Social Security

Information Resources Management Strategic Plan

Fiscal Year 2004

www.socialsecurity.gov

From the Office of the Chief Information Officer

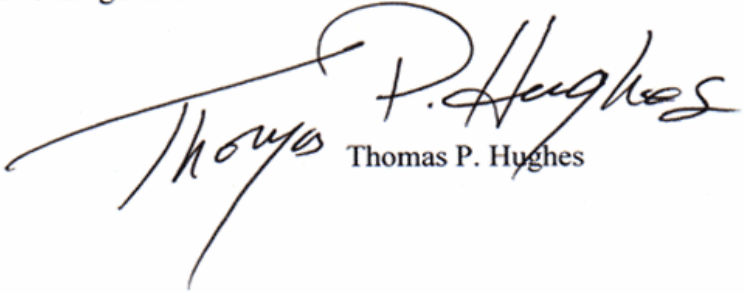
During the course of the past year we have made considerable progress in addressing the significant challenges SSA faces in administering its complex programs. Efficient and effective management of our information technology resources is a major factor in the progress that has been made.

Our efforts continue to be focused on initiatives supporting SSA's mission, values, goals and objectives as articulated in the Agency Strategic Plan, the Agency Performance Plan, and the President's Management Agenda. These information technology initiatives include paperless processing and moving to electronic folders. We are well into implementation of the accelerated electronic disability process, a major initiative to move all SSA components involved in disability claims process to an electronic business process through the use of an electronic disability folder. Also, our use of speech recognition technology has reduced processing times for drafting hearing decisions and we are using scanning technology to control incoming folders in the Office of Appellate Operations Megasite.

Expanding E-Government is one of the items included in the President's Management Agenda and represents a major commitment by this Agency. SSA is expanding the use of services via the Internet to provide an alternative method of service delivery for the increasing numbers of Americans who are conducting business through the Internet. These and other technology development approaches are described in this document.

We have implemented our System Security Plan that integrates security into all information systems major investments and adopts a security architecture which has been integrated into our Enterprise Architecture. The System Security Plan also integrates new security standards and technology into SSA's business processes to protect software and hardware from both physical and cyber security threats. These are critical steps in ensuring protection of the public trust.

This IRM Strategic Plan will continue to evolve throughout 2004 as we address workloads ahead and the opportunities they present. Implementation of the Medicare Prescription Drug Bill recently passed by Congress tied with budget constraints poses a significant challenge for the Agency. We will use the IRM Strategic Plan as a tool to assist the Agency in making effective decisions regarding the use of technology for our employees and the citizens and businesses we serve. In conclusion, we will continue to hone the careful delivery of Information Technology to meet Commissioner Barnhart's priorities as they are reflected in the Agency's strategic goals and objectives, as well as the goals of President Bush's Administration.



Thomas P. Hughes

This Page Has Been Left Blank Intentionally

Table of Contents

Executive Summary 1

Chapter 1: Introduction 5

Brief History of Information Technology Planning 5
Regulatory basis 6
Relationship to Other Strategic Planning Documents 7
President's Management Agenda 7
Agency Strategic Plan (ASP) 8
Information Planning and Management Framework 9
Governance 10
Use of the IRM Plan 10

Chapter 2: IRM Strategic Goals and Objectives 13

IRM Objectives/Systems Management Objectives 13
Planning Assumptions 13
Systems Guiding Principles 14
SSA Organizational Chart 14

Chapter 3: SSA Enterprise Architecture Framework 17

Conformance to Federal Standards and Guidelines 17
Purpose of the EA Framework 18
Tailoring the Framework Content 19
Framework Structure 20
Description of Architecture Definitions 22

Chapter 4: IT Security Strategy 27

Overview 27
Security Functions and Responsibilities 27
Statutory Requirements 28
Strategy for current and strategic planning efforts 29
System Development Life Cycle (SDLC) 29
Secure Communications & Authentication 29
SmartCards 30
Biometrics 30
Sensitive Systems Security Plans 30
Access Controls 31
Audit Trail System 31
Critical Infrastructure Protection 31
Intrusion Protection Team 32
Security Response Team 32

Chapter 5: IT Performance/Investments 35

Performance 35

Agency Priorities 36
E-Government 36
Electronic Service Delivery 39
IT Capital Plan Summary 40
Major Investment Initiatives 43
Infrastructure 43
Telecommunications 44
Office Automation 45
Accelerated eDib 45
Electronic Wage Reporting System 46
Ongoing DDS Automation 47
Financial Accounting System Replacement 48
Digital Audio for the Recording of ALJ Hearings 48
Access to Financial Institutions 49
Title II System Redesign 50
Paperless Processing Centers 51
SUMS/MCAS 51
eVital 52
Employees With Disabilities 53
Interactive Video Teletraining 54
Software Imaging Management 55

Chapter 6: Process Management 61

Capital Planning and Investment Control 61
Information Technology Capital Plan 61
Target Capital Planning and Investment Control Process 62
Systems Development Management 64
Software Process Improvement Using the Capability Maturity Model 64
Systems Development Process Engineering 64
Process Assets Library 64
Project and Integration Management 65
Quality Control and Quality Assurance 65
Systems Validation and Verification 66
Systems Validation 66
Systems Verification 66
Web Testing and Validation 66
Systems Life Cycle Management 67
Data Administration 68
Architecture Review Board 68
Usability 69
Section 508 Compliance 69
Configuration Management 69
Data Center Management 70
Network Customer Service Center 70
National Network Service Center 71
Capacity Management 71

Methodology 71
Performance and Service Level Management 72
Business Recovery 75
Business Recovery Computing Environment 75
Business Continuity and Contingency 76
Applied Technology at SSA 76
Technology Trends 77

Chapter 7: IT Human Resources Management 81

Commitments to SSA Employees 81
The Staffing Picture 81
Future Skill Needs 83
Plan for Meeting Future Skill Needs 86
Employee Training 87
E-Learning 89
Graduate-Level Training Program 90
Recruitment Strategy and Employment Incentives 91
Recruitment Strategy 91
Compensation 92
Entry-Level Commitment 92
Recruitment Focus 93
Workplace Incentives 93
Support Services and Competitive Sourcing 94

Chapter 8: Budget Perspective 95

The Budget Outlook 96

Appendix 98

Summaries of Current and Target Architectures 98

Business Process Architecture 98
Information flow/Relationships of Core Business Processes 98
Enumeration 100
Earnings 101
Claims 103
Postentitlement 104
Informing The Public 107
Key Support Processes 107
Administrative and Management Information Systems 107
Program Policy Process 108
Information Technology Infrastructure 108
Application Architecture 108
Application Software 108
Programmatic Systems 110
Strategic Goals for Programmatic Systems 110
Increased Automation 111

Enhanced Applications Security 113
Local Support System Integration 114
Client Self-Help Capabilities 115
Paperless Processing 116
Software Efficiency and Maintainability 118
Additional Target Architecture Information 119
Administrative Systems 119
Administrative Business Architecture 121
Management Information 124
Workload Management 125
Work Measurement 125
General Management Information 126
Management Information (MI) Architecture 126
Data Architecture 128
Data Administration Sub-Architecture 130
Existing Data Administration Sub-architecture 130
Target Data Administration Sub-architecture 131
Database Management Sub-architecture 132
Future Database Management Sub-Architecture 134
Infrastructure Architecture 136
Client/Server 138
Service Area Definition 138
Current Architecture 138
Target Architecture 139
Transition 140
Database Management Support 141
Service Area Definition 141
Current Architecture 141
Target Architecture 142
Transition 142
Desktop 143
Service Area Definition 143
Current Architecture 143
Target Architecture 144
Transition 144
Electronic Messaging 145
Service Area Definition 145
Current Architecture 145
Target Architecture 146
Transition 146
Imaging and Document Management 149
Service Area Definition 149
Current Architecture 149
Target Architecture 150
Transition 151
Internet 152

Service Area Definition 152
Current Architecture 152
Target Architecture 153
Transition 153
Intranet 155
Service Area Definition 155
Current Architecture 155
Target Architecture 156
Transition 156
Local Area Network 158
Service Area Definition 158
Current Architecture 158
Target Architecture 159
Transition 159
Mainframe 160
Service Area Definition 160
Current Architecture 160
Target Architecture 161
Transition 162
Print Services 163
Service Area Definition 163
Current Architecture 163
Target Architecture 164
Transition 164
Security Systems 166
Service Area Definition 166
Current Architecture 166
Target Architecture 170
Transition 171
Storage 172
Service Area Definition 172
Current Architecture 172
Target Architecture 173
Transition 173
Telephone 175
Service Area Definition 175
Current Architecture 175
Target Architecture 177
Transition 177
Video Architecture 179
Service Area Definition 179
Current Architecture 179
Target Architecture 180
Transition 180
Wide Area Network 182
Service Area Definition 182

Current Architecture 182
Target Architecture 183
Transition 184

Transition Strategy 186

Summary of strategy 186
Nature and Scope of the Transition Effort 186
Adoption of Enterprise-Based Methodologies 188
Implementation Segment Selection 189
Work Planning and Scheduling 191
Prototypes, Pilots and Phased Implementations 192
Integration Planning 193
Transition Architectures 194
Integration Testing 196
Communication and Feedback 196
Conclusion 197

SSA IT Systems Security Plan 198

Introduction 198
Incorporating and Funding Security in Information Systems Investments 198
SSA's Security Architecture 199
Identification 200
Authentication 201
Authorization 201
Other Security Considerations 202
Agency Current and Future IT Security Initiatives 203
Intrusion Detection 203
Smart Card Technology 203
Biometrics 204
Access Control (Computer Associates - Top Secret) 204
Standardized Security Profile Project (SSPP) 204
PSC Segregation of Duties 204
eTrust Single Sign-On (SSO) 204
Roles and Responsibilities 205
Chief Information Officer (CIO) 205
SSA Chief Security Officer (SSACSO) 206
Office of Systems Security Operations Management (OSSOM) 206
Office of Facilities Management (OFM) 206
Deputy Commissioner for Systems (DCS) 207
Deputy Commissioner for Operations (DCO) 207
Office of Inspector General (OIG) 207
All Deputy Commissioners 207

Glossary 208

Index 218

Figures

Figure 1: Alignment of Strategy/Planning Documents 9
Figure 2: SSA's Organizational Chart 15
Figure 3: Federal Enterprise Architecture Planning Model 19
Figure 4: Milestone Chart 1 56
Figure 5: Milestone Chart 2 57
Figure 6: Milestone Chart 3 58
Figure 7: Milestone Chart 4 59
Figure 8: Target Capital Planning and Investment Control Process 63
Figure 9: Service Level Methodology 74
Figure 10: FY 2002 Losses and Hires 82
Figure 11: FY 2003 Estimated FTEs 83
Figure 12: SSA / Information Technology FY 2005 President's Budget 95
Figure 13: The Budget Outlook 96
Figure 14: The Social Security Administration's Core Business Processes 99
Figure 15: Enumeration 100
Figure 16: Earnings 102
Figure 17: Claims 103
Figure 18: Postentitlement 106
Figure 19: Informing the Public 107
Figure 20: Programmatic Software Architecture 109
Figure 21: Administrative Business Architecture 122
Figure 22: Management Information Architecture 126
Figure 23: Components of Data Architecture 128
Figure 24: Assignment of Data Management Functions to Architectural Components 129
Figure 25: SSA's Database Architecture 133
Figure 26: Service Area Relationships 137
Figure 27: Client/Server Architecture 138
Figure 28: Database Architecture 141
Figure 29: Desktop Architecture 143
Figure 30: Electronic Messaging Architecture 145
Figure 31: Imaging Architecture 149
Figure 32: Internet Architecture 152
Figure 33: Intranet Architecture 155
Figure 34: LAN Architecture 158
Figure 35: Mainframe Architecture 160
Figure 36: Print Services Architecture 163
Figure 37: Security Architecture 166
Figure 38: Storage Architecture 172
Figure 39: Telephone Architecture 175
Figure 40: Video Architecture 179
Figure 41: WAN Architecture 182
Figure 42: Basis of Transition Strategy 187
Figure 43: Identification of Implementation Segments 190
Figure 44: Transition Architectures 195
Figure 45: SSA's Security Architecture 200

Tables

Table 1: Federal Enterprise Architecture Framework, Level IV 19
Table 2: SSA Enterprise Information Technical Architecture Framework 21
Table 3: Descriptions of Models and Other Architectural Products 22
Table 4: Major SSA Workloads 35
Table 5: Major Investment Initiatives 43
Table 6: Future Skill Areas 84
Table 7: Initiatives to Achieve Programmatic Application Goals 111
Table 8: Components of the SSA Data Administration Sub-architecture 131

Executive Summary

The Social Security Administration's (SSA) Information Resources Management (IRM) Strategic Plan provides a description of how IRM activities help accomplish the Agency's mission and realize SSA's strategic goals and objectives. The plan ensures that IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management and program decisions. The IRM Strategic Plan is aligned with and driven by SSA's Agency Strategic Plan (ASP), the Administrative Budget and the Annual Performance Plan (APP), and it supports the President's Management Agenda (PMA). The IRM Strategic Plan is a key component in SSA's information technology (IT) capital planning and investment control (CPIC) process that is used for the ongoing identification, selection, control and evaluation of investments in information resources.

The ASP establishes the course for achieving measurable results that matter to the American public. It articulates the Agency's mission, values, goals and objectives as well as key outcomes the Agency aims to achieve. It sets forth four comprehensive strategic goals:

- To deliver high-quality, citizen-centered service
- To ensure superior stewardship of social security programs and resources
- To achieve sustainable solvency and ensure social security programs meet the needs of current and future generations
- To strategically manage and align staff to support SSA's mission today and in the years ahead.

The APP is aligned with the ASP and describes the specific levels of performance the Agency is committed to achieve for each of the strategic goals and associated long-term objectives during the current and upcoming fiscal years. IRM activities play a key role in the support of mission performance and the attainment of strategic goals and objectives.

IRM Strategic Plan activities support the objectives of each of the strategic goals. Two of the objectives to help accomplish the service goal are aimed at the disability process, i.e., making the right decision in the disability process as early as possible, and increasing employment for people with disabilities. The third objective is improving service through technology. The Accelerated Electronic Disability initiative is designed to reduce delays inherent in mailing, locating and organizing paper folders. SSA is effectively using technology in this initiative by accelerating its transition to an electronic disability folder.

Two of the objectives for the superior stewardship goal involve increasing the accuracy of earnings records and efficiently managing Agency finances and assets. To those ends, SSA is improving its electronic wage reporting system to enable the

submission of wage reports in a variety of methods, i.e., diskette, bulletin board, Internet, value-added networks and electronic data transfer, and expanding services to wage reporting customers by providing information on processing results, testing capabilities, and customer support. Another initiative, vital to the objective of efficiently managing Agency finances and assets is the Social Security Unified Measurement System (SUMS) and the Managerial Cost Accountability System (MCAS). SUMS focuses on the detailed data needed by managers and employees to track, monitor and forecast critical Agency workloads, while MCAS focuses on critical performance and financial information needed by managers and employees throughout the Agency.

With regard to solvency, the IRM Strategic Plan must maintain flexibility so that both the Enterprise Architecture (EA) and the Human Resources plans can accommodate solvency solutions that will significantly affect IT priorities and resources.

To recruit, develop and retain a high-performing workforce is the objective of the goal to strategically manage and align staff to support SSA's mission. Chapter 7 of this plan describes our efforts to recruit, retain and train SSA's most important asset, its Human Capital. In this vein, the chapter addresses activities pertinent to SSA's IT Human Resources. IRM activities include providing the infrastructure, telecommunications and office automation support needed by all of our employees. Interactive Video Teletraining is used to provide training to SSA's widely dispersed staff. SSA is using the Internet to give employees access to over 250 courses from work or from home. SSA is developing efficient tools such as decision support software and more fully automated case processing systems to support higher productivity per employee.

Social Security is an essential facet of contemporary life, and touches just about every American citizen. One in six Americans receives a Social Security benefit and about 98 percent of all workers are in jobs covered by Social Security. SSA is responsible for administering these successful programs that are of such great benefit to the American people—the Old Age Survivors Insurance (OASI), Disability Insurance (DI) and the Supplemental Security Income (SSI) programs.

