exhibit 300.	06/10/2008
HHS finalizes HHS Consolidated IT Commodity Infrastructure Exhibit 300.	06/18/2008
HHS finalizes HHS Consolidated IT Commodity Infrastructure Exhibit 300 for submission to OMB.	08/29/2008

These sequencing recommendations will become part of an overall modernization transition blueprint supporting HHS Enterprise Transition Strategy. The schedule and timing of these recommendations may also be based on their funding impact. The recommendations should fall into one of the following categories;

1. New Investments
   - HHS will submit a consolidated ITILoB E-300 for BY 2010
     - Consolidated ITILoB E-300 supported by 6 OPDIV contributing ITILoB E-300s
     - Shared infrastructure reported by lead/operating OPDIV
     - Content will be consistent with HHS 5-Year Optimization Plan
   - Separate non ITILoB Infrastructure
     - Specialized non-dedicated infrastructure
     - Infrastructure dedicated to mission investments
     - Program Initiatives
     - Other
   - HHS will submit a remediation plan to OMB for developing a BY 2010 Consolidated ITILoB E-300

2. HHS CIO Assumptions

- HHS will be held to current performance levels regardless of benchmarks
- Industry benchmarks will show improvement over time that we will be expected to match
- Exhibit 300 consolidation will be limited to the scope of ITILoB

3. HHS CIO Expectations
   - Infrastructure is overhead and should be minimized consistent with providing required mission support
   - OPDIVs will use the ITILoB 5 year plan process to add value to their infrastructure management
     - Continue to find opportunities to lower cost/improve service
     - Defend legitimate costs/relate cost to service levels
   - OPDIVs will be developing 5-Year ITI Optimization Plans that will be rolled up into an HHS Consolidated Plan
   - OPDIVs will align existing ITI metrics/management controls with ITILoB metrics, categories, and standards
   - HHS will have a standard IT Infrastructure Architecture
     - ITILoB (Commodity)
     - Other (Non commodity)
   - Completion of the government-wide IOI providing additional guidance toward the development of the IT infrastructure.

4.3.3 IT Security

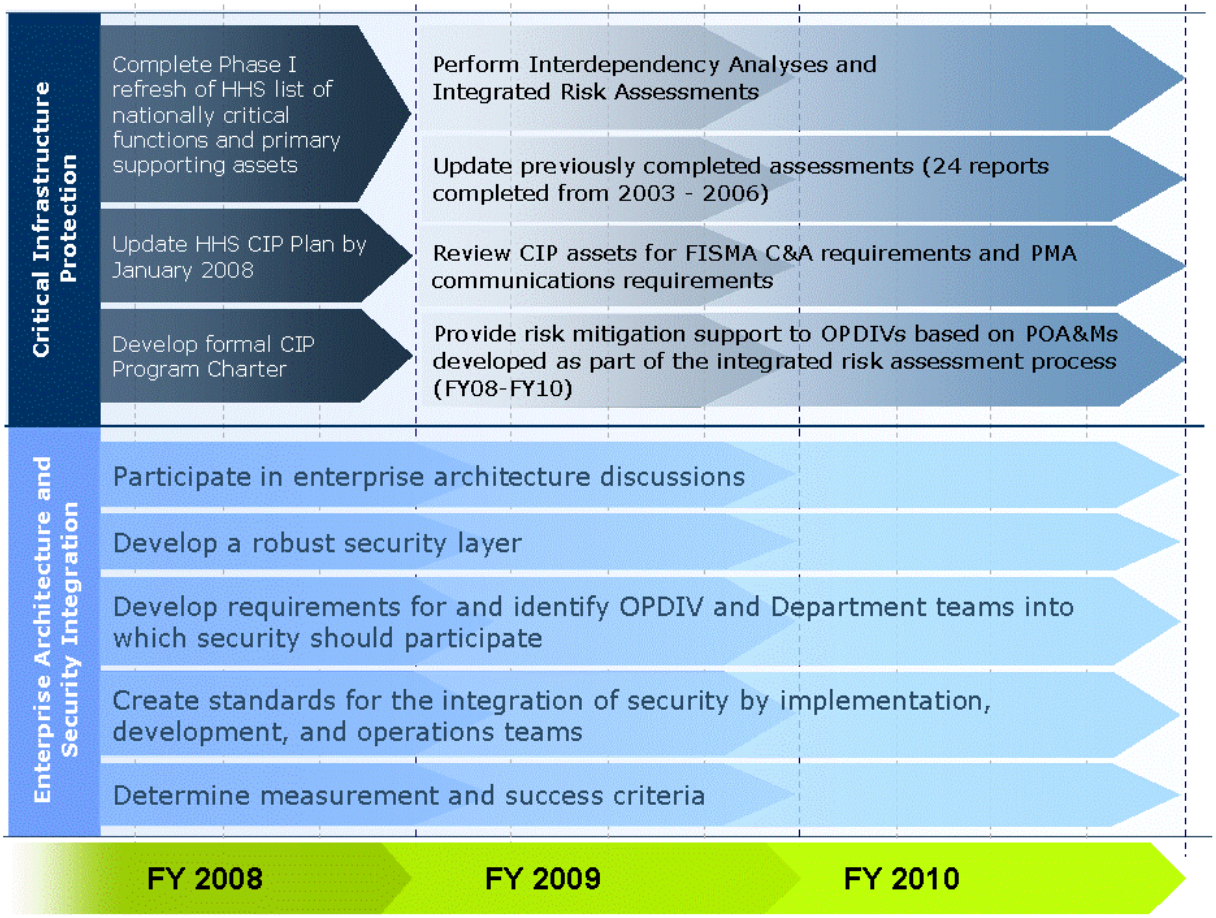
Integration with Enterprise Projects and Enterprise Architecture