SSA efficiently integrates activities across these programs through a single national service delivery structure. This service delivery structure is supported by the Agency's EA that describes and documents the current and desired relationships among business and management processes and IT. The EA is based on the Agency's view of future service delivery, ensures compliance with the broader Federal EA and provides a strategy that will enable SSA to support its future environment. The SSA IRM Strategic Plan documents the Agency's baseline IT architecture and the processes for managing change to that architecture to support the Agency's service delivery goals and strategies.

Pursuant to Federal statutory requirements and directives, SSA has implemented a Systems Security Plan that integrates security into all major information systems investments, defines a security architecture and integrates new security standards and technology into SSA's business processes to protect IT assets from both physical and

cyber security threats. This security architecture is an integral part of the Agency's EA and is consistent with OMB's Federal Enterprise Architecture model.

SSA is playing an important role in the PMA E-government initiative. The Agency was a partner in the Quicksilver task force which was formed with OMB and the President's Management Council to identify E-government projects that can deliver significant performance and productivity gains across government. Of the twenty-four projects selected for development, SSA is the managing partner for one of these, eVital, and a supporting partner for several others. In addition, SSA is expanding electronic service delivery in ways that improve current business processes by increasing opportunities for the public to conduct SSA business and to access information electronically in a private and secure environment. The Agency also has initiatives underway that support the other PMA areas of Improved Financial Management, Budget and Performance Integration, Strategic Management of Human Capital, and Competitive Sourcing.

SSA's IRM strategic planning is influenced by the following legislation and demographic trends.

- By 2006 SSA is committed to fully integrate a new Medicare Prescription Drug process into its processing environment. This new legislation will have a major impact on IT priorities and resources.
- By 2010 SSA's workloads will swell to unprecedented volumes. The most significant factor contributing to this change will be the aging of the baby-boom generation (those persons born in 1946 through 1964).
- Along with the workload increase, the incredible pace of technology change will have a profound impact on both the public's expectations and SSA's abilities to meet those expectations.
- SSA will lose a substantial number of experienced employees by 2010. Over 28,000 SSA employees will be eligible to retire and another 10,000 are expected to leave the Agency for other reasons. This retirement wave will result in a significant loss of institutional knowledge in all Agency components, including SSA's Office of Systems (OS). The OS workforce includes almost 3,000 technical employees who are skilled in a wide variety of computer-related areas. Personnel projections indicate that OS is at the beginning of a retirement wave—43 percent, or 1,235 employees, will reach average retirement age by 2007.

Considering these factors, SSA's IRM strategic planning is focused on the achievement of the following strategic results:

- The EA, IT Human Resources plan and options for the use of IT contractors are adequate to achieve the Agency's strategic goals and objectives and provide the flexibility to support substantial workload growth as well as changes with major impacts on priorities and resources,

such as those associated with new legislation and potential solvency initiatives, in a timely and cost-effective manner.

- The EA supports the fully integrated delivery of government services permitting business to be done using the means of service delivery that the public prefers. These include increased use of electronic service delivery, such as self-help over the Internet, which allows SSA to redirect resources to more labor-intensive workloads.
- Back-up and recovery and continuity of operations capabilities are in place to provide uninterrupted service as the Agency becomes increasingly dependent on automation to provide integrated service delivery.
- IT security and privacy safeguards are in place to keep pace with the movement to an electronic processing environment.

Conclusion

This IRM Strategic Plan will continue to evolve throughout 2004. As this document is being completed, additional challenges have arisen. They include the implementation of the previously mentioned Medicare Prescription Drug Bill just passed by Congress and budget constraints. The IRM Strategic Plan is a framework but also a guiding tool to assist the Agency in making effective decisions regarding the delivery of technology for staff and citizen. We will continue to work throughout 2004 to hone the careful delivery of IT to meet the Agency's strategic goals and objectives and the goals of the Bush Administration.

Chapter 1: Introduction

It is the mission of the Social Security Administration to *advance the economic security of the nation's people through compassionate and vigilant leadership in shaping and managing America's social security programs.*

The Social SecurityAdministration (SSA) is responsible for administering the most successful domestic programs in the nation's history: the Old Age Survivors Insurance (OASI), Disability Insurance (DI) and the Supplemental Security Income (SSI) programs. SSA also provides substantial support to the closely related Medicare and Medicaid programs and more limited, but critical, support to several other important Federal programs. SSA efficiently integrates activities across all these programs through a single national service delivery structure. This service structure is supported by an Agency information technology architecture (ITA) that is based on the Agency strategic goals, the objectives supporting the goals, and performance indicators to measure success.

The SSA Information Resource Management (IRM) Plan documents this baseline information technology architecture and the process for managing change to that architecture. The IRM plan, like the plans before it, will remain a work in progress as SSA continuously attempts to balance the changing service delivery needs of our citizens with rapidly advancing technology and limited fiscal resources.

The audience for this plan is both internal and external to the Agency. It is a management tool for use on a day-to-day basis. It defines plans and strategies for achieving well defined goals and objectives. It also serves as a comprehensive reference for SSA management and external monitoring authorities. As a long range planning tool it provides the context and justification for the ITS budget and ensures that our investments support the Agency's mission and are consistent with the enterprise architecture.

Brief History of Information Technology Planning

- During the 1950s and 1960s, SSA was a consistent leader among users of information technology. However, by the end of the 1970s, SSA's systems were in serious need of an overhaul. Hardware was outmoded and inadequate, lacking the capacity to support many basic program services and software systems required major redesigns.
- In 1982, SSA launched an urgent **Systems Modernization** effort to return the quality of its information systems to earlier levels. Between 1983 and 1986, SSA installed mainframes with increased processing and memory capacities and moved programmatic master files onto direct access storage devices as part of the systems modernization effort. During that same period, SSA

implemented a national telecommunications system enabling field users to access the centrally housed applications and data for the first time.

- The increased processing capacity, the online master files and the national data communications network enabled field personnel to provide faster, more responsive service to the public for high-volume workloads. In addition, these technology improvements established the foundation needed for redesigning the programmatic software and databases for operation in an online environment.
- In January 1988, SSA published its **Agency Strategic Plan**. Titled "2000—A Strategic Plan," this document stated the vision of what SSA's business would be like by the year 2000. The theme of the plan was that SSA should assume a proactive posture to tailor its business processes to its advantage by making maximum use of available technology. SSA has published three new plans since. The Strategic Plan for FY 2003 – 2008 was published in March 2003.
- In June 1990, SSA released **the Interim Systems Plan** in response to a request from the Senate Appropriations Committee for background information to support the FY 1991 ITS budget. The plan was considered "interim" in that a more comprehensive Information Systems Plan would follow.
- **The Information Systems Plan** (ISP) was published annually from 1991 through 1997. The plan supported the Agency goals and objectives articulated in the refreshed Agency Strategic Plan and reflected major systems planning decisions. It described the current systems environment and identified four areas of opportunity that set the general direction of future SSA systems: computing platforms, application software, data management and communications.
- **The Information Technology Architecture Plan** (ITAP) was largely influenced by Clinger-Cohen legislation. It documents SSA's baseline ITA and the processes for managing change to that architecture. It incorporates many of the well-received elements of the ISP and is more contemporary in addressing the influence of the Clinger-Cohen Act on IT planning and management requirements. The ITAP was published in October 2001.
- **The IRM Strategic Plan** is the cornerstone for IT budget planning and management—and has evolved from the ITAP. It continues to document in more detail SSA's ITA and the processes for managing change to that architecture. It emphasizes management of the information resources to accomplish the Agency mission, including human capital, data, hardware and software, capital investments and other related resources. The plan was first published in October 2002. It is published annually.

Regulatory basis

The IRM plan addresses the influence of the Clinger-Cohen Act on IT planning and management requirements. It also addresses the requirements of managing Federal

information resources as expressed in OMB Circular A-130, and the Paperwork Reduction Acts of 1980 and 1995.

Relationship to Other Strategic Planning Documents

President's Management Agenda

"Government likes to begin things— to declare grand new programs and causes. But good beginnings are not the measure of success. What matters in the end is completion. Performance. Results. Not just making promises, but making good on promises. In my Administration, that will be the standard from the farthest regional office of government to the highest office in the land."—George W. Bush

Moving to improve management practices and performance across the Federal government the President has issued an agenda of high priority initiatives which reflect the Administration's commitment to achieve immediate, concrete and measurable results. The President's Management Agenda includes 5 initiatives that are mutually reinforcing and reflect a coherent and coordinated plan. The initiatives are:

- Expanded E-government;
- Strategic Management of Human Capital;
- Improved Financial Management.
- Budget and Performance Integration; and
- Competitive Sourcing.

SSA is aggressively acting on these initiatives in the context of SSA's mission. These activities are integral to the Agency Strategic Plan and are a major factor in this IRM Plan. The strategic objective to improve service through technology is a focal point for managing information resources activities.

SSA was a partner in the Quicksilver taskforce which was formed with OMB and the President's Management Council to identify E-government projects that can deliver significant performance and productivity gains across government. Twenty-four projects were selected for initial development. SSA is the managing partner for one of these, eVital, and a supporting partner for several others. In addition, SSA is expanding electronic service delivery in ways that improve current business processes by increasing opportunities for the public to conduct SSA business and to access information electronically in a private and secure environment. A description of the Quick Silver initiatives in which SSA is participating can be found in Chapter 5.

SSA remains committed to maintaining a highly skilled and motivated workforce through continued training, staff development and an effective work environment. Chapter 9 of this plan describes SSA's IT Human Resources Management strategy

including a support services and outsourcing strategy that supports the corresponding items of the President's Management Agenda.

SSA has undertaken initiatives that support Improved Financial Management. These major initiatives include Financial Accounting System Replacement and Access to Financial Institutions.

The major initiative Managerial Cost Accountability System (MCAS) provides an essential means of accomplishing the President's Initiative regarding Budget and Performance Integration. A description of MCAS and the other major initiatives mentioned above can be found in chapter 5 of this plan.

Agency Strategic Plan (ASP)

SSA's Strategic Plan is the blueprint for responding to the short and long-term challenges the Agency faces. It is the driving force for the Agency Performance Plan, the IRM Strategic Plan and other lower-level plans. See the section following for more discussion concerning the planning framework.

The ASP articulates the Agency's mission, values, and four strategic goals that define in outcome terms how the Agency will carry out its mission. Supporting each goal are objectives that describe issues, means and strategies which are key to achieving each goal. The goals and their subordinate objectives are:

- **To deliver high quality, citizen-centered service;**
  - Make the right decision in the disability process as early as possible,
  - Increase employment for people with disabilities, and
  - Improve service through technology.
- **To ensure superior stewardship of Social Security programs and resources;**
  - Prevent fraudulent and improper payments and improve debt management,
  - Strengthen the integrity of the SSN,
  - Increase the accuracy of earnings records, and
  - Efficiently manage Agency finances and assets and effectively link resources to performance outcomes.
- **To achieve sustainable solvency and ensure Social Security programs meet the needs of current and future generations;**
  - Through education and research efforts, support reforms to ensure sustainable solvency and more responsive Retirement and Disability programs.
- **To strategically manage and align staff to support SSA's mission.**
  - Recruit, develop and retain a high-performing workforce.

Establishing an agency strategic plan, goals and objectives is prescribed by the Government Performance and Results Act. The ASP directly impacts information resource management planning decisions and activities.

Information Planning and Management Framework

The figure below illustrates how IT planning and management requirements are aligned at the strategic level.

SSA's Unified Planning System provides a comprehensive, cohesive approach to Agency planning. Under the planning system, SSA establishes linkages to ensure that resources needed to support planned activities are identified and ultimately reflected in the Agency budget and acquisition plan.

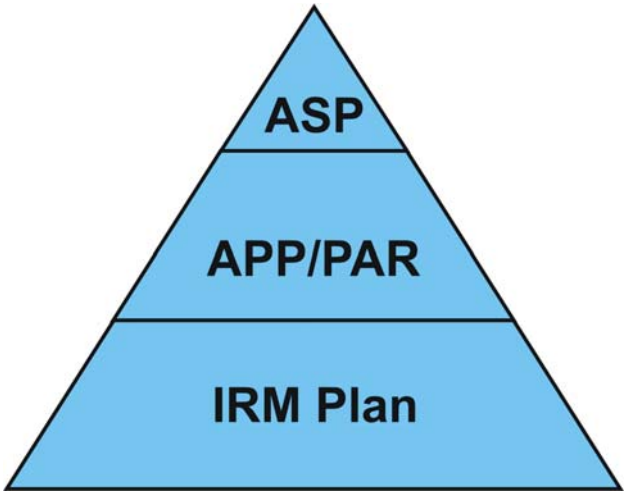


Figure 1: Alignment of Strategy/Planning Documents

At the pinnacle of the triangle, the ASP drives all lower level planning, including the objectives, priorities and constraints for Agency managers to adopt in constructing more detailed support plans. The Commissioner provides the direction for the ASP. In keeping with the requirements specified in the Government Performance and Results Act (GPRA), SSA's most recent strategic plan was published in March 2003. It is for Fiscal Years 2003–2008 and describes strategies for delivering results by integrating performance with a multi-year service delivery plan. Strategic goals and objectives, strategies and expected long-term outcomes associated with each strategic goal.

SSA's *Annual Performance Plan* (APP) reiterates the Agency's goals and objectives expressed in the ASP and focuses on the performance targets and the means and strategies for achieving them. Performance targets or output/outcome measures are used to assess success in meeting a performance goal or initiative. The performance plan is integrated with the annual budget submission and provided to OMB and to Congress.

The *Performance and Accountability Report*, published shortly after the close of the fiscal year, shows how SSA has performed in administering its programs during the past year.

The *IRM Strategic Plan* describes how IRM activities help to accomplish the Agency's mission and realize SSA's strategic goals and objectives. It also supports the President's Management Agenda.The plan ensures that IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management and program decisions. The IRM Strategic Plan is driven by the ASP and the APP. The IRM Strategic Plan is a key component in SSA's information technology capital planning and investment control process that is used for the ongoing identification, selection, control and evaluation of investments in information resources. The plan also presents SSA's Enterprise Architecture that describes and documents both the current and desired relationships among business and management processes and IT. The Plan documents the Agency's baseline IT architecture and the processes for managing change to that architecture to support the Agency's service delivery goals and strategies. The Chief Information Officer (CIO) is responsible for the IRM Strategic Plan.

At the tactical level, the formulation of *Information Technology (IT) Systems Plan* uses a methodology highlighting sponsor involvement in the identification and prioritization of initiatives that support the ASP. Each Deputy Commissioner prepares an IT plan outlining the Agency goals and objectives they are responsible for meeting. Each IT Plan further documents the specific IT initiatives requiring Systems support. These plans also include the ongoing maintenance and cyclical workloads. As part of the Capital Planning and Investment Control (CPIC) process, the IT Plans are consolidated and reviewed and approved by the Information Technology Advisory Board (ITAB) prior to the beginning of the fiscal year. The IT Plan becomes the blueprint for the developmental, cyclical and maintenance activity within the Office of Systems.

Governance

On a quarterly basis, the Executive-level ITAB reviews the progress of each IT Plan and the capital investments it has approved. Major investments are assessed at key decision points to ensure they are well founded, are achieved within the approved cost and schedule, and provide expected benefits such as the return on investment. They may be redirected or terminated when necessary. These activities are key to SSA's capital investment and control process.

Use of the IRM Plan

This IRM Plan is a management tool for use on a day-to-day basis. Not only does it serve as a comprehensive reference, it ensures that our investments support the Agency's mission and that they are consistent with the Enterprise Architecture (EA). Target architectures will be modified to incorporate new ideas and technologies if they are compatible with the target architecture. If they are not compatible and new

ideas or technologies have undeniable merit, then SSA will make changes to the architecture if appropriate. The IRM Plan will be updated annually to document major management and investment planning decisions.

Chapter 2: IRM Strategic Goals and Objectives

IRM Objectives/Systems Management Objectives

SSA's IRM Strategic Plan defines strategies for achieving a variety of systems management objectives:

- Support the President's Management Agenda;
- Support the SSA's mission, goals and objectives;
- Deliver high quality, citizen-centered service;
- Secure data and IT resources;
- Operate and maintain IT infrastructure;
- Provide future IT infrastructure;
- Maintain and enhance existing applications;
- Build and/or acquire new applications;
- Provide operational support for IT customers;
- Support end-user development;
- Manage and nurture IT personnel; and
- Actively support inter-governmental information sharing.

Planning Assumptions

The following planning assumptions, some of which are beyond the direct control of SSA, are factors that influence Systems plans.

- By 2006 SSA is committed to fully integrate the new Medicare Prescription Drug subsidy eligibility process as required by Public Law 108-173, the Medicare Prescription Drug Improvement and Modernization Act of 2003 into its processing environment. This new legislation will have a major impact on IT priorities and resources.
- By 2010 SSA's workloads will swell to unprecedented volumes. The most significant factor contributing to this change will be the aging of the baby-boom generation (those born in 1946 through 1964).
- Along with the workload increase, the incredible pace of technology change will have a profound impact on both the public's expectations and SSA's abilities to meet those expectations.

- SSA will lose a substantial number of experienced employees by 2010. Over 28,000 SSA employees will be eligible to retire and another 10,000 are expected to leave the Agency for other reasons. This retirement wave will result in a significant loss of institutional knowledge.

Systems Guiding Principles

The guiding principles for systems planning are:

- Improved citizen-centered service and overall operational efficiency and effectiveness drive all efforts for the development, modification and redesign of systems.
- Systems initiatives are undertaken to achieve a future vision and to be compatible with our Enterprise Architecture.
- Initiatives are designed to be implemented incrementally.
- SSA is refining its integrated architecture to more fully support all of its programmatic, administrative and management information systems.
- Sound business principles are applied to all systems proposals and investments.
- Ongoing employee training provides skills to enable the workforce to perform effectively using new technologies.
- Technology upgrades are balanced with human considerations.
- Capacity needs are satisfied through accurate forecasting and timely and orderly acquisitions related to planned objectives.
- SSA will continue to develop systems which ensure superior stewardship of SSA programs and resources.
- SSA will provide Information Systems Security for sensitive Agency data.
- SSA will conduct privacy impact assessments for all new IT investments and online information collection systems.

SSA Organizational Chart

The Social Security Administration (SSA) is headed by a Commissioner and has a staff of approximately 65,000 employees. The Agency's central office is located in Baltimore, Maryland.

The Office of the Commissioner (OC) provides executive leadership to SSA and exercises general supervision over its major components. It is directly responsible for all programs administered by SSA, and for State-administered programs directed by SSA.

The Office of the Chief Information Officer (OCIO) develops the Information Resource Management Plan and defines the Agency's Information Technology (IT) vision and strategy. The Office shapes the application of technology in support of the

Agency's Strategic Plan including the Information Technology Architecture that outlines the long term Strategic Architecture and Systems Plans for the Agency and includes Agency IT Capital Planning.

The Agency achieves its core business goals through a joint partnership between SSA's Office of Systems and the other SSA components. These components include: Communications; Disability and Income Security Programs; Finance, Assessment and Management; Human Resources; Legislation and Congressional Affairs; Operations; and Policy. The field organization, which is decentralized to provide services at the local level, includes a network of 10 Regional Offices overseeing 1338 field offices, 138 hearings offices, 36 teleservice centers, 7 processing centers and 1 data operations center.

Social Security's organizational structure is designed to provide timely, accurate and responsive service to the American public. All components within SSA's Central Office provide critical support to the field office structure, including uniform policy development, procedures, information technology, administrative functions and much more. By integrating support services for all of the Agency's programs, we enhance efficiency, avoid duplication of effort and increase opportunities to provide one-stop service to the public.

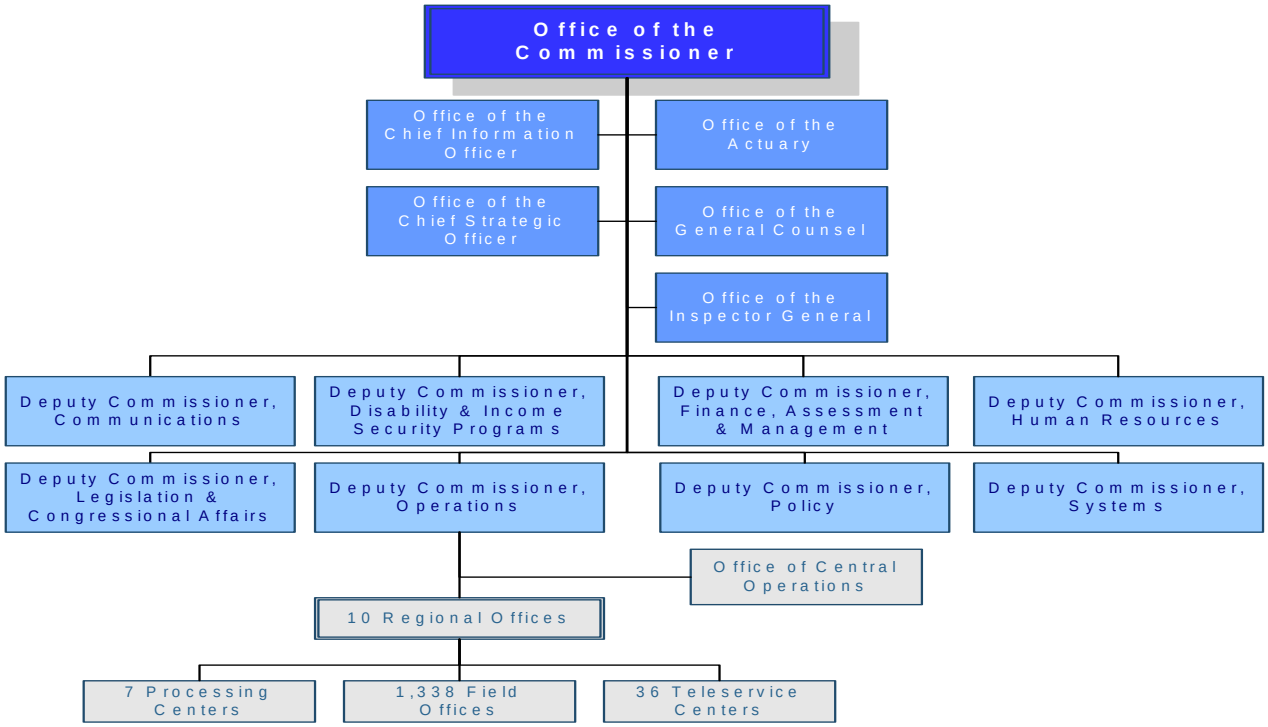


Figure 2: SSA's Organizational Chart

Chapter 3: SSA Enterprise Architecture Framework

The Enterprise Architecture (EA) Framework provides the over-arching guide for defining SSA's existing and planned architectures. The EA Framework identifies the strategic information assets that define the SSA business processes; the information necessary to operate these processes; the technologies needed to support business operations; and a transition process for implementing new technologies in response to the changing needs of the Agency.

After two years of operating experience, the EA Framework remains a work-in-progress. The initial version of the Framework was recently refined to incorporate the lessons the Agency learned by documenting the current IT infrastructure and the development of the target enterprise architecture. The Framework continues to serve as a guidepost in our current efforts to restructure the SSA system development life cycle (SDLC) and related information resource management (IRM) procedures. As the EA Framework continues to be used in day-to-day operations, it will undoubtedly require some degree of further refinement. This description will be updated periodically to accurately reflect the architectural products that are being used to help manage the Agency's IRM assets.

Conformance to Federal Standards and Guidelines

The EA Framework was developed following the directions and using the guidance provided by the following Federal publications:

- Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources;
- National Institute of Standards and Technology (NIST) Enterprise Architecture Model;
- The Federal Enterprise Architecture Framework as defined by the Chief Information Officer's Council (Architecture and Infrastructure Committee); and
- The Chief Information Officer's Council's *A Practical Guide to Federal Enterprise Architecture, Version 1*.

Conformance to Federal standards and guidelines will be maintained as the EA Framework is refined based on operational experience.

Purpose of the EA Framework

The EA Framework provides a structure for organizing the products that describe existing and future SSA architectures. It identifies the documentation products that are the key architectural definitions created by the systems development life cycle as well as any retrospective documentation that is required for existing IT architectures. The framework does not include the actual documentation products; it establishes an organizing structure, with placeholders for the continued population of the EA.

The creation and population of the EA Framework enables SSA to work in partnership with other Federal Agencies to promote interoperability and information sharing. The populated framework also provides several benefits within SSA, including:

- Organization of existing architectural models, life cycle documentation artifacts, and other information assets within an enterprise-wide structure;
- Development of retrospective documentation for selected classes of existing architecture definitions considered essential for effective systems management;
- Creation of enterprise-level target architecture definitions that clearly support SSA's mission objectives and strategic business plans;
- Use of enterprise-level target architecture definitions to plan and guide the acquisition of information technologies;
- Development of transition architectures to guide incremental implementation planning and effective change management;
- Definition of the specific architectural models and other key life cycle products that will be produced for each future implementation segment; and
- Development of proven architectural reference models to guide the design of future automated systems.

Tailoring the Framework Content

SSA's EA Framework is based on the CIO Council's Enterprise Architecture Planning Model and the Level IV Framework depicted in the Council's publication Federal Enterprise Architecture Framework, Version 1.1. For reference purposes, the Planning Model and Level IV Framework are reproduced as Figure 3 and Table 1 respectively.

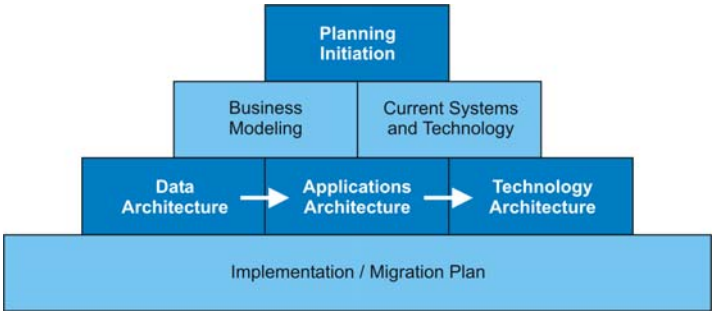


Figure 3: Federal Enterprise Architecture Planning Model

Perspectives	Applications Architecture (activities = how)	Data Architecture (entities = what)	Technology Architecture (locations = where)
Planner's View Objectives / Scope	List of Business Processes	List of Business Objects	List of Business Locations
Owner's View Enterprise Model	Business Process Model	Semantic Model (E/R Model)	Business Logistics System
Designer's View Information Systems Model	Application Architecture	Logical Data Model	System Geographic Deployment Architecture
Builder's View Technology Model	System Design	Physical Data Model	Technology Architecture
Subcontractor's View Detailed Specifications	Programs 'Supporting Software Components'	Data Definitions 'Library or Encyclopedia'	Network Architecture

Table 1: Federal Enterprise Architecture Framework, Level IV

As recommended by the CIO Council, we tailored the Federal framework to accurately reflect the methods and terminology used within SSA to describe existing and planned architectures. In tailoring the framework, we also decided which of the Federal framework cells we should make explicit within our framework (i.e., include

as a discrete model or other documentation product) and which ones we should define as implicit (i.e. omit or combine within another model). We made these decisions considering the potential benefits and risks of implicit framework cells:

- The potential benefits of explicit definitions for the full-range of architecture definitions for *existing* SSA business processes and systems do not justify the cost of retrospective development and maintenance of all SDLC documentation products. That is, some life cycle products are important during the system development process but are of little continuing use once the target system has been successfully installed.
- There are, however, certain types of architecture definitions for existing processes/systems (such as functional requirements and system design documents) where it does make good business sense to organize and maintain existing architecture definitions and provide for retrospective documentation in the case of missing or out-of-date definitions.
- For *target* architectures, development of the full-range of models, as suggested by the Federal Framework, is appropriate.
- The EA Framework should clearly define which architectural products will be made explicit for both existing and target architectures. Refer to the CIO Council's publication *Federal Enterprise Architecture Framework, Version 1.1* dated September 1999 for a complete explanation of explicit versus implicit framework cells.
- There are certain classes of architectural models that should be defined at the *enterprise* level and others that are best approached on a project or *implementation segment* basis.
- The EA Framework should clearly indicate which architectural products would be defined at the enterprise level and which ones are to be created on a project-by-project basis.

Framework Structure

Table 2 below depicts the EA Framework. The framework is structured as follows:

- As with the Federal Enterprise Architecture Framework, three general categories of architectures are defined: *data, applications, and infrastructure* architectures. (NOTE: To simplify the framework, business process models are included in the application grouping.) Placeholders for these categories are defined within the three vertical columns of the framework (labeled A, B and C). The cells formed by numbered rows contain descriptions of the various EA architectural definitions.
- The alpha-numeric labeling of the framework cells provides a familiar (spreadsheet style) way of quickly identifying a specific EA model type in the exchange of correspondence and day-to-day working sessions.
- The upper segment of the framework (rows 1-4) establishes placeholders for architecture representations that describe *existing* architectures.

- Two categories of existing architectures are defined; those that are

			A	B	C
Documentation of Existing Architectures :			**Data**	**Business Processes & Applications**	**Technology Infrastructure**
Enterprise Level	***Owner's View***	1	**A1** **Enterprise Data Model** • Entity - relationship diagrams • Attributed, non-keyed	**B1** **SSA Business Process Model** • High-level context diagrams • Baseline for business planning	**C1** **Technical Reference Model** • Graphic, enterprise-level • Platforms and product classes
	Designer's View	2	**A2** **SSA Data Architecture** • High-level context diagrams • Logical and physical views	**B2** **SSA Application Architecture** • High-level context diagrams • Baseline for future architecture	**C2** **IT Infrastructure Existing Architecture Definition** • Logical & physical diagrams
System (Project) Level	***Owner's View***	3	**A3** **Entity - Relationship Model** • Project-Based E- R Model • Fully attributed, keyed	**B3** **Functional Requirements and Business Rules** • Project FRDs, operations manuals	**C3** **IT Resource Projections** • Accommodate workload growth • CPU, DASD, telecommunications
	Designer's View	4	**A4** **Database Models** • Physical schemata • Tuned for performance	**B4** **Application Architectures** • System- level application design documentation	**C4** **Infrastructure Utilization Data** • Resources used by applications • CPU, DASD, telecommunications
Target Architecture Definitions :			**Data**	**Business Process & Applications**	**Technology Infrastructure**
Enterprise Level	***Planner's View*** ***Owner's View***	5	**ABC5** **SSA Strategic Planning Documents** • SSA Vision	• Strategic Plan 'Mastering the Challenge'	• SSA Performance Plan
	Designer's View	6	**A6** **New Data Requirements** • Additional data required to support target business processes	**B6** **Target Business Process Model** • Future business process description • Contrasted to current (B1 above)	**C6** **Target Deployment Strategy** • Future deployment needed to support target business processes
		7	**A7** **Target Data Architecture** • Future architecture description • Contrasted to current (A2 above)	**B7** **Target Application Architecture** • High-level graphical model • Contrasted to current (B2 above)	**C7** **Target Infrastructure Architecture** • High-level graphical diagrams • Contrasted to current (C1&2 above)
		8	**A8** **Data Transition Architectures** • Multiple iterations • Focused on integration issues	**B8** **Application Transition Architectures** • Multiple iterations • Focused on integration issues	**C8** **Infrastructure Transition Architecture** • Multiple iterations, focused on integration
Future Implementation Segments:			**Data**	**Business Process & Applications**	**Technology Infrastructure**
Project Level	***Owner's View***	9	**A9** **Logical Data Models** • Project-level E-R diagram • Relational tables (iterations)	**B9** **Systems Requirement Specification** • Process flow diagrams • Business rules, etc.	**C9** **Infrastructure Support Reqmts** • Workload / resource projections • Service level agreements
	Designer's View	10	**A10** **Physical Data Models** • Database schema • Tuned for performance	**B10** **System Design Specifications** • Application structure • Program/object specifications	**C10** **System Deployment Architecture** • IT infrastructure models • Infrastructure specifications (as nec)
	Developer's View	11	**A11** **Data Repository Updates** • Data Resource Management System	**B11** **Application Software** • Source & object code	**C11** **Infrastructure Configuration** • (System-specific) IT infrastructure

Table 2: SSA Enterprise Information Technical Architecture Framework

documented at the *enterprise* level (rows 1 and 2) and those that are documented at the *project or existing system* level (rows 3 and 4).