The Secure One HHS integration of enterprise projects and enterprise architecture engages teams and organizations enterprise-wide to ensure that they are aware of and consider security requirements in their projects and planning activities.

The integration of security during the planning stages of enterprise projects and architecture efforts results in improved security at lower cost. This is achieved through the consistent application of security across HHS and requires a comprehensive approach that integrates security across the enterprise and ensures communication of, and compliance with security requirements, standards, and policies.

Secure One HHS will actively participate with enterprise teams and act as security advocates with necessary stakeholders managing the development, implementation, and operations of systems. Secure One HHS will also work closely with the Enterprise Architecture team to ensure that security is represented in all aspects of long term enterprise planning. Furthermore, Secure One HHS will collaborate with OPDIVs, the Office of the Assistant Secretary for Preparedness and Response (ASPR), and the Office of Security and Strategic Information (OSSI) on CIP, contingency / continuity of operations plan / procedures (COOP), and physical security initiatives.

Figure 2: IT Security EA Integration Milestones

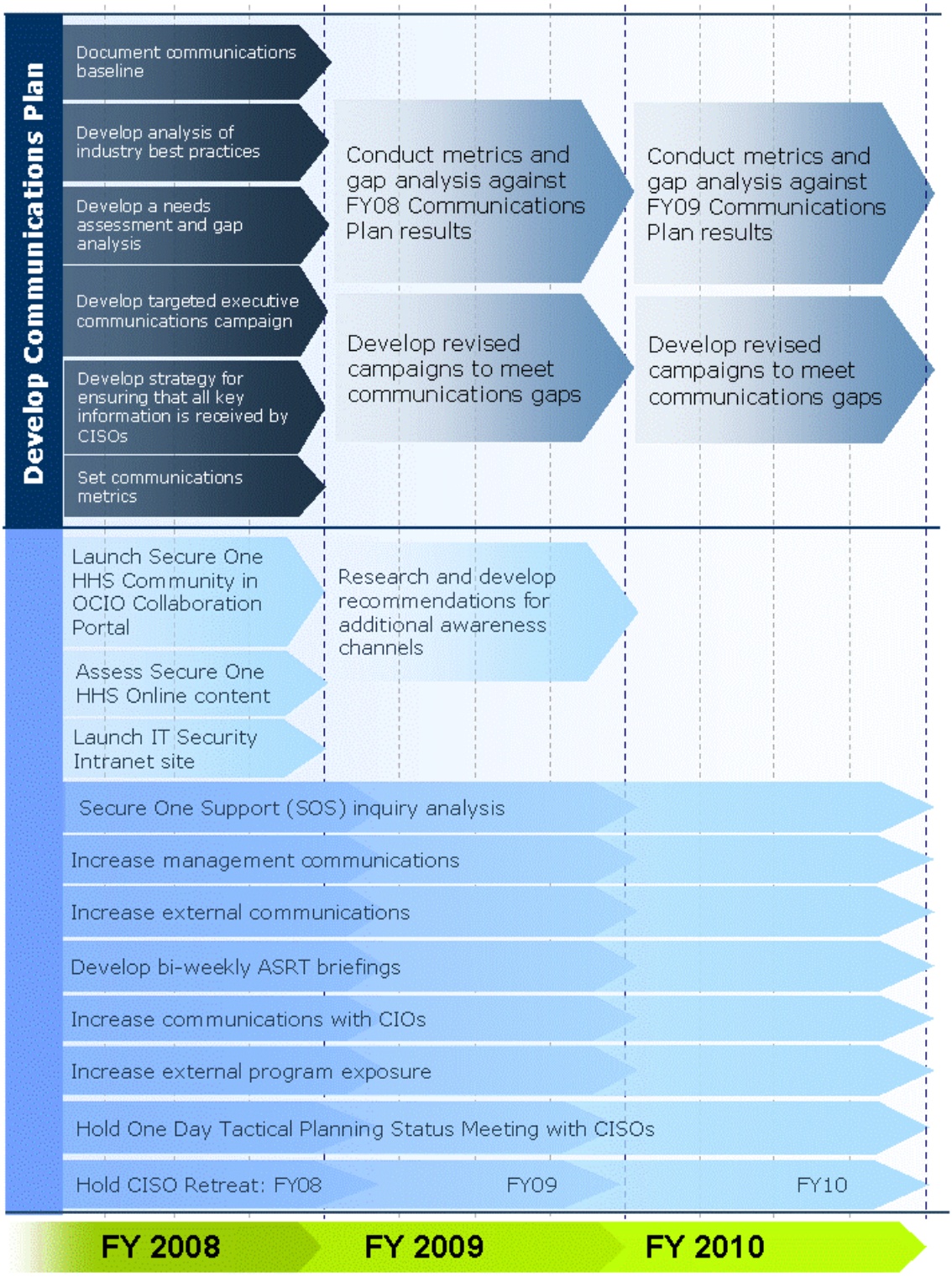


Communications

The importance of communication reaches beyond the notion of simply informing; it also creates a medium for establishing awareness, creating buy-in, and managing change. Effective communication is a critical component to any successful program. Stakeholders are often saturated with information, trying to sift the "must know" from the "nice to know" and processing new and complex information while meeting aggressive deadlines. Irrelevant, erroneous, or confusing messages often result in wasted time and effort, and poor decision making. Communications that enable stakeholders to take action and make informed decisions quickly and precisely must be developed.

In order to keep stakeholders informed, Secure One HHS will continue to communicate with executive leadership to ensure project goals and objectives are aligned. Additionally, we will continue to communicate new policy developments and technology implementations, so that deployment within the OPDIVs can occur in a timely manner. Finally, the Secure One HHS team will continue to focus communications around creating awareness and understanding of project goals and objectives, fostering support for the Secure One HHS program, and empowering stakeholders to take action.