- Refer to Table 3 for thumbnail descriptions of the existing architecture definitions that SSA deems necessary for these critical management activities.
- The middle segment of the framework (rows 5-8) establishes placeholders for architecture representations that describe *future (target)* architectures. The bottom segment of the framework (rows 9-11) identifies the architectural products that will be produced for *implementation segments* that will be initiated as SSA transitions from the current to the target enterprise architecture.
- The three cells in line 5 are merged to form a single entry (since these strategic planning documents apply equally to data, applications and infrastructure).

Description of Architecture Definitions

Table 3 provides summary descriptions of each of the architectural products defined by the EA Framework.

Table 3: Descriptions of Models and Other Architectural Products

Current Architecture Definitions

Scope	Data	Business Processes and Applications	Infrastructure
Enterprise Level	**[A1] Enterprise Data Model—**A set of fully attributed, non-keyed entity-relationship (E-R) diagrams identifying the entities about which data are currently collected and stored and the relationships between such entities. The E-R diagrams conform to the standards and conventions of IDEF0 (Integrated Computer Automated Manufacturing Definition). The enterprise data model is being posted to the EA Intranet website.	**[B1] SSA Business Process Model—**A set of enterprise-level, graphical models of the SSA programmatic, administrative and MI business processes. These enterprise-level models provide: • Context for the more detailed definitions of current business processes (described in Cell B3 below). • Baseline definitions for the future process architecture (see Cell B6 below). Enterprise-level process models will be developed using the essential elements of IDEF0 (Integrated Computer Automated Manufacturing Definition). Process models will be posted to the EA Intranet website.	**[C1] Technical Reference Model—**A set of diagrams that identify the processing platform categories currently in use and the enterprise standard commercial off-the-shelf (COTS) products that are to be used for the development of target applications. Such products will be identified within functional classifications. The reference model will be enterprise-wide in its scope. It's basic structure and content will be based on the suggestions contained in the CIO Council document 'A Practical Guide to Federal Enterprise Architecture'. Upon completion, the model will be posted to the EA Intranet website and included in future publications of the IRM Strategic Plan.
Enterprise Level **Designer's View**	**[A2] SSA Data Architecture Model—**An enterprise-level, graphical model of the existing SSA data architecture, providing: • Context for the more detailed descriptions of current SSA data structures (described in Cells A3 and A4 below). • Baseline definition for developing a future data architecture (see Cell B6 below). The SSA Data Architecture Model has been posted to the EA Intranet website and included in future publications of the SSA IRM Strategic Plan.	**[B2] SSA Application Architecture Model—**An enterprise-level, graphical model of the SSA application architecture, providing: • Context for the more detailed descriptions of current application systems (described in Cell B4 below). • Baseline definitions for the future application architecture (see Cell B7 below). Enterprise-level process models will be developed using the essential elements of IDEF0. Process models will be posted to the EA Intranet website and included in future publications of the SSA IRM Strategic Plan.	**[C2] IT Infrastructure Existing Architecture Definition—**A comprehensive set of information assets that document the existing SSA information technology (IT) infrastructure including hardware, non-applications software, and infrastructure support services. The architecture definition consists of logical and physical diagrams for 15 infrastructure 'service areas' along with supporting narrative descriptions and a database of detailed component information including make, model, version of the IT hardware and software infrastructure products currently used by SSA. All such infrastructure information is accessible via the SSA Intranet.

— The following architectural models are defined at the project / system level —			
System / Project Level	**[A3] Entity-Relationship Models—**A set of models that identify the actual data objects that are used by existing programmatic, administrative, and MI systems. These models are represented as E-R diagrams. They illustrate the data and data relationships that guided the development of project level systems requirements and business rules.	**[B3] Functional Requirements and Business Rules—**The combination of policy instructions, operating manuals, and project level documentation products that provide functional requirements and business rules for existing programmatic, administrative and MI systems.	**[C3] IT Resource Projections—** Periodic projections of the IT infrastructure resources required for use by production systems (to accommodate new requirements and workload growth).
System / Project Level	**[A4] Database Models—**A set of models that define the physical database(s) used by production applications. Such models include: • Relational tables (application sub-schema) and the physical storage schema for systems developed using a relational database management system (RDBMS). • File and record specifications for systems using a non-relational DBMS or file management system. Logical database models created during the development life cycle may be also be maintained for selected application systems.	**[B4] Application Architectures** The systems design descriptions that document the general design of existing programmatic, administrative and MI application systems. At a minimum, such documentation will describe the geographic hardware—software deployment structure, the software infrastructure products utilized, major application components and their functions, data storage methods, and macro-level data flows. Instructions for documenting existing applications are being developed for the EA website.	**[C4] Infrastructure Utilization Data—**Management information data showing the amount of IT infrastructure resources (CPU, disk storage, telecommunications bandwidth, etc.) used by the various programmatic, administrative and MI systems.

Future (Target) Architecture Definitions

Scope	Data	Business Processes and Applications	Infrastructure
Enterprise Level **Planner and Owner's Views**	**[ABC5] SSA Strategic Planning Documents—**A set of documents that define SSA's mission and the strategic plans for meeting future mission goals and objectives: •**Agency Strategic Plan —**SSA's strategic business plan that defines the Agency's mission, goals and objectives. • **Annual Performance Plan**—The plan that establishes measurable objectives and specific metrics for achieving the business goals defined by the Agency Strategic Plan.		

Future (Target) Architecture Definitions

Scope	Data	Business Processes and Applications	Infrastructure
Enterprise Level **Planner and Designer's Views**	**[A6] New Data Requirements—**A strategic planning document that broadly identifies any new major data subjects that will be required to support the target business process (described in Cell B6). Envisioned changes in the media used to store data (such as the conversion from paper to audio or video) will also be identified. Summary descriptions of these new data requirements will be included in future publications of the SSA IRM Strategic Plan. *Note: This document will be produced only if required by the target business process.*	**[B6] SSA Target Business Process Model—**An enterprise-level, strategic model of the new and/or revised business processes that will be needed to achieve the mission goals defined by the SSA Strategic Plan. This future process model will be structured to highlight the envisioned changes to the current process model (described in Cell B2 above). The Target Application Architecture will be posted to the EA website and included in future publications of the SSA IRM Strategic Plan.	**[C6] Target Deployment Strategy—**A strategic planning document that broadly identifies any new physical locations for the installation of IT computing equipment to support the target business process (described in Cell B6). A summary description of the target deployment strategy will be included in future publications of the SSA IRM Strategic Plan. *Note: This document will be produced only if required by the target business process.*
Enterprise Level **Planner and Designer's Views**	**[A7] SSA Target Data Architecture—**An enterprise-level, strategic model of the data structures that will be needed to achieve the business objectives defined by the SSA Strategic Plan and support the Target Application Architecture (described in Cell B6). The Target Data Model will be posted to the EA website and included in future publications of the SSA IRM Strategic Plan.	**[B7] SSA Target Application Architecture—**An enterprise-level, strategic model of the application structure that will be needed to support the target business process model described in Cell B6 above. This future architecture model will be structured to highlight the envisioned changes to the current architecture model (described in Cell B1 above). The Target Business Process Model will be posted to the EA website and included in future publications of the SSA IRM Strategic Plan.	**[C7] SSA Target Infrastructure Architecture—**A set of strategic planning models that define how the SSA IT Infrastructure will need to change to support the future SSA business processes and keep pace with evolving technologies. Target architecture definitions will be developed for each of the 15 infrastructure service areas described on page 136. The Target Infrastructure Architecture definitions will be posted to the EA website and included in future publications of the SSA IRM Strategic Plan.
Enterprise Level **Designer's View**	**[A8] Data Transition Architectures—**A series of (tactical) architecture definitions that illustrate how the SSA data structures and data management technologies infrastructure will be incrementally changed to support a phased transition from the current to the future (target) data architecture. Transition architecture definitions will be posted to the EA website. Refer to Chapter 6 of this document for additional information about transition planning.	**[B8] Application Transition Architectures—**A series of (tactical) architecture definitions that illustrate how the SSA application structures will be incrementally changed to support a phased transition from the current to the future (target) application architecture. Transition architecture definitions will be posted to the EA website. Refer to Chapter 6 of this document for additional information about transition planning.	**[C8] IT Infrastructure Transition Architectures—**A series of (tactical) architecture definitions that illustrate how the SSA infrastructure will be incrementally changed to support a phased transition from the current to the future (target) infrastructure architecture. Transition architecture definitions will be posted to the EA website. Refer to Chapter 6 of this document for additional information about transition planning.

Future Implementation Segments

Scope	Data	Business Processes and Applications	Infrastructure
System / Project Level **Owner and Designer's Views**	**[A9] Logical Data Models—**A related set of logical representation of the objects of the system or project about which information is to be recorded (in either automated or non-automated form) including one or more of the following: • Fully attributed, keyed, entity-relationship (E-R) diagram • Create, read, update, delete (CRUD) table mapping data subjects to business process functions • Diagrams illustrating the application developer's view of the relational database tables and/or other types of data records to be used by the target application.	**[B9] System Requirements Specification—**A definition of system functions expressed in logical terms. The system requirements specification defines 'what' functions are to be performed by the automated system. It is typically refined via an iterative process that analyzes functional requirements in relationship to various system design alternatives. Such specifications will typically identify the system inputs and outputs along with logical representations of the functions and/or algorithms to be performed by the target application.	**[C9] Infrastructure Support Requirements—**Documented projections of the type and amount of IT infrastructure support required to develop, test, install and operate the target implementation segment. Such projections will typically include CPU, direct access storage, communications bandwidth, and any new technologies not currently identified by the Technical Reference Model. The projections (that will be used for performance simulations and infrastructure planning) will be refined over the development life cycle.
System / Project Level **Designer's View**	**[A10] Physical Data Model—**A technology constrained, physical representation of the objects of the system or project. The representation style of this model will depend on the technology chosen for implementation: • If a relational technology were chosen, this would be a model of the table structure(s) for the physical database(s) that will support the target application. • In an object-oriented notation, this would be a class-hierarchy/association style model. • For implementations using other SSA-specific data storage methods, the models will be in the form of hierarchical or network file and record specifications.	**[B10] System Design Specification—**At an enterprise-level of abstraction, the system design specification is a structure chart with associated information describing the nature, function, and interrelationships of the component parts of the specified application or application system. The design specification describes 'how' the target functional requirements will be satisfied, including: • Geographic system structure • System inputs, outputs • Data flows • Software deployment structure • Target languages, protocols • Interface specifications • System security solution	**[C10] System Deployment Architecture—**The physical depiction of the IT infrastructure that will be used to support the system or project under development. The deployment architecture will specify the actual hardware components, operating system(s), middle-ware, and other infrastructure software what will be used by the target application. The deployment architecture can be documented separately or as part of the System Design Specification.
System / Project Level **Developer's View**	**[A11] Data Repository Updates—**The definition of all the data objects specified by the physical data model for the target system. Definitions for newly defined data objects shall be recorded in the SSA DRMS or another automated data repository that can be accessed via the DRMS.	**[B11] Application Software—**The custom developed and/or COTS applications defined by the system design specification. Includes source code (for custom developed software) and object code, as well as other application documentation products; e.g., • program/module/object specifications • test plans, test results • configuration management release authorization • operating instructions, user	**[C11] Infrastructure Configuration—**The enterprise level IT infrastructure architecture documented in the EA Intranet website will be updated to incorporate any newly installed infrastructure components, including hardware, operating system(s), middle-ware, or other infrastructure software. New infrastructure components can be installed to support a single target application system, a collection of new applications, or as a periodic technology upgrade.

Chapter 4: IT Security Strategy

Overview

SSA has had a comprehensive and complex information systems security program in effect for many years. The program undergoes constant evaluation and modification to effectively protect SSA data and other ITS resources. SSA's systems consist of sensitive but unclassified (SBU) data comprising some of the largest electronic files in any Federal agency. The Agency has instituted a security program which is comprehensive and far-reaching based on sound management principals and governing directives. For example, the IT security program is integrated into the system development life cycle from initiation statement through development, testing and validation and post-implementation testing. In addition, SSA has implemented policies, management controls and safeguards at the Agency level to protect the confidentiality, integrity and availability of the data and ITS assets critical to performing SSA's mission.

The Agency has recently designed and implemented a Systems Security Plan that consists of the following elements:

- integrating security into all information system major investments,
- adopting a security architecture, and
- integrating new security standards and technology into SSA's business processes to protect software and hardware from both physical and cyber security threats.

The security architecture documents the policies, management controls and safeguards at the Agency level to protect the confidentiality, integrity and availability of the data and the ITS assets critical to performing SSA's mission. The systems security architecture will act as a framework for adding new capabilities as well as enhancing or replacing existing capabilities. This security Architecture is integrated with the Agency's EA and is consistent with OMB's Federal Enterprise Architecture model.

The SSA IT Systems Security Plan can be found in the appendix of this document.

Security Functions and Responsibilities

SSA has implemented an extensive and comprehensive security infrastructure to fulfill its security responsibilities. SSA's Chief Security Officer (SSACSO), reports directly to the CIO and is responsible for establishing Agency-wide security policies and managing the reporting and monitoring processes to ensure compliance. This is accomplished utilizing a network of security professionals in various components throughout the Agency. Primary among these is The Office of Systems Security Operations Management (OSSOM) in the Office of Financial Policy and Operations

under the Deputy Commissioner for Finance, Assessment and Management. OSSOM coordinates, and manages SSA's information systems security programs. This includes:

- Developing SSA's security program requirements and procedures;
- Implementing governing directives in the area of systems security;
- Administering the Agency access control program;
- Managing an onsite systems review and a comprehensive security compliance and monitoring program;
- Providing educational training and awareness programs to management and employees on systems security operational policies, procedures, and requirements;
- Serving as the operational focal point for day-to-day information system security issues;
- Providing direction to the Agency's systems security officers in other components; and
- Implementing security requirements and executing safeguards for SSA's state information exchange program.

The head of every major SSA component has designated individuals or staffs with primary responsibility for security. At headquarters these individuals are component and/or principal security officers; regionally a center director for security and integrity is in place. The security officers are usually assisted by one or more access control administrators and regional staffs, and have additional security personnel responsible for other security functions. The security personnel work together and with management to ensure that preventative, detective and corrective controls are in place to adequately safeguard SSA's assets.

Statutory Requirements

The Agency complies with many statutory requirements and directives which include:

- Privacy Act of 1974
- Federal Managers' Financial Integrity Act of 1982
- Office of Management and Budget Circulars A-123, A-127 and A-130
- Clinger-Cohen Act
- Presidential Decision Directives
  - Critical Infrastructure Protection (PDD-63)
  - Enduring Constitutional Government and Continuity of Government Operations (PDD-67)
- Federal Information Security Management Act

Strategy for current and strategic planning efforts

As noted earlier, SSA has a comprehensive information systems security program in effect that undergoes constant evaluation and modification to effectively protect SSA data and other ITS resources. Below are some of the strategies implemented to protect SSA's systems.

System Development Life Cycle (SDLC)

The SDLC process applies to all applications and incorporates systems security into the software design and redesign of all major SSA systems. Security involvement begins at the initiation of an application and continues through post-implementation. Additionally, risk assessment is required for all applications throughout the process and is an inherent part of the SDLC. This process ensures that security safeguards are addressed at every stage of the life cycle process. Security personnel from all components involved with developing a specific system are consulted at each stage of systems development. They are offered an opportunity to provide input to incorporate security improvements before development proceeds to the next stage of the life cycle. This process ensures security functions are developed and tested along with all other system functionality. When validation is complete the system is certified and released to production. Re-certification is performed periodically to ensure the system's applications and security functions still meet the intended objectives.

Secure Communications & Authentication

SSA is committed to finding and deploying an Agency solution to securing e-mail communications and encrypting data transmissions for those business operations where it is prudent to do so. This effort is critical to SSA's missions because of the inter-Governmental exchange of sensitive information and data. Executives and security personnel are currently participating in a pilot using secure e-mail communications and encrypted data transmissions. Participation in this pilot is limited to a small number of personnel for a specific purpose. This and other product pilots are being run to determine a viable Agency solution.

Single sign-on and supplemental authentication devices are being examined to facilitate SSA's varied business processes. Supplemental authentication devices being considered are biometrics and SmartCards, PKI, tokens or a combination.

Agency objectives include interoperability with computing platforms, possible elimination of user maintained passwords, improvements in user account management, improved authentication controls and strengthened security for mobile users.

While growth of SSANet has benefited the Agency's overall mission, new risks from outside attacks to the enterprise become evident as the system is opened up. The more sensitive web-based enterprise applications are particularly vulnerable if not protected sufficiently. The first line of defense in mitigating these vulnerabilities is

access management technology. Firewalls, encryption, VPN and PKI complement access management to strengthen the environment.

SmartCards

The SmartCard can be used as an identity card, allowing a number of security features, including biometrics, to authenticate identification. Card personalization may include a picture and personal data including name, agency and other basic information. It is possible to include PKI certificates on the card. SSA has a draft Certificate Policy document and is piloting the role of Certificate Authority. As evaluation proceeds, expansion designating local registration authorities will be considered. Consistency and interoperability with the Federal Bridge Certification Authority effort is being monitored.

SSA has replaced the first generation remote access technology, Remote LAN Node, with the new VPN technology. The VPN allows remote users to securely connect to a private network via the Internet or an IP (Internet Protocol) backbone, while providing optimum security to the SSA Network. The SmartCard can provide additional encryption and authentication technologies. The combined technology of a digital certificate on the card and a Personal Identification Number (PIN)/Password allows authentication of the individual requesting access. SSA now requires all remote access clients to use SmartCards.

The Agency is also participating in the Federal Identity Credentialing Committee which is co-sponsored by OMB and GSA. The committee is tasked to enable SmartCard credentials to all civilian federal employees by the end of FY 2005. A single authentication card for both physical and logical access would be issued to each employee. The policy definition and technical requirements for the SmartCard and the PKI digital certificates are being developed.

Biometrics

SSA is currently reviewing, testing and evaluating the use of biometrics in combination with the SmartCard technology. Biometrics involves the use of a unique biological feature used to verify the identity of an individual through automated means. The biological feature may be based on a physiological or behavioral characteristic. The biometrics available under the Smart Identification Card includes Fingerprint Scan, Hand Geometry, Facial Recognition, Iris Scan and Voice recognition. SSA is currently testing the Fingerprint Scan biometric option, and will evaluate and test other biometrics solutions before determining if biometrics is a viable option to employ at SSA.

Sensitive Systems Security Plans

To comply with the provisions of the E-Gov Act of 2002 and the Federal Information Security Management Act, the Agency has established Sensitive Systems Security Plans for all of its systems identified as meeting the definition of a sensitive system under the Act. The systems managers are responsible for developing their plans and ensuring that they comply with the specific guidance in National Institute of Standards and Technology (NIST) Special Publication 800-18, Guide for Developing

Security Plans for Information Technology Systems. The Sensitive Systems Security Plans provide an overview of the security requirements of the system and describe how management has provided both adequate and cost-effective safeguards and controls to meet the NIST requirements. For example, sensitive systems are assigned sensitivity levels, are tested and certified prior to going into service and are certified annually thereafter.

Access Controls

Computer security at SSA involves multiple processing platforms. All users accessing SSA's computing platform are subject to SSA's rules for users and managers of SSA's automated information resources. Each user is required to have a personal identification number and password to access systems which are generated from and registered in the TOP SECRET access and control mechanism. The TOP SECRET software controls access to all of SSA's critical and sensitive mainframe computer applications. TOP SECRET contains three features that control access to SSA systems; a unique personal identification number, the individual's password, and an individual's profile. The profile is one of the primary access control mechanisms used by TOP SECRET. Most profiles are developed for a specific job position (positional profile) and contain a unique mix of transactions needed by that position for data entry purposes. Authorized users are granted access based on the principle of "least privilege" only after they have had their requests for access reviewed and approved by both their management and the appropriate security personnel. This provides the first line of defense to prevent unauthorized access to SSA systems and/or data by employees or outsiders.

Audit Trail System

SSA implements audit trails for all SSA applications which process critical data. Audit trail systems are effective tools that the SSA Regional Security Officers and staff in the Center for Security and Integrity, the primary users of the Audit Trail System, use to monitor data entry and to ensure that the integrity of SSA systems is maintained. Only authorized users are allowed access to the audit trail system. Audit trail systems provide the information necessary to detect, investigate and support prosecution of individuals suspected of fraud, waste or abuse. The use of audit trails provides assurance that SSA is living up to its responsibility to protect information and processes that are critical to all Americans. The Audit Trail System has four approved uses. It can be used to obtain information about transactions:

- of an employee suspected of systems abuse or fraud,
- of a suspect claim, application or action,
- of a selected office in support of a regional office integrity review function, or
- that are suspicious types of actions.

Critical Infrastructure Protection

Contingency planning and disaster recovery are the processes that are used to minimize the impact of situations that affect the availability and reliability of

computer services. These processes are consistent with Presidential Decision Directives (PDD) 63 and 67.

PDD 63 calls for a national level effort to assure the security of increasingly vulnerable and interconnected infrastructures, and provides for a protection plan for national assets from both physical and cyber attack. The national initiative is supported by the Critical Infrastructure Assurance Office, and the SSA effort is supported by our agency-wide Critical Infrastructure Protection (CIP) Workgroup.

PDD 67 requires a continuity of operations plan. SSA has developed a Continuity of Operations Plan (COOP) to ensure that critical functions are maintained. SSA has plans in effect for systems operations that are critical to meeting the Agency's mission, e.g., plans exist to keep critical system functions in operation during a NCC emergency lasting for several hours to several days, as well as plans for long term solutions.

SSA developed a CIP Plan (CIPP) outlining a comprehensive Agency approach to address physical security, continuity of operations and information systems security. The CIPP outlines the milestones and timeline to: identify critical assets and address vulnerabilities, detect attacks and unauthorized intrusions, develop law enforcement liaisons, share attacks and warnings, create capabilities for response and recovery, train, recruit and provide employee security awareness, and secure appropriations in support of the programs.

Intrusion Protection Team

The Agency's Intrusion Protection Team (IPT) is a combination of contracted penetration testing specialists and Agency employees whose mission is to assist in the protection of SSA's enterprise architecture by anticipating and responding to potential systems threats and vulnerabilities, and acting in an assessment and advisory capacity. Specifically, the IPT protects SSA systems by:

- Detecting unauthorized intrusions into the network;
- Conducting risk assessments and issuing vulnerability assessment reports;
- Implementing safeguards to overcome hacker tools;
- Researching security advisories issued by Federal and private entities; and
- Responding to incidents by reporting them, evaluating their seriousness, controlling damage, notifying users, and resolving similar future threats.

In addition to the IPT activities, SSA has contracted with IBM Managed Security Services to provide real-time Intrusion Detection Services (IDS). IDS uses IBM's in-house National Security Administration scanning/reporting product and other off-the-shelf products to identify attempts to gain unauthorized access to network resources.

Security Response Team

SSA established an Agency-wide Security Response Team (SSASRT) to better deal with threats to its electronic systems, to assist employees with handling systems incidents, and to share information concerning common vulnerabilities and threats

with external entities like the Homeland Security's Federal Computer Incident Response Center (FedCIRC). The SSASRT reports to the Executive Staff and is tasked with responding to incidents involving computer systems, Internet and Intranet servers and Local Area Network Servers. Once a security threat is detected, the SSASRT issues advisories to employees on actions to take to combat the attack and shares information regarding the incident with the FedCIRC. The SSASRT created and documented the Agency's incident response procedures.

Chapter 5: IT Performance/Investments

Performance

By the very nature of its mission, SSA has a strong customer focus, and is dedicated to product and service quality. The table below provides a sample of SSA's major workloads, the volume actually processed in FY 2003, and the volume expected to be processed in FY 2004.

MAJOR WORKLOAD	FY 2003	FY 2004
RSDI Claims	5,448,518	5,344,000
RSDI Postentitlement	80,646,738	76,362,600
SSI Claims	2,142,405	2,068,300
SSI Posteligibility	21,307,741	15,755,784
Hearings	571,928	543,200
Social Security Statements	140,656,512	136,000,000
Annual Earnings Items	257,188,087	265,000,000

Table 4: Major SSA Workloads

Underlying the ability to process these large workloads is SSA's capacity to produce application software as promised, on-time and within the resources estimated. The Systems Process Improvement (SPI) project is a major initiative underway that includes establishing a method of measuring how fast and how accurately SSA is able to produce application software. To do this, yearly productivity baselines using function point analysis are being established against which planned projects can be measured. (Function point analysis is a qualitative methodology for measuring the size and complexity of a project in terms of its functionality and estimating its development costs in terms of time and effort.) Once the baseline is established with empirical information, application development time will be more predictable. SSA's users and the pace of technology demand that software be delivered in a short amount of time, and that when it is delivered, it performs accurately, according to the user requirements. With the metrics in place, SSA will have an additional tool to ensure that it has a high performing, productive and efficient systems organization.

Agency Priorities

SSA's priorities are defined by the Agency's four strategic goals, which are shaped by the President's Management Agenda and the Agency Strategic Plan:

- To deliver high quality, citizen-centered service;
- To ensure superior stewardship of Social Security programs and resources;
- To achieve sustainable solvency and ensure Social Security programs meet the needs of current and future generations; and
- To strategically manage and align staff to support SSA's mission.

These goals are presented in the Agency Strategic Plan, along with supporting objectives that add specificity and define what the goals mean for SSA. Target levels of performance have been or are being established for each objective, and the systems to measure success are planned or are already in place. In May 2003, SSA provided Congress with the Agency's FY 2004 Annual Performance Plan, which outlined the measures used to meet the new strategic goals shown above. SSA's Annual Performance and Accountability Report is published shortly after the close of the fiscal year. The Performance and Accountability Report, reflecting the performance of FY 2003, was published in November 2003.

E-Government

"Effective implementation of E-Government is important in making Government more responsive and cost-effective." — George W. Bush

E-Government has changed the way that government operates and the way that citizens relate to government. Americans are taking advantage of E-Government services offered to them. A recent study conducted by Hart-Teeter on behalf of the Council for Excellence in Government shows that half of all Americans and three quarters of American Internet users already have used a government website to find information or conduct a transaction.

SSA is aggressively acting on the initiative to expand electronic government, one of the elements outlined in the President's Management Agenda. The key goals of this element are to improve IT planning through the budget process and champion citizen-centered electronic government that will result in a major improvement in the value of the federal government to the citizens.

The Agency was a partner in the Quicksilver taskforce which was formed with OMB and the President's Management Council to identify E-Government projects that can deliver significant performance and productivity gains across government. Twenty four projects were selected for initial development. Information on Quicksilver is available at www.egov.gov. SSA is the managing partner for one of these, E-Vital, which is described in the IT Capital Plan Summary later in this chapter. SSA is a supporting partner or participating in 17 of the other efforts that are described below. Each initiative supports one or more of SSA's strategic goals.

E-Authentication—The E-Authentication initiative will provide the trusted and secure infrastructure to support the 24 government-wide E-Government initiatives, eliminating the need for each initiative to develop a redundant solution for the verification of identity and electronic signatures. Common solutions, addressing how identity is established electronically, authentication security, privacy, and electronic signing capabilities, which are an appropriate match to the level of risk and agency business needs will be shared across the E-Government initiatives.

For SSA, this initiative supports the following Strategic Goal: To deliver high-quality, citizen-centered service.

E-Travel—In order to streamline government travel administration, this initiative provides a government wide web-based service that applies world-class travel management practices to consolidate federal travel, minimize cost and produce superior customer satisfaction. The E-Travel Service will be commercially hosted to minimize technology costs to the government and guarantee refreshed functionality. From travel planning and authorization to reimbursement, end-to-end service will leverage administrative, financial and information technology best practices to realize significant cost savings and improved employee productivity.

For SSA, this initiative supports the following Strategic Goals: To deliver high-quality, citizen-centered service; and, To strategically manage and align staff to support SSA's mission.

GovBenefits—This effort provides a single point of access for citizens to locate and determine potential eligibility for government benefits and services. Ultimately it will include state and local government programs in addition to the federal programs it includes now.

For SSA, this initiative supports the following Strategic Goal: To deliver high-quality, citizen-centered service.

Integrated Acquisition—The design of this effort is to create a secure business environment that will facilitate and support cost-effective acquisition of goods and services by agencies, while eliminating inefficiencies in the current acquisition environment.

For SSA, this initiative supports the following Strategic Goals: 1) To deliver high-quality, citizen-centered service and 2) To ensure superior stewardship of Social security programs and resources.

USA Services—This initiative seeks to develop and deploy government wide citizen customer service using industry best practices that will provide citizens with timely, consistent responses about government information and services.

For SSA, this initiative supports the following Strategic Goal: To deliver high-quality, citizen-centered service.

Recruitment One Stop—The purpose of this initiative is to deliver state-of-the-art on-line recruitment services to job seekers. They include intuitive job searching, on-line resume submission, applicant data mining, and on-line feedback on status and eligibility.

For SSA, this initiative supports the following Strategic Goals: 1)To deliver high-quality, citizen-centered service and 2) To strategically manage and align staff to support SSA's mission.

Online Rulemaking—This initiative allows a citizen to easily access and participate in a high quality, efficient rule making process. It improves the access to and quality of the rulemaking process for individuals, businesses and other government entities while streamlining and increasing the efficiency of internal agency processes.

For SSA, this initiative supports the following Strategic Goal: To deliver high-quality, citizen-centered service.

E-Training—The goals of this initiative are to provide a single point of online training and strategic human capital development solutions for all federal employees. This will reduce instructor and travel costs and improve human capital management.

For SSA, this initiative supports the following Strategic Goals: 1)To deliver high-quality, citizen-centered service and 2) To strategically manage and align staff to support SSA's mission.

E-Grants—Creating a single, online portal for all federal grant customers to find and apply for grants will make it easier for potential recipients to obtain information about federal grants.

For SSA, this initiative supports the following Strategic Goal: To deliver high-quality, citizen-centered service.

E-Clearance—This effort streamlines and improves the quality of the current security clearance process for individuals working for the Federal government whose jobs require that they handle sensitive and classified information.

For SSA, this initiative supports the following Strategic Goals: 1)To deliver high-quality, citizen-centered service and 2) To strategically manage and align staff to support SSA's mission.

Integrated HR—The intent of this effort is to streamline and automate the exchange of federal employee human resources information. It replaces official paper employee records, and will allow comprehensive workforce analysis, forecasting, and reporting across the Executive Branch for the strategic management of human capital.

For SSA, this initiative supports the following Strategic Goals: 1)To deliver high-quality, citizen-centered service and 2) To strategically manage and align staff to support SSA's mission.

Federal Asset Sales—This initiative will identify, recommend, and implement improvements for asset recovery and disposition, making it easier for agencies, businesses and citizens to find and acquire or buy federal assets.

For SSA, this initiative supports the following Strategic Goals: 1) To deliver high-quality, citizen-centered service and 2) To ensure superior stewardship of Social security programs and resources.

Consolidated Health Informatics—Adopting a portfolio of existing health information interoperability standards (health vocabulary and messaging) will enable all agencies in the federal health enterprise to "speak the same language" based on common enterprise-wide business and information technology architectures.

For SSA, this initiative supports the following Strategic Goals: 1) To deliver high-quality, citizen-centered service and 2) To ensure superior stewardship of Social security programs and resources.

E-Payroll—This initiative involves consolidating 22 federal payroll systems to simplify and standardize federal human resources/payroll policies and procedures to better integrate payroll, human resources, and finance functions.

For SSA, this initiative supports the following Strategic Goals: 1)To deliver high-quality, citizen-centered service and 2) To strategically manage and align staff to support SSA's mission.

E-Records Management—This initiative provides policy guidance to help agencies better manage their electronic records so that records information can be used effectively to support timely and informed decision making, enhance service delivery, and ensure accountability.