Figure 3: IT Security Communications Milestones



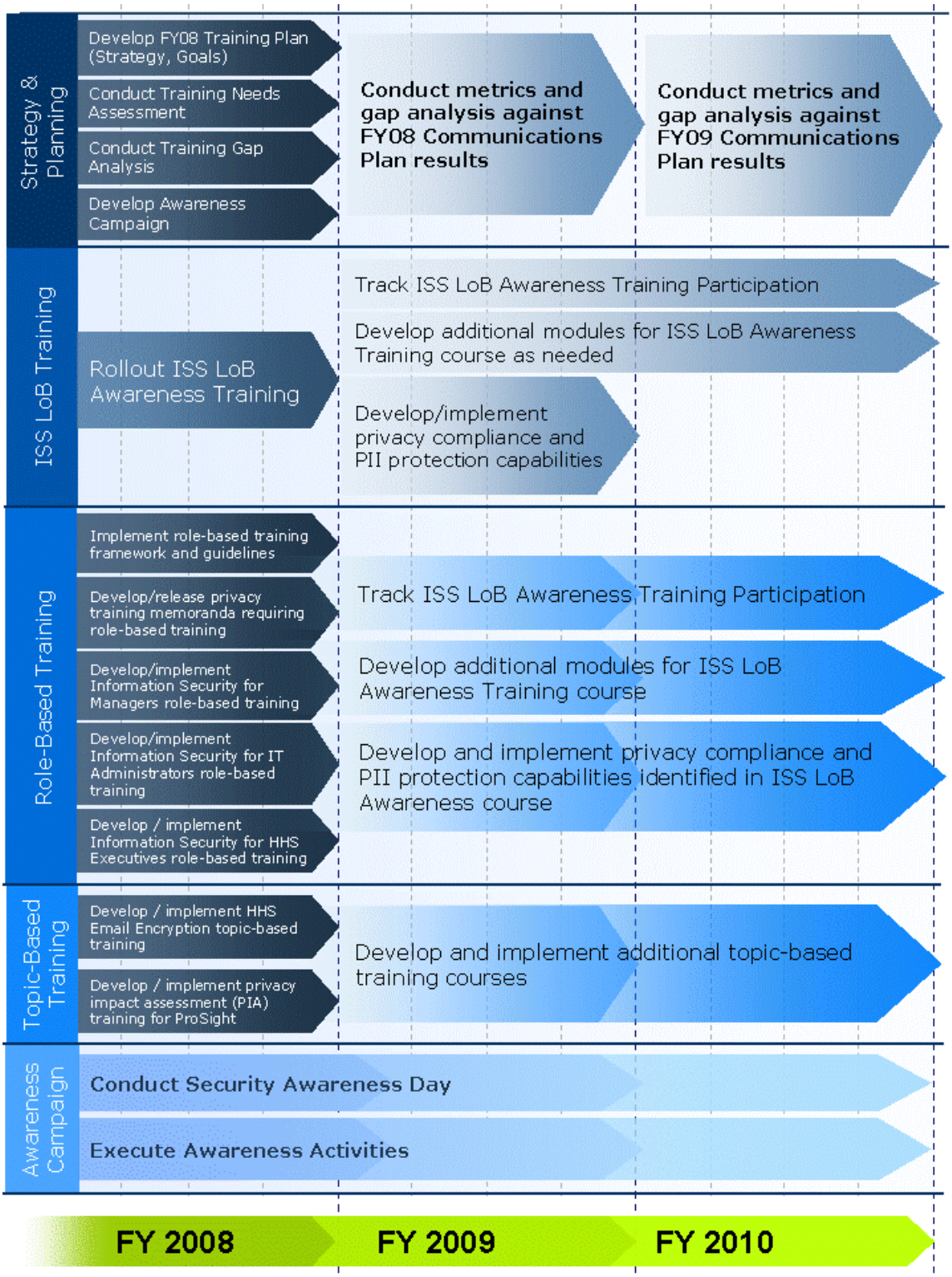
Structured Training Program

Training is a critical element of Program success and should be driven by workforce training goals in support of the Program's mission. A structured training program is a threefold. Primarily, it provides oversight for addressing baseline FISMA training requirements, such as the provision of annual security awareness and role-based training. Secondly, it provides a core security curriculum and course content that aligns with workforce training needs. Lastly, in addition to course delivery, a structured training program concurrently executes security awareness campaigns throughout the Department.

Establishing a structured training program will enable support to improve security competencies of the HHS workforce, enhance Department-wide security performance, and remove material weakness in HHS' information security program. It also promotes security workforce professional development as an effective countermeasure and an essential means of reducing operational risk. Lastly, a structured security program provides role-based security training to personnel with significant security responsibilities and tracks compliance.

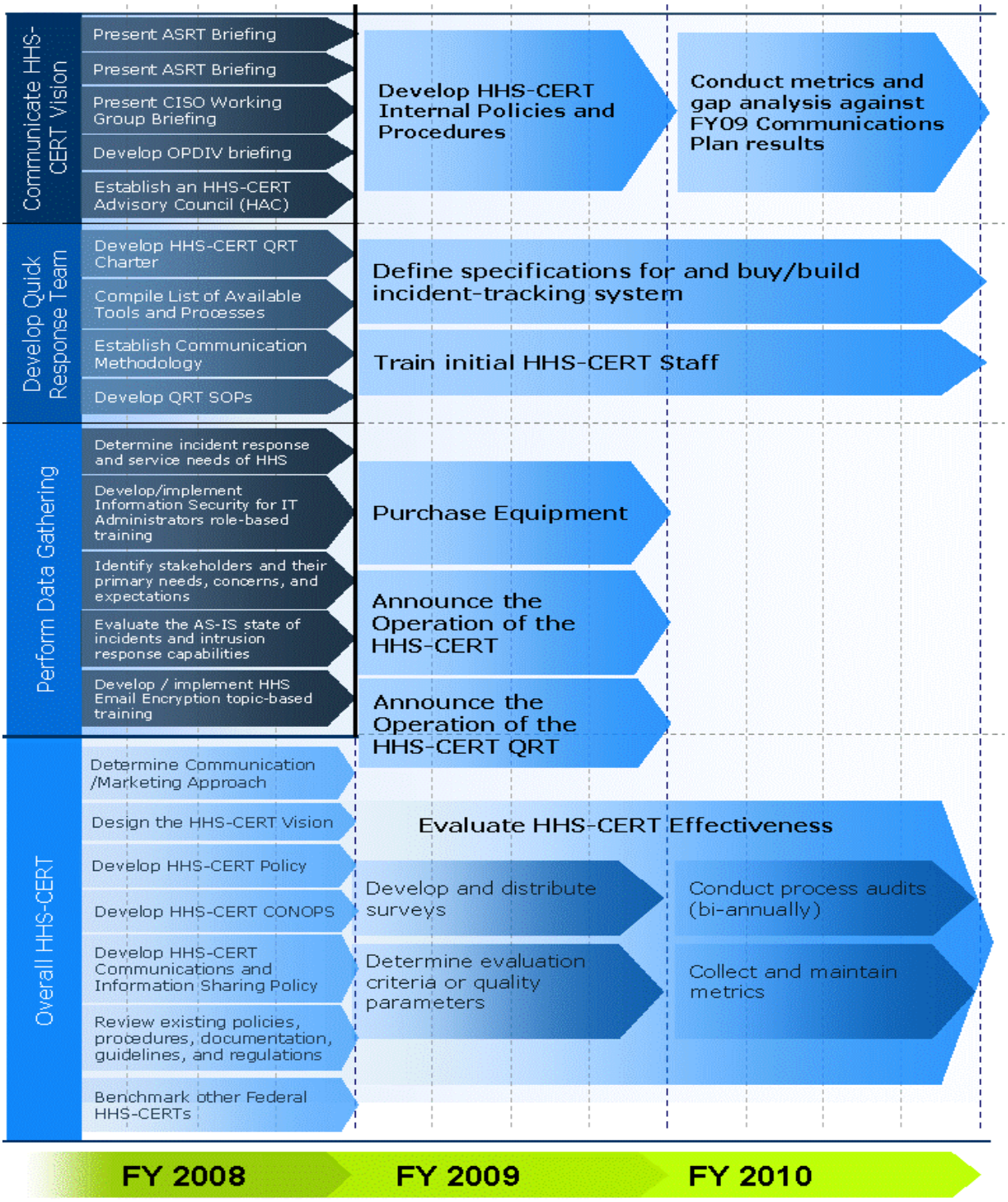
To establish a structured training program, an overarching training plan will be developed to identify the Program's training strategy and workforce development goals. A training needs assessment and gap analysis will then be conducted to determine workforce training needs and establish how existing courses address these needs. Finally, the results of this analysis will guide development of a core security curriculum and associated course content.