For SSA, this initiative supports the following Strategic Goals: 1) To deliver high-quality, citizen-centered service and 2) To ensure superior stewardship of Social Security programs and resources.

Disaster Management—This initiative provides federal, state and local emergency managers with online access to disaster management related information, planning and response tools.

For SSA, this initiative supports the following Strategic Goal: To deliver high-quality, citizen-centered service.

Business Gateway/eForms Portal—This initiative has been recently restructured and will put all government forms online at a single web site. This will enable business and citizens to electronically complete business with the government.

For SSA, this initiative supports the following Strategic Goal: To deliver high-quality, citizen-centered service.

Electronic Service Delivery

SSA has always looked for innovative ways to better use technology. The Agency uses IT creatively, responsibly and in a manner that demonstrates strong support of the Federal IT vision which is to achieve a dramatic improvement in the federal governments' value to the citizen; with decisions in minutes or hours, not weeks or months.

In support of providing high-quality, citizen-centered service, the Agency has created an easy-to-find single point of access to Social Security services for citizens on its website, www.socialsecurity.gov. In 1994, SSA was one of the first Federal Agencies to establish an Internet website. By 2003, SSA's website was attracting over 30 million visitors. SSA's initial focus was to provide information online; now the

Agency's strategy involves aggressively pursuing a portfolio of services that enable online transactions. The website was redesigned in April 2003 to make it more user-friendly and easier to find information and to conduct transactions.

SSA has reduced the reporting burden on business in the area of filing W-2 forms electronically and efforts are underway to improve that even more. The Electronic Wage Reporting project supports the Stewardship strategic goal. The Agency shares information quickly and conveniently between federal, state and local governments with computer data exchanges and data matches, saving many hundreds of millions of dollars annually. And the Agency has automated a number of internal processes which have reduced internal costs and has been working with other federal agencies to find and share best practices.

As SSA continues to automate services for citizens, private and public sector partners, and improve internal efficiencies and effectiveness, it will do so in light of its own vision statement, which is: Within the next five years we will provide cost-effective e-government services to citizens, business and other government agencies that will give them the ability to easily and securely transact most of their business with SSA electronically.

Five goals have been established in support of this vision:

- Offer to citizens the e-government services they want and need;
- Ensure stewardship by protecting online security and privacy;
- Pursue e-government partnerships and collaboration with other government agencies and private sector organizations;
- Implement e-government programs that offer sound business case justification; and,
- Align the organization and invest in human capital to maximize e-government progress.

SSA's strategy to pursue these goals is based on the expansion of electronic service delivery in ways that improve current business processes by increasing opportunities for the public to conduct SSA business, and to access information in a private and secure environment. While continuing to add services, SSA is focusing on increasing the public's usage of these transactional services. For citizens, this will mean greater convenience and access. For SSA, this translates into more effective and efficient public service.

IT Capital Plan Summary

Critical to this planning structure of goal setting, performance measurement and reporting are the linkages to ensure that the resources needed to support planned activities are identified and reflected in the budget. The Agency will continue to make well-planned changes in pursuit of performance objective achievement; changes that are found to be operationally effective and economically sound before resources are committed to their implementation. A system for monitoring

performance objectives has been developed. This system provides the information SSA needs to assess progress at key decision points and determine whether initiatives should proceed as planned or be redirected.

At the operational level, SSA has instituted a Systems Planning process that affords the customer community the opportunity to take an active role in deciding current and future systems workloads. Working together, the customer and systems personnel clearly define the scope of a project, and the return on investment of the work undertaken. The joint decisions between the two parties facilitate allocation of limited resources to the work deemed most important. Systems initiatives undertaken support Agency priorities, legislation and other Agency strategic directions, all of which are part of the Systems Plans.

The following section contains high-level descriptions of SSA's major IT initiatives found in the Capital Plan and milestone charts extending to FY 2009. As a result of implementation, the initiatives will serve to enhance Agency productivity, program integrity, customer service, and other desirable Agency attributes. These initiatives are also integral to achieving the future Service Vision. The table on the next page shows the relationship between the Agency's goals and objectives and the supporting major investment initiatives.

For ease of reference, the Agency goals and subordinate objectives are listed and the objectives are numbered as shown below. In the chart, the objective numbers appear in line with the major investment initiative that contributes to its support, under the appropriate goal.

- **To deliver high quality, citizen-centered service;**
  1. Make the right decision in the disability process as early as possible,
  2. Increase employment for people with disabilities, and
  3. Improve service through technology.
- **To ensure superior stewardship of Social Security programs and resources;**
  4. Prevent fraudulent and improper payments and improve debt management
  5. Strengthen the integrity of the SSN,
  6. Increase the accuracy of earnings records, and
  7. Efficiently manage Agency finances and assets and effectively link resources to performance outcomes.
- **To achieve sustainable solvency and ensure Social Security programs meet the needs of current and future generations;**
  8. Through education and research efforts, support reforms to ensure sustainable solvency and more responsive Retirement and Disability programs.
- **To strategically manage and align staff to support SSA's mission.**
  9. Recruit, develop and retain a high-performing workforce.

Agency Goal / Investment Initiative	Sustainable Solvency	Citizen-Centered Service	Superior Stewardship	Manage and Align Staff
Infrastructure	8	1,2,3	4,5,6,7	9
Telecommunications		1,2,3	4,5,6,7	9
Office Automation		1,2,3	4,5,6,7	9
Accelerated eDib		1,3		9
Electronic Wage Reporting System		3	6	
Ongoing DDS Automation		1,3		9
Financial Accounting System Replacement		3	4	
Digital Audio for the Recording of ALJ Hearings		1,3		
Access to Financial Institutions		3	4	
Title II System Redesign		3	4	
Paperless Processing Centers		3	4	9
SUMS/MCAS		3	7	9
eVital (Electronic Death Registration)		3	4	
Employees with Disabilities		2,3		9
Interactive Video Teletraining		3		9
Software Imaging Management		3		9

Table 5: Major Investment Initiatives

Major Investment Initiatives

Infrastructure

The Infrastructure initiative supports the information technology (IT) resources that enable SSA to promote the nation's economic security by administering America's major income support programs for the elderly, disabled, and their dependents and survivors. It provides a data computing architecture that permits fast and accurate processing of claims for beneficiaries. Some data is stored on a mainframe central repository, while other databases and applications are distributed across the enterprise at the desktop level. Much of this data is also available to the public via web based applications.

This initiative integrates four major segments of IT resources: mainframe, storage, web services, and security/business recovery. The mainframe segment includes: mainframe capacity infrastructure; mainframe software acquisitions and upgrades; IBM proprietary mainframe software; system monitoring and network management; and enterprise output infrastructure. Storage is a narrow segment comprised of

storage architecture and enterprise system capacity management infrastructure. Web services is a broad segment consisting of: enterprise server infrastructure; client server software; extranet/internet/intranet; internet environment support; data exchange infrastructure; and ongoing website enhancements. Security/business recovery is a specialized segment which incorporates: security infrastructure; public key infrastructure; and the business recovery computing environment. Collectively, these segments provide acquisition, upgrade, refreshment, and relocation solutions to support SSA's mission, and they provide the basis for expanded eGovernment and eCommerce initiatives.

SSA's infrastructure supports an increase in interactive automated services via the Internet, for purposes of simplifying business transactions that do not require interaction with an SSA representative. Infrastructure technology will enable SSA to more accurately forecast service demands and maximize the efficient use of the Internet as a resource to provide those services.

This initiative provides continued software and hardware support and upgrades as well as technical service support to ensure efficient systems operations and effective utilization of Agency resources, paving the way for expanded service to the public and to other SSA customers. IT hardware must be compatible with existing and emerging technologies, and software must be upgradeable and have the ability to seamlessly integrate with hardware technology changes. Providing employees immediate access to the latest software configurations will allow employees to increase their productivity at a time when SSA workloads are increasing and staff levels are stagnant.

Telecommunications

Telecommunication investments include ongoing operations for maintaining citizen-centered service to the public in the face of growing workloads, while providing the infrastructure now and in the future to support the many ways that SSA currently does business with the public.

The ongoing operations for this initiative encompass the Telephone, Wide Area Network (WAN), Video Teleconferencing (VTC) and the National 800 Number Network (N8NN). This investment provides funding for new installations, maintenance, upgrades and monthly recurring charges for essential hardware, connectivity and bandwidth required for data, voice and video to transport mission critical information in support of the many Agency activities.

This initiative includes the personnel, support services, hardware, software, maintenance, and usage for the following items: Telephone/WAN/VTC Moves, Adds and Changes, Telephone System Purchases, Network Infrastructure, N8NN Usage, ATM/Frame Relay Usage, FTS Long Distance Usage, Telephone Switch Infrastructure, Local Telephone Usage, Cellular Telephone and Pager Usage, Fax Maintenance, VTC Infrastructure and Usage, Subnetted VoIP, Remote Network Access, Telephone System Replacement Project, Ethernet Migration Project, Campus WAN Extension Project, VTC Expansion Project, and the National 800 Number Screen Pop Project and speech enabling the national 800 number network platform. Without a robust and optimized telecommunications investment, SSA

would be unable to provide timely payments for the increasing number of older Americans, Americans with disabilities, and their dependents.

Office Automation

SSA relies on a complex IT architecture in order to support its mission-critical programmatic and administrative workloads. The Office Automation initiative will provide the necessary funding to upgrade the existing hardware and software to eliminate costly, obsolete technology. Office Automation is focused on building and maintaining the environment needed for SSA's applications and resources.

The following platforms are linked and create the Agency's overall architecture. They include the desktop, server, and laptop infrastructure totaling over 150,000 devices, and the network and support services to maintain those devices including engineering, systems operations and product support, electronic messaging infrastructure including the hardware and software needed to support e-mail, local area network expansion and support services, and small purchase capability to sustain the infrastructure.

Upgrading hardware allows SSA to remain on the cutting edge; therefore, providing the latest technological advances to employees and the general public. By centralizing hardware and software procurement SSA benefits from competition and economies of scale resulting in lower cost to the government and a more standardized environment.

Accelerated eDib

Accelerated eDib (AeDib) is the Agency's plan for using technology to support the business changes required to administer the Disability Program. This initiative, a key component of Disability Systems Modernization, will build integrated disability processing software for use by SSA components and state Disability Determination Services. AeDib is the enabler to ensure that SSA meets and exceeds established performance goals and fulfills Agency service level objectives. In addition, AeDib supports expanding E-government, one of the five Government-wide initiatives identified in the President's Management Agenda.

The AeDib initiative will transform the current paper-intensive and geographically dependent disability process into an electronic processing environment with no geographic boundaries. AeDib and the electronic folder technology infrastructure will automate, streamline, and simplify data collection, documentation and verification functions for all components involved in the disability process. The combined impact will be improved services to the public through a reduction in processing times.

These are the activities that support AeDib:

- **Expand Electronic Disability Collection System (EDCS)**—Enhance the automated system that captures information collected during the disability interview to support all types of disability claims and deploy the system nationally.

- **Expand Internet**—Provide the capability for claimants to complete the most widely used disability reports via the Internet.
- **Create an Electronic Folder**—Create a repository to store electronically all of the documents, evidence and records upon which the disability determination is based. Interface this electronic folder with SSA and DDS systems.
- **Develop a Case Processing Management System for OHA**—Provide a case processing and management system for OHA to support its business process and develop an interface to the electronic folder.
- **Accelerate AS/400 Migration**—Ensure that all DDSs, which currently depend upon Wang VS minicomputers, are transitioned to the AS/400 and have software that is able to run on the more stable platform so that they can interface with the electronic folder.

AeDib will significantly change the SSA disability business process for the better and will contribute to the Agency's outcome goals of more timely and accurate adjudication at all levels. Through the effective application of information technology to the disability process, the Agency expects to reduce the time it takes to make disability decisions while improving cost efficiency and decisional accuracy.

Electronic Wage Reporting System

The Electronic Wage Reporting System (EWRS) will enable the employer community to electronically transmit forms W-2/W-3 to SSA. Congress has mandated that 80% of all Federal tax and information returns be processed in electronic form by the year 2007. This legislation has been interpreted by the Internal Revenue Service to extend to Forms W-2/W-3, which are filed with SSA. In addition, this project is an enabler to meet many of the goals of the Simplified Tax and Wage Reporting System.

Recent Congressional and Office of the Inspector General interest in the growth rate of SSA's Earnings Suspense File have placed additional pressure on the Agency to improve the efficiency and effectiveness of processing and maintaining earnings information. This requires SSA to re-engineer the business procedures and front-end systems used to process annual wage reports (AWR) submitted electronically and on magnetic media.

The EWRS will enable SSA to process efficiently and effectively wage reports submitted on various media in a variety of methods (i.e., diskette, bulletin board, Internet, value-added networks and electronic data transfer). The system will also provide expanded services to SSA's annual wage reporting customers by providing an acknowledgement of receipt, filing status information, complete and timely information on processing results, testing capabilities and additional customer support. The electronic wage reporting capability will not only provide the business community additional easy-to-use and cost-effective ways to file wage reports, but also lower SSA's processing costs, capture data more quickly and transmit data to the Internal Revenue Service within shorter timeframes.

Like all Federal agencies, SSA is reviewing and reevaluating many of its existing programs to assure that appropriate security controls are in place to identify potential fraudulent activity and to implement appropriate controls to prevent future occurrences. As part of this, the EWR project requires enhancements to the Integrated Registration System for Employers and Submitters (IRES) to implement additional security controls. IRES is the registration gateway to a number of other applications (e.g., Social Security Number Verification Service (SSNVS) and must be modified and maintained to meet the security needs of those applications.

The EWR system is important to the Agency's efforts to promote and increase electronic commerce and paperless processing in support of the President's Management Agenda. The administration's expeditious and efficient posting of earnings to the master earnings file results in more accurate payment of social security benefits. An accurate benefit payment not only reduces benefit overpayments and agency collection efforts; it also builds the public's confidence in the administration.

Ongoing DDS Automation

The Ongoing Disability Determination Service (DDS) Automation initiative will provide the Agency with more flexibility and a timelier means to meet DDS automation requirements and the means to better manage both Federal and State funded projects. The Social Security Act mandates that a DDS in each State perform determinations of disability for residents of that State who file for Social Security benefits. The DDSs are agencies of the State governments, yet they are entirely federally funded and perform services subject to the regulatory authority of SSA. SSA provides approximately $1.7 billion annually to process disability cases.

As DDSs rely on their automated systems to effectively process disability claims, maintaining and enhancing the technical viability of these systems is paramount in order for them to meet their budgeted workloads. The initiative provides for application software maintenance and enhancements, IBM iSeries 400 mid-range processors and supporting peripheral equipment, infrastructure upgrades, IBM integration services, IBM support services, hardware maintenance, mid-range processor security standards, 508 compliance, disaster recovery and technical training of DDS personnel.

This project specifically supports the Agency's goal to improve the accuracy, timeliness and efficiency of service to the public applying for DI and SSI disability benefits by implementing the necessary activities to have the software and infrastructure in place for electronic processing of disability claims. It further supports the President's Management Agenda's government-wide goal of competitive sourcing and expanded electronic government, as well as budget and performance integration to improve Federal management and deliver results that matter to the American people.

Ongoing DDS automation is a critical enabler of SSA's strategic objective to position the Agency's resources and processes to meet emerging workloads as it supports automation in the 54 State DDS offices and the Federal DDS (FDDS). The Agency

expects improved processing times and better service. In addition, these system improvements will pay for themselves in DDS work year savings within a few years.

Financial Accounting System Replacement

The Social Security Online Accounting and Reporting System (SSOARS) project provides the Agency with a COTS comprehensive financial accounting system, which is certified by the Joint Financial Management Improvement Program (JFMIP) and complies with the Federal Accounting Standards Board (FASB) principles. The Oracle Federal Financial COTS package was selected as the foundation for the new system.

The new system includes accounts payable, accounts receivable, purchasing and general ledger functions and reporting. It also utilizes state of the art technology, so SSA may take advantage of modern efficiencies. Overall, SSOARS will provide better control of funds and data consistency across the Agency.