Figure 4: IT Security Structured Training Milestones



HHS-CERT Implementation

Figure 5: IT Security HHS-CERT Implementation Milestones



4.3.4 Public Health Informatics

To move from the current environment of large, monolithic systems and point to point interfaces to an environment of a Public Health Grid, CDC proposes a strategy consisting of these elements:

- Create a SOA Roadmap
- Establish the grid support environments
- Establish the test instance of the Grid.
- Create the minimal set of core services
- Establish short and long term transition strategies for all legacy systems and services
- Determine gaps in information services and prioritize development of new services

4.4 IT Investment Milestones

In an effort to increase HHS' ability to accurately gauge progress of its initiatives and activities, IT investment owners have been asked to provide quarterly milestones for all major and tactical investments proposed for inclusion in the FY2010 HHS IT investment portfolio. The resulting milestones are included at Appendix C, which is provided as a separate attachment due to the size of the report.

Appendix A HHS INVESTMENT ALIGNMENT TO SEGMENTS

Table 18: HHS Investments Aligned to Segments (with Business Area)

Due to the size of this table, Appendix A is provided as a separate attachment to the Enterprise Transition Strategy.

Appendix B HHS INVESTMENT ALIGNMENT TO THE FEDERAL TRANSITION FRAMEWORK

Table 19: HHS IT Investments Aligned to FTF Initiatives

FTF Initiatives	Investments
Budget Formulation and Execution Line of Business	CDC Health Impact Planning (HI.net/IRIS)
	Consolidated Infrastructure
	Financial Enterprise Solutions (FES)
	IT Governance
	NIH CIT Administrative Database System (ADB)
	NIH CIT Central Accounting System (CAS)
	NIH OD NIH Business System (NBS)
	FDA Financial Enterprise Solutions (FES)
	FDA IT Governance
	Financial Enterprise Solutions (FES)
	IT Governance
	OS ASAM Accounting for Pay System (AFPS)
	Department of Education
Case Management Line of Business	IT Governance
	Agency Information Management System (AIMS)
	FDA Mission Accomplishments and Regulatory Compliance Services (MARCS)
	Department of Justice
Disaster Management	CDC Enterprise Communication Technology Platform (ECTP)
	Consolidated Infrastructure
	FDA Automated Laboratory Management (ALM)
	IT Governance
	IT Security Program
	MDI Security System
	CDC Enterprise Communication Technology Platform (ECTP)
	Emergency Operations Network Incident Management System (EON IMS)
	FDA Emergency Operations Network Incident Management System (EON IMS)
	FDA Unified Registration and Listing (FURLS)
	HHS Secure One HHS
	Information and Computer Technologies for the 21st Century (ICT 21)
	MDI Security
	MDI Security System
	Department of Homeland Security