The initial procurement consisted of two elements—products and services. Products constitute the contractor's baseline financial system as offered to the public for sale. Services were required to implement and maintain the operational financial system, and to meet SSA's technical and functional requirements, which are above and beyond the baseline system. There has been no software customization of the Oracle COTS package but rather extensions have been incorporated into the software to meet the SSA's requirements. As a result, SSA will be able to benefit from upgrades to the baseline software without the need for customization. Support IV and V services were also acquired to monitor and assure the success of the SSOARS system implementation project.

With the initial release of the project in October 2003, SSOARS has become SSA's system of record. Additional releases will incorporate functionality which was deferred in release 1 and to implement system interfaces to other feeder systems, such as SSA's Streamlined Acquisition System (SSASy), Third Party Payment System, Credit Card System, Travel Manager, and the Field Financial Information System (FIS).

This system ensures integrity and efficiency in the Agency's role as steward of public funds. It ensures that our financial and management information systems provide managers and other decision-makers with reliable, timely and useful financial information so that they can make informed operational and investing decisions, given limited resources. SSOARS also aims to improve security and data integrity in compliance with OMB Circular A-130, Management of Federal Information Resources. The system directly supports the Presidential Management Agenda initiative to improve financial management by: improving the timeliness [of financial data]; enhancing the usefulness [of financial systems]; and ensuring the reliability by obtaining and sustaining clean audit opinions [of financial statements].

Digital Audio for the Recording of ALJ Hearings

This project will replace unsupported and obsolete analog recording technology with digital recording technology to support judicial hearings by Administrative Law Judges (ALJs) in SSA's Office of Hearings and Appeals (OHA). OHA is responsible

for holding hearings and for providing appellate reviews of these hearings as part of the Social Security administrative appeals process. OHA also prepares the certified administrative record of a case if a claimant files a subsequent civil action. Part of the hearing process involves making an audio recording of the hearing, including the claimant and expert witness testimony. The recordings are made at 150 hearing offices nationwide and at remote sites where ALJs travel to hold hearings.

The industry change from analog to digital technology, the need to better address information storage, retrieval and processing concerns, the need to improve the quality of service delivery, and the need to keep pace with changes to key segments of the government's ESD architecture demand that the Agency move from the current analog cassette format to a digital audio format. Further, it is believed that the vendor will soon cease to service and produce the analog 4-track cassette recorder that the Agency has used in the past.

OHA has developed an IT strategy, identified key technological parameters and business needs, developed a tactical IT plan descriptive of its business processes, and is proceeding to replace its analog recording system with a digital audio recording system. This system is designed to capture hearing recordings in the more durable, flexible digital format, which also provides superior sound quality.

One of the Commissioner's highest priorities is to improve service to the public in the disability program from initial claim through final review. The digital format will enable OHA to store the recordings within a central repository, such as SSA's Document Management Architecture (DMA), and make electronic sharing of information possible to all SSA users who review these recordings.

This new recording system will improve the efficiency and the quality of services delivered to the public while reducing costs to the public for supporting the system. Installation of this technology will allow for electronic access to hearing recordings and the ability to more quickly process cases and make decisions on this information in an electronic environment.

Access to Financial Institutions

SSA is required to verify the income and resources of SSI applicants and recipients in order to determine their eligibility for benefits. The Access to Financial Institutions initiative allows SSA to establish an automated method of contacting financial institutions (FI) to verify and uncover the financial resources of applicants/recipients, while ultimately lowering the number of payment errors. Current manual and paper processes are extremely slow, labor-intensive and non-comprehensive.

Today more than 6.7 million people in the United States receive Supplemental Security Income (SSI). To be eligible for SSI benefits, recipients must meet specific income and resource criteria. Section 213 of the Foster Care Independence Act of 1999, "Access to Information Held by Financial Institutions," provides SSA with the right to require applicants and recipients to authorize the Commissioner to request from any FI any record concerning an applicant's or recipient's financial resources. It allows SSA to obtain the information without furnishing the FI with a copy of the

authorization, thereby allowing for an electronic process. Any requests made under this provision are deemed to meet the requirements of the Right to Financial Privacy Act.

Over the past decade, the accuracy rates of SSI payment outlays compare favorably to the accuracy levels achieved in other income maintenance programs. However, in a program the size of SSI, a small percentage of error translates into large dollar amounts. Consequently, SSA has committed to continually improve the SSI payment accuracy rate. By 2008, the Agency plans to increase SSI payment accuracy to 96% (based on preventable error). SSA's strategy for increasing the accuracy of SSI payments is part of a comprehensive plan to improve the management of the SSI program.

To test the feasibility of electronic verification of bank accounts, SSA is conducting a one-year proof-of-concept (POC) test. At the conclusion of the POC, a decision will be made on whether or not to proceed with nationwide expansion of the project.

Title II System Redesign

The goal of the title II System Redesign initiative is to provide a single system for processing virtually all social security initial claims and client-initiated postentitlement actions in an online interactive mode. Previously there were a number of separate systems to process this data and this led to flaws in data integrity and program maintainability.

The backbone of the redesigned system will be the use of common code to perform processing of common business functions. The net effect will be a greater capability to process work at the customer's first point of contact with the Agency, online user access to more comprehensive customer information, and an automated system that is easier and less costly to maintain and modify.

The redesigned title II System will automate all but the most complex tasks and will allow employees serving the public to concentrate their time on more complex claims and transactions. The benefit will be realized in improved customer service and decreased annual work years.

A phased implementation through FY 2005 will result in:

- Title II initial claims and postentitlement releases to support processing of cases in which data were collected over the Internet;
- Increased automation of Workers Compensation cases;
- Full implementation of "Expedited Reinstatement" legislation;
- An improved interface with title XVI systems and processing;
- Common business function software for initial claims and postentitlement processing;
- Improved interface with Treasury;
- Improved disability processing;
- Processing transactions with beneficiaries entitled on two accounts;

- Automation will increase to 92 percent of all title II transactions;
- Improved processing of overpayments; and
- Capability to process 99% of all claims and postentitlement actions electronically.

Beyond FY 2005, there will continue to be major improvements to title II systems that will focus on further increasing automation, responding to legislative mandates and taking advantage of new technology.

Paperless Processing Centers

The Paperless Program Service Centers initiative is an image-based workflow management system for the Program Service Centers (PSC), Office of Disability Operations (ODO) and Office of International Operations (OIO). It provides for capturing information received on paper through electronic imaging. The information is then available for case processing on demand. The PPC initiative addresses the storage management, retrieval, and routing of document images and electronic forms, providing a framework for further Agency-wide planning and development.

Paperless PC, through software release 2, is fully developed, deployed and operational in all intended sites. Operational components have requested the development and installation of additional enhancements that will be incorporated in release 3.

The availability and performance of the system are essential for the users to meet the Agency's strategic goal of providing high quality citizen-centered service. Since the initial implementation, Systems has made significant progress in both software and infrastructure stability. Paperless PSC has been operating with a 98 percent or better availability since January 2001. In addition to improving service and stewardship, SSA increases the security and protects the privacy of its information by eliminating the repeated handling of paper and moving it through multiple physical locations.

SSA has seen a reduction in the length of time it takes to act on information received in the PSC. Furthermore, management has received a number of anecdotal reports of improved employee satisfaction and morale from people using the new way of doing business.

SUMS/MCAS

SSA uses management information (MI) as the tool to quantify information for all of its workload categories and expenses. The Social Security Unified Measurement System (SUMS) and Managerial Cost Accountability System (MCAS) projects will revolutionize our MI and managerial accountability and control systems.

Both of these projects rely on information collected throughout the Agency as a result of the work being performed. MCAS focuses on critical performance and financial information needed by managers and employees throughout the Agency, while SUMS focuses on the detailed data needed by managers and employees to track, monitor and forecast critical Agency workloads. Both will support improved service to members of the public and to SSA beneficiaries.

SUMS/MCAS consists of the following interrelated initiatives:

- **Workload Counts and Performance Measures** - Produce consistent workload counts, processing time and other performance measures from the same data source;
- **Time Allocation** - Replace current labor-intensive work sampling processes with more automated processes that will provide the information needed to calculate workpower;
- **Customer Service Record** - Provide interviewers with access to customer information from existing data sources in a concise and easily understood format while capturing more complete data on customer interactions; and
- **Managerial Accountability** - Replace the current fragmented management, cost and accountability systems with a unified expanded and improved system that will eliminate manual processing. The new system will include all workloads, costs, goals, performance measures, efficiency measures, effectiveness measures and managerial accountability measures. It will provide management, control, accountability, performance, financial and productivity data that are valid at the local office level through the Agency level.

SUMS and MCAS have common goals of using more accurate and consistent information, providing improved access to MI, improving work power allocation, improving customer service and reducing manual work. The investments will provide access to information needed to meet changing business requirements, support process reviews and comply with government-wide standards for cost accountability.

The systems provide the essential means of accomplishing the President's Initiative for Budget and Performance Integration, which expects Agencies to: "identify high quality outcome measures, accurately monitor the performance of programs, and begin integrating this presentation with associated cost." MCAS implementation also fulfills SSA's commitment to Congress to develop and implement this process and system as related to the Social Security Independent Agency Act.

eVital

eVital is one of the twenty-four initiatives targeted to rapidly expand electronic government in support of the President's Management Agenda. eVital also supports Homeland Security and the Improper Payments Collection Act of 2002. This initiative was an outgrowth of a partnership between SSA and state level directors of vital statistics (VS) registrars through their national organization—the National Association for Public Health Statistics and Information Systems (NAPHSIS). SSA is also working with other organizations, such as the National Association of State CIOs (NASCIO) to further build partnerships to support this effort. Other Federal agencies, as direct or indirect participants in the exchange of vital records information with the states, are supporting partners in the eVital initiative. These agencies include: Departments of State, Defense, Veterans Affairs, Education, and

Homeland Security, Office of Personnel Management, the Railroad Retirement Board, and the Internal Revenue Service.

eVital is designed to contribute to improved government service delivery along a number of avenues. These include: simplifying delivery of services to citizens by streamlining and automating the death registration process and the exchange of vital records information between state and Federal agencies; making it possible for government agencies and employees to find vital records information required to deliver government services effectively and on a timely basis; and reducing operating costs by constructing an integrated data exchange mechanism.

eVital was comprised of two distinct projects, the Electronic Death Registration (EDR) process and the Electronic Verification of Vital Events (EVVE). The latter project, EVVE, was concluded at the end of calendar year 2003. SSA and its various partners continue to build EDR. Individual states will be added to the national infrastructure being created for EDR as funding permits and as the technological readiness of each state matures.

ELECTRONIC DEATH REGISTRATION (EDR)

Recent advances in computer and network access technology allow for the practical and efficient development and implementation of automated systems to register death information. EDR methods have been independently pioneered in several states. These different approaches serve as the basis for developing standardized EDR attributes, methods and processes in order that the states may successfully implement electronic death registration to satisfy administrative and statistical death information needs.

The EDR investment is designed to:

- build a uniform data exchange mechanism for SSN verification at the start of the death registration process;
- enable electronic receipt of verified first-party death reports as a basis to terminate benefit payments;
- provide more accurate and timely reports of death; and
- enable improved quality of data on SSA's Death Master File.

An electronic death registration system is expected to reduce reporting delays, reduce improper payments improve data quality, and ultimately to increase the usefulness of information related to death (i.e., morbidity and mortality information) via a single, standardized death certificate format needed by Federal agencies such as National Center for Health Statistics and the Centers for Disease Control.

Employees With Disabilities

Executive Order 13163 challenged all Federal agencies to hire 100,000 qualified individuals with disabilities over a period of 5 years (FY2001 to FY 2005). This plan for expansion will result in an estimated SSA workforce increase of approximately 3,000 disabled employees—50% of the employees with targeted disabilities and 50% with non-targeted disabilities.

The Employees With Disabilities (EWD) project provides for the purchase of new and replacement workstations for employees with disabilities, IWS/LAN training for new EWD hires, and IT that will meet Section 508 compliance. The initiatives associated with this project include:

- Additional workstations for 300 new EWD hires per fiscal year and training classes for these new hires;
- EWD workstations/notebooks to continue the replacement of workstations/notebooks every three years;
- Software to develop accessible electronic forms to meet Section 508 compliance;
- Diagnostic automated software tools to diagnose and retrofit websites to meet Section 508 standards;
- Software licenses to participate in a government-wide (sponsored by GSA) TTY system for the deaf and hard of hearing;
- Software for research and testing to find solutions that are compliant with Government Paperwork Elimination Act (GPEA) and Section 508 (e.g., Adobe PDF files and scanning software); and
- Acquisition of assistive technologies (e.g., magnification software, voice recognition software, Telecommunications Devices for the Deaf (TDD) hardware and software, large monitors, CCTVs, scanners, Braille terminals, Braille printers, speech synthesizers, alternate input devices, etc.).

Interactive Video Teletraining

The IVT system is an interactive tool that brings the traditional classroom to distance-learning classes using video, audio and data communications so that a centrally located Instructor can communicate with each member of a classroom. IVT allows SSA to deliver timely, consistent and job-specific training to its employees. With IVT, SSA can perform live training broadcasts with interactivity from its studios. These live training broadcasts are transmitted to many of SSA's field offices throughout the 48 contiguous states, Hawaii, Alaska, Puerto Rico and United States Virgin Islands. This allows SSA to provide on-the-job training to many of its employees right from their offices, while at the same time, providing consistent training on numerous SSA policies and regulations.

The IVT infrastructure provides funding for new installations, maintenance, upgrades and monthly recurring charges for essential hardware, connectivity and bandwidth required for voice, data, and video to transport mission critical training in support of the many Agency activities. A small amount of funds are used for pilots to continue to make enhancements in order to meet the training needs of the future.

IVT is one of the key avenues used to provide training to SSA's widely dispersed staff. The net result will be that individual offices will accelerate their ability to address growing individual training needs while concurrently meeting increased workload demands.

Software Imaging Management

A reliable, automated Software Distribution (Imaging) and Configuration Management tool is a vital part of the Agency's IT infrastructure. This solution will play a key role in providing SSA field personnel with the latest and most accurate software that will allow them to perform their duties for the public.

This initiative provides a single software distribution (imaging) product that can provide unattended distribution of, and greater flexibility for, new software releases to as many of SSA's diverse platforms as possible. The current method of software distribution cannot be used to distribute to the Unix platform or to Internet web servers, the direction the Agency is headed towards.

The initiative includes funding for the:

- Purchase of configuration management and distribution software beyond the Windows 2000 (W2K) desktop environment (i.e., Unix and web-based platforms);
- Technical support services; and
- Maintenance upgrades of the configuration management and distribution software.

This initiative provides continued software distribution upgrades and technical support to ensure efficient systems operations and effective utilization of Agency resources. Software problems must be expeditiously resolved and upgrades applied, which will result in reduced workstation downtime. Problems that are not resolved expeditiously could jeopardize the Agency's service to the public. In addition, a Software Distribution (Imaging) and Configuration Management tool will permit SSA to quickly and reliably distribute and install application software to all employees. Giving employees immediate access to the latest software builds will allow employees to increase their productivity at a time when SSA workloads are increasing and staff levels are stagnant.