FTF Initiatives	Investments
E-Authentication	Electronic Submission Gateway (ESG)
	IT Governance
	IT Security Program
	CDC Enterprise Security
	CDC Secure Data Network (SDN)
	Electronic Submission Gateway (ESG)
	FDA Electronic Submission Gateway (ESG)
	HHS Secure One HHS
	HHSIdentity
	General Services Administration (GSA)
E-Travel	Consolidated Infrastructure
	FDA Automated Laboratory Management (ALM)
	Financial Enterprise Solutions (FES)
	IT Governance
	FDA Financial Enterprise Solutions (FES)
	Financial Enterprise Solutions (FES)
	PMA OS ASAM E-Gov Travel
	General Services Administration (GSA)
Federal Health Architecture (FHA)	CDC CCID Vaccine eXchange NETwork (VaX.NET)
	CDC Enterprise Communication Technology Platform (ECTP)
	CDC Health Impact Planning (HI.net/IRIS)
	CDC Information Technology Infrastructure
	CDC Knowledge Management Platform (formerly CDC Web Redesign)
	CDC National Health and Nutrition Examination Survey (NHANES)
	CDC National Select Agent Registry (NSAR)
	CDC National Vital Statistics System (NVSS)
	CDC NCHHSTP/GAP Country Specific Infrastructure
	CDC PHIN: BioSense
	CDC PHIN: LRN Real Time Laboratory Information Exchange
	CDC PHIN: National Electronic Disease Surveillance System (NEDSS)
	CDC PHIN: National Environmental Public Health Tracking Network (NEPHTN)
	CDC Public Health Information Network (PHIN)

FTF Initiatives	Investments
	CDC Stockpile Resource Planning System (SRP)
	CDC Surveillance, Preparedness, Awareness, and Response System for Vaccines (SPARx)
	CDC Technical Assistance Group (TAG) (formerly HAN and TADA)
	FDA Regulatory Business Information Services (RBIS)
	IHS Infrastructure, Office Automation & Telecommunications (IOAT)
	IHS National Patient Information Reporting System (NPIRS) - Maintenance & Enhancements
	IHS Resource Patient Management System (RPMS) - Maintenance & Enhancements
	IT Governance
	NIH CC Clinical Research Information System
	CDC Enterprise Communication Technology Platform (ECTP)
	CDC Health Impact Planning (HI.net/IRIS)
	CDC Knowledge Management Platform (formerly CDC Web Redesign)
	CDC National Health and Nutrition Examination Survey (NHANES)
	CDC National Healthcare Safety Network (NHSN)
	CDC National Healthcare Safety Network (NHSN)
	CDC National Select Agent Registry (NSAR)
	CDC National Vital Statistics System (NVSS)
	CDC NCHSTP/GAP Country Specific Infrastructure
	CDC PHIN: BioSense
	CDC PHIN: LRN Real Time Laboratory Information Exchange
	CDC PHIN: National Electronic Disease Surveillance System (NEDSS)
	CDC PHIN: National Environmental Public Health Tracking Network (NEPHTN)
	CDC Public Health Information Network (PHIN)
	CDC Stockpile Resource Planning System (SRP)
	CDC Surveillance, Preparedness, Awareness, and Response System for Vaccines (SPARx)
	CDC Technical Assistance Group (TAG) (formerly HAN and TADA)
	CDC Vaccine Ordering and Distribution System (VODS)
	CDER Postmarketing
	CDRH Electronic Submissions (CeSub)
	Center Legacy Applications and Support Systems (CLASS)
	Center Tracking System (CTS)
	CFSAN CAERS
	CFSAN FARM
	Compliance

FTF Initiatives	Investments
	Content Management System (CMS)
	Corporate Database Management System (CDMS)
	Corporate Database Portal (CDP)
	Electronic Submission System (ESS)
	FACTS@FDA
	FACTS@FDA
	FDA Automated Drug Information Management System
	FDA Automated Laboratory Management (ALM)
	FDA CBER Electonric Submission (FY09)
	FDA CBER Electronic Submission Program (FY08)
	FDA CBER NonPDUFA (FY09)
	FDA CBER NonPDUFA Systems (FY08)
	FDA CBER PDUFA (FY09)
	FDA CBER PDUFA Systems (FY08)
	FDA CBER Regulatory Management System- BLA (FY08)
	FDA CBER RMS-BLA (FY09)
	FDA CFSAN CAERS
	FDA CFSAN Core IT
	FDA CFSAN FARM
	FDA CFSAN Scientific Computing & Application Interface
	FDA CFSAN Supporting and Enabling IT
	FDA Mission Accomplishments and Regulatory Compliance Services (MARCS)
	FDA Regulatory Business Information Services (RBIS)
	FDA Unified Registration and Listing (FURLS)
	Federal Health Architecture -- Managing Partner
	Integrated Services for Veterinary Medicine (ISVM)
	IT Governance
	Mammography Program Reporting and Information System (MPRIS)
	Medical Expenditure Panel Survey (MEPS)
	Medical Product Surveillance Network (MedSuN)
	MedWatch Plus
	NCTR Research IT (FY08)
	OS ONC Prototype Nationwide Health Informtion Network (NHIN)
	OS ONC Standards & Certification for Health IT
	Premarket Modernization Program (PMP)
	Science FIRST
	United States Department of Health & Human Services
Financial Management Line of Business	CDC Health Impact Planning (HI.net/IRIS)
	CDC Integrated Contracts Expert (ICE)
	Consolidated Infrastructure
	FDA Automated Laboratory Management (ALM)
	Financial Enterprise Solutions (FES)
	IT Governance

FTF Initiatives	Investments
	NIH CIT Administrative Database System (ADB)
	NIH CIT Central Accounting System (CAS)
	NIH OD NIH Business System (NBS)
	CDC Health Impact Planning (HI.net/IRIS)
	CDC Integrated Contracts Expert (ICE)
	FDA Financial Enterprise Solutions (FES)
	FDA IT Governance
	Financial Enterprise Solutions (FES)
	HHS Unified Financial Management System
	IT Governance
	OS ASAM Accounting for Pay System (AFPS)
	OS ASAM Core Accounting System (CORE)
	OS ASAM Debt Management and Collection System (DMCS)
	OS ASAM Payment Management System (PMS)
	General Services Administration (GSA)
Geospatial Line of Business	CDC ATSDR Geographic Information System
	FDA Automated Laboratory Management (ALM)
	IT Governance
	CDC ATSDR Geographic Information System
	Emergency Operations Network Incident Management System (EON IMS)
	Department of Interior
Geospatial One-Stop	CDC ATSDR Geographic Information System
	FDA Automated Laboratory Management (ALM)
	IT Governance
	CDC ATSDR Geographic Information System
	Department of Interior
Grants Management Line of Business	ACF Grants Administration Tracking Evaluation System (GATES) - Grants Center for Excellence
	FDA Automated Laboratory Management (ALM)
	IT Governance
	Grants.gov -- Find and Apply
	NIH OD Electronic Research Admin (eRA)
	United States Department of Health & Human Services
Grants.gov	ACF Grants Administration Tracking Evaluation System (GATES) - Grants Center for Excellence
	FDA Automated Laboratory Management (ALM)
	IT Governance
	NIH NCI Cancer Therapy Evaluation Program (CTEP)
	NIH OD Electronic Research Admin (eRA)
	Grants.gov -- Find and Apply
	United States Department of Health & Human Services
HSPD-12	Consolidated Infrastructure
	FDA Automated Laboratory Management (ALM)
	IHS Infrastructure, Office Automation & Telecommunications (IOAT)
	IT Governance

FTF Initiatives	Investments
	IT Security Program
	MDI Security System
	CDC Enterprise Security
	CDC Secure Data Network (SDN)
	HHS Secure One HHS
	HHSIdentity
	MDI Security
	MDI Security System
	General Services Administration (GSA)
Human Resources Line of Business	Consolidated Infrastructure
	FDA Automated Laboratory Management (ALM)
	IT Governance
	Administrative Systems Automation Project (ASAP)
	HHS HR LOB IT
	OS ASAM Enterprise Human Resource System (EHRP)
	OS OPHS Commissioned Corps Force Management (CCFM)
	OS OPHS Commissioned Officers Personnel and Payroll System (COPPS)
	Office of Personnel Management (OPM)
Information Sharing Environment (ISE)	Consolidated Infrastructure
	FDA Automated Laboratory Management (ALM)
	IHS Infrastructure, Office Automation & Telecommunications (IOAT)
	IHS National Patient Information Reporting System (NPIRS) - Maintenance & Enhancements
	IHS Resource Patient Management System (RPMS) - Maintenance & Enhancements
	IT Governance
	NIH Business Intelligence System (NBIS)
	Administrative Systems Automation Project (ASAP)
	FDA IT Governance
	FDA Unified Registration and Listing (FURLS)
	HHS Web Management Project
	Information and Computer Technologies for the 21st Century (ICT 21)
	IT Governance
	Office of the Director of National Intelligence (DNI)
Information Systems Security Line of Business	FDA Automated Laboratory Management (ALM)
	IHS Infrastructure, Office Automation & Telecommunications (IOAT)
	IT Governance
	CDC Enterprise Security
	CDC Secure Data Network (SDN)
	HHS Secure One HHS
	HHSIdentity
	Information and Computer Technologies for the 21st Century (ICT 21)

FTF Initiatives	Investments
	IT Security Program
	Department of Homeland Security
Integrated Acquisition Environment (IAE)	FDA Automated Laboratory Management (ALM)
	Financial Enterprise Solutions (FES)
	IT Governance
	FDA Financial Enterprise Solutions (FES)
	Financial Enterprise Solutions (FES)
	General Services Administration (GSA)
Internet Protocol Version 6 (IPv6)	FDA Automated Laboratory Management (ALM)
	IHS Infrastructure, Office Automation & Telecommunications (IOAT)
	IT Governance
	CDC Information Technology Infrastructure
	Consolidated Infrastructure
	HHS Secure One HHS
	HHSIdentity
	Information and Computer Technologies for the 21st Century (ICT 21)
	Office of Management and Budget (OMB)
IT Infrastructure Optimization Line of Business	FDA Automated Laboratory Management (ALM)
	IHS Infrastructure, Office Automation & Telecommunications (IOAT)
	IT Governance
	NIH IT Infrastructure
	CDC Information Technology Infrastructure
	Consolidated Infrastructure
	HHS Enterprise E-mail System (HHSMail)
	Information and Computer Technologies for the 21st Century (ICT 21)
	OS IT Service Center
	General Services Administration (GSA)

Appendix C HHS MILESTONES FOR MAJOR AND TACTICAL INVESTMENTS

Table 20: Quarterly Milestones for HHS Major and Tactical Investments

Due to the size of this table, Appendix C is provided as a separate attachment to the Enterprise Transition Strategy.

Appendix D ACRONYMS AND ABBREVIATIONS

Table 21: Acronyms and Abbreviations

ACF	Administration for Children and Families
AOA	Administration on Aging
AHRQ	Agency for Healthcare Research and Quality
ASPR	Assistant Secretary for Preparedness and Response
ASRT	Assistant Secretary for Resources and Technology
ATSDR	Agency for Toxic Substances and Disease Registry
BRM	Business Reference Model
CCA	Clinger-Cohen Act of 1996 (Information Technology Management Reform Act)
CDC	Centers for Disease Control and Prevention
CEA	Chief Enterprise Architect
CFO	Chief Financial Officer
CHI	Consolidated Health Informatics
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare and Medicaid Services
CPIC	Capital Planning and Investment Control
CRM	Consolidated Reference Model
CTO	Chief Technology Officer
DASIT	Deputy Assistant Secretary for Information Technology
DRM	Data Reference Model
E-Gov	Electronic Government
EA	Enterprise Architecture
EHRP	Enterprise Human Resources and Personnel System
EPLC	Enterprise Performance Life Cycle
FDA	Food and Drug Administration
FEA	Federal Enterprise Architecture
FHA	Federal Health Architecture
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002 (E-Government Act)
FTF	Federal Transition Framework
GAO	Government Accountability Office
GPRA	Government Performance Results Act of 1993
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITSP	Health Information Technology Standards Panel

HHS	Health and Human Services
HR	Human Resources
HRSA	Health Resources and Services Administration
HSPD-12	Homeland Security Presidential Directive 12
IHS	Indian Health Services
IRM	Information Resources Management
IT	Information Technology
ITIRB	Information Technology Investment Review Board
ITSC	Information Technology Services Center
LOB	Line of Business
NBS	NIH Business System
NIH	National Institutes of Health
NIST	National Institute for Standards and Technology
OCIO	Office of the Chief Information Officer
OEA	Office of Enterprise Architecture
OIG	Office of the Inspector General
OMB	Office of Management and Budget
ONC	Office of the National Coordinator for Health Information Technology
OPDIV	Operating Division
OS	Office of the Secretary
PMA	President's Management Agenda
PRM	Performance Reference Model
PSC	Program Support Center
RPMS	Resource and Patient Management System
SAMHSA	Substance Abuse and Mental Health Services Administration
SOA	Service-Oriented Architecture
SRM	Service Component Reference Model
SSP	Shared Service Provider
STAFFDIV	Staff Division
TRM	Technical Reference Model
UFMS	Unified Financial Management System

Appendix E REFERENCES

Table 22: References

Reference
HHS Information Resources Management Strategic Plan 2007-2012
HHS Performance Management Plan
HHS OCIO Policy for IT Capital Planning and Investment Control
HHS OCIO CPIC Procedures
HHS Enterprise Performance Life Cycle
HHS OCIO IT Policy for Enterprise Architecture
HHS Information Security Program Policy
HHS Transition Strategy
HHS EA Program Management Plan
HHS EA Configuration Management Plan
HHS EA Communications and Outreach Plan
HHS EA Segment Architecture Development Methodology
HHS EA Framework
HHS EA Modeling Guide
Federal Enterprise Architecture Consolidated Reference Model v2.1
Federal Transition Framework v1.0
Federal Enterprise Architecture Practice Guidance