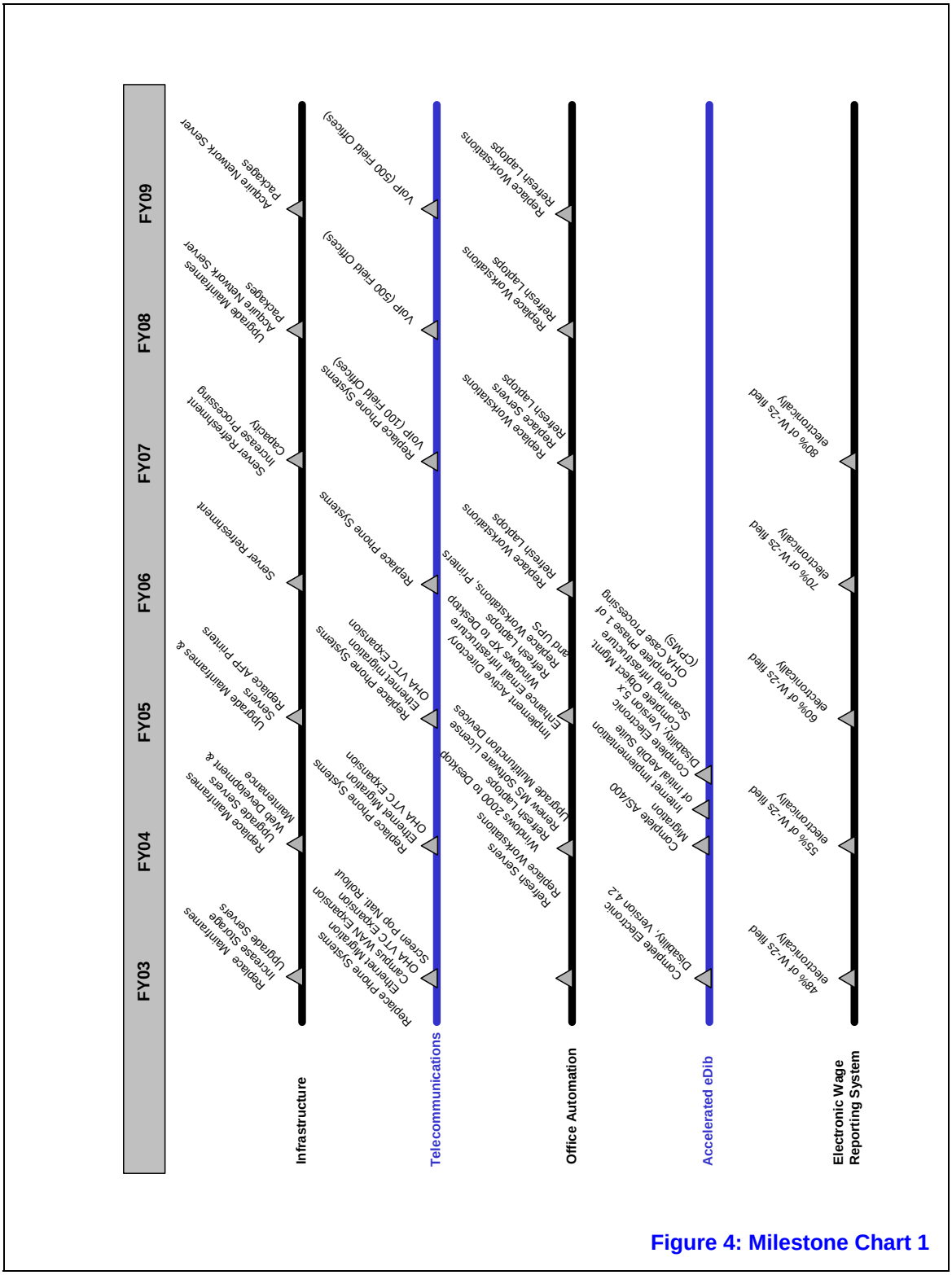


Figure 4: Milestone Chart 1

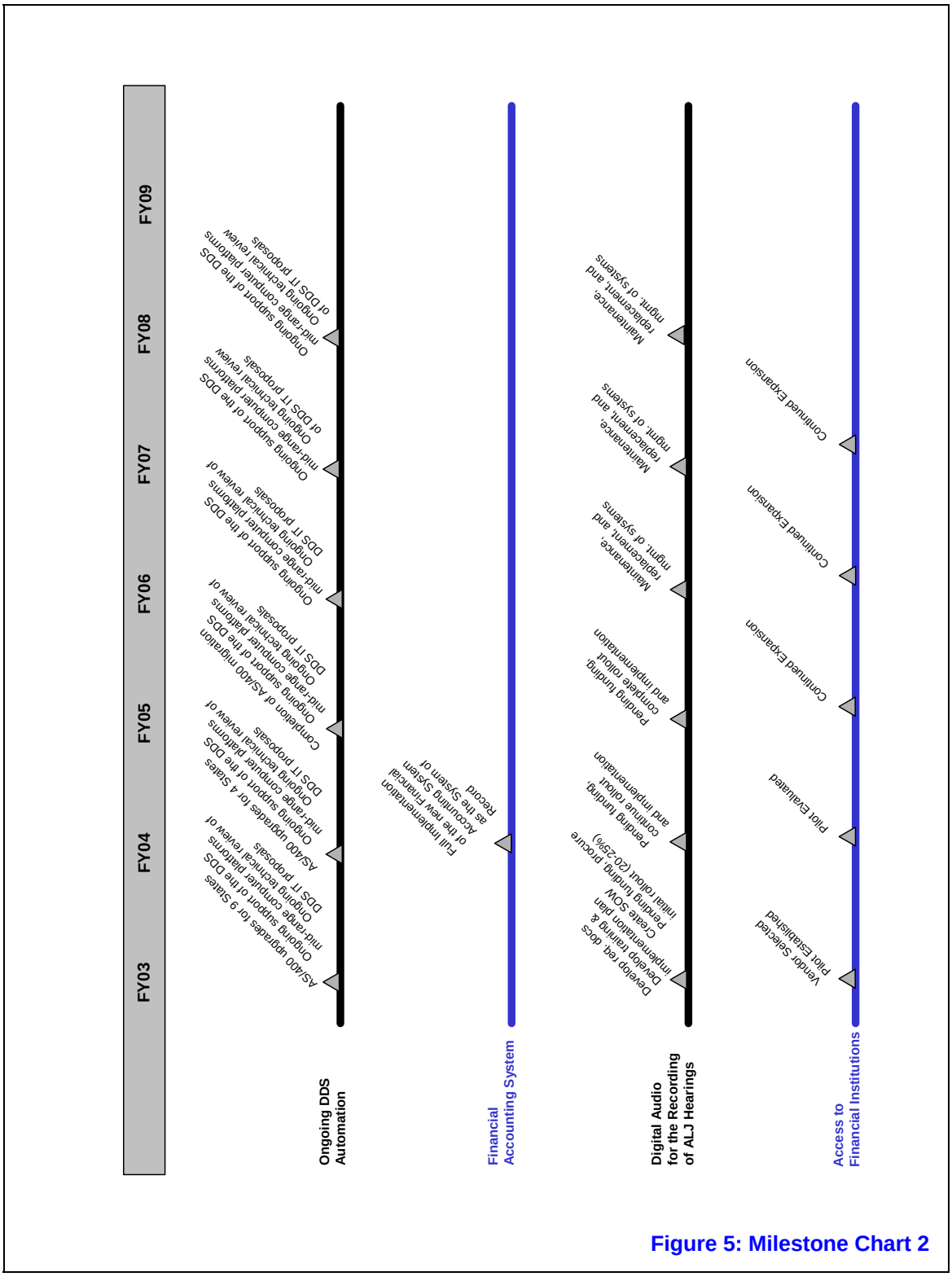


Figure 5: Milestone Chart 2

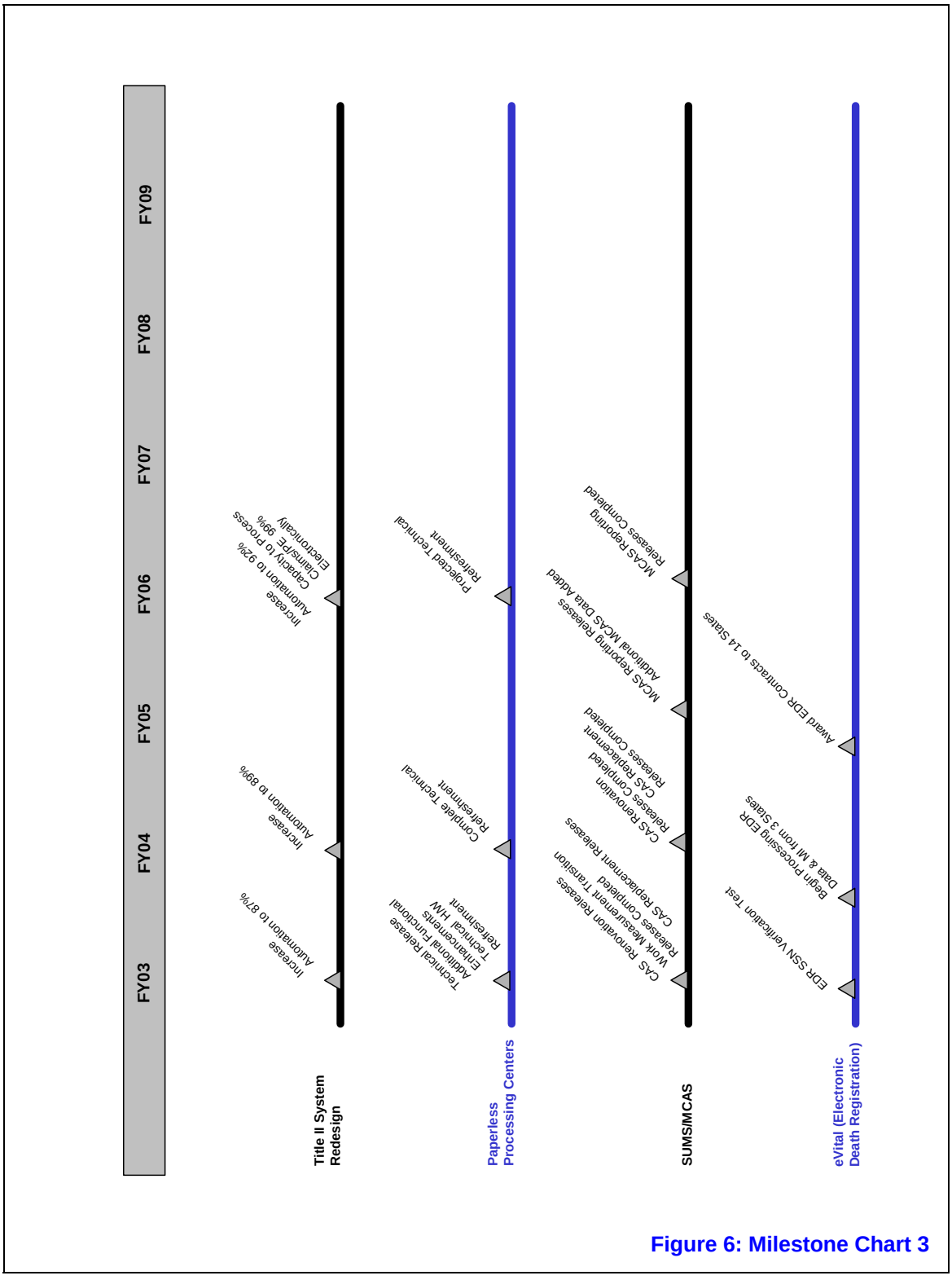


Figure 6: Milestone Chart 3

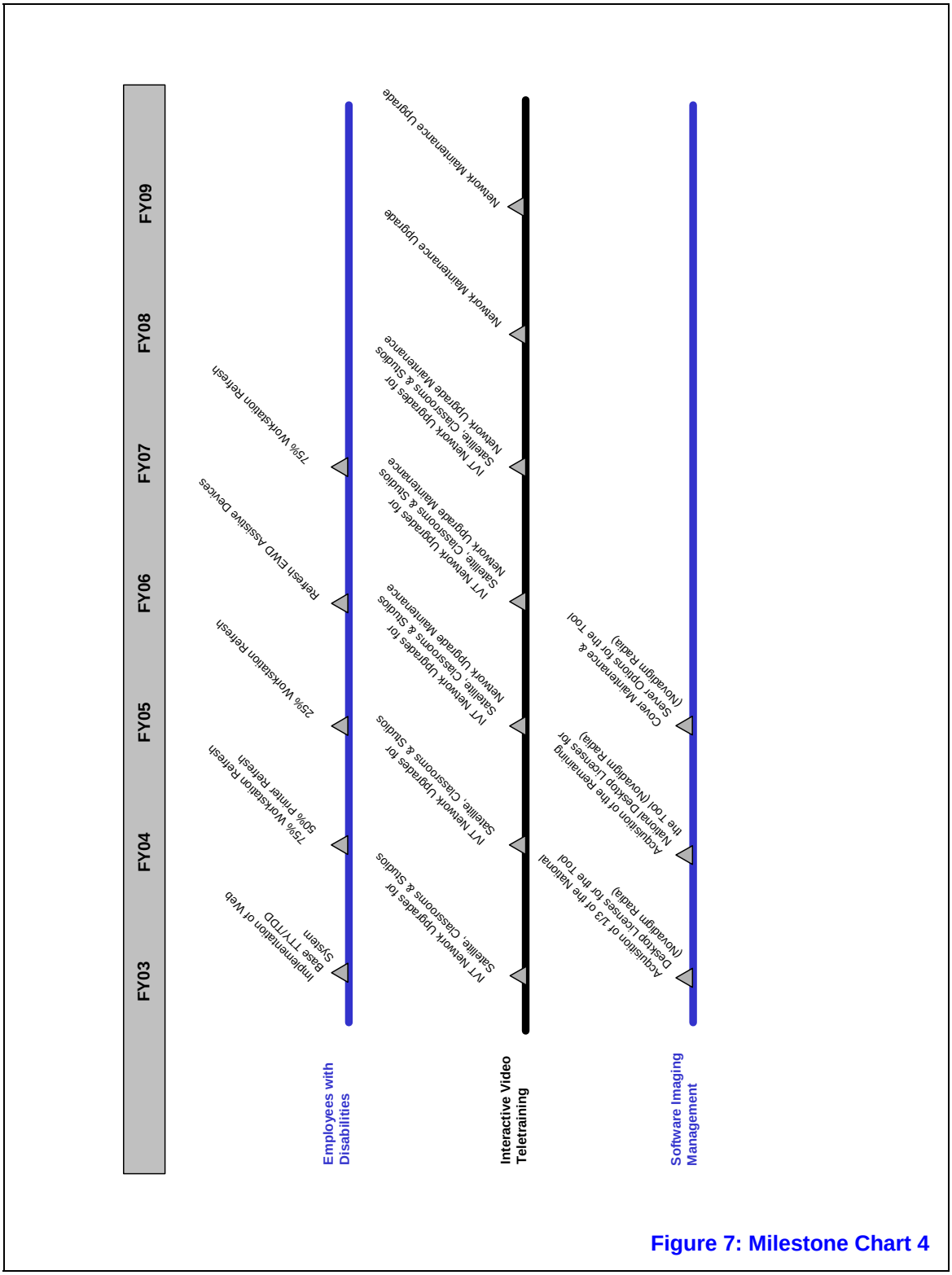


Figure 7: Milestone Chart 4

Chapter 6: Process Management

Capital Planning and Investment Control

Information Technology Capital Plan

The Information Technology (IT) Capital Plan provides information for OMB to use annually to evaluate and compare progress made by Federal agencies in support of the Administration's overall IT agenda.

SSA's IT Capital Plan is operational in nature. It is used to transmit the Agency approved initial budget to OMB. During the annual budget cycle this plan is updated to reflect the President's decisions on the Agency's budget. The IT Capital Plan includes the major and significant Agency projects that are approved for implementation. All project implementations adhere to the Agency's Capital Planning and Investment Control process that is documented as part of the Agency's IT Capital Plan.

The IT Capital Plan and its project portfolio support the elements of SSA's unified planning system described in Chapter 1, as well as legislative mandates with which the Agency complies.

Components of the Agency's IT Capital Plan include:

1. All IT Capital Asset Plans and Justifications as required by OMB Circular A-11, Section 300.
2. A description of the Agency's management of its IT investments for the other than major projects (this addresses the Clinger-Cohen Act requirement that agencies manage all IT investments).
3. A description of the Agency's Capital Planning and Investment Control process including descriptions of the criteria used to select investments into the Agency's portfolio, how the investments are controlled and managed, and how the investments are evaluated based on planned performance versus actual accomplishments.
4. The summary plan included in the Agency's five-year Security plan as required by 44 U.S.C. 3505 and Appendix III of OMB Circular A-130. The Plan must demonstrate that IT projects and the Enterprise Architecture include security controls for components, applications and systems that are consistent with the Agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality and explain any planned or actual variance from NIST standards.

Target Capital Planning and Investment Control Process

The Agency's Target Capital Planning and Investment Control (CPIC) process for Information Technology (IT) establishes and manages the Agency IT portfolio. The Agency CPIC process facilitates project oversight and the integration of Agency processes for making budget, financial and program management decisions.

The Agency CPIC process involves three distinct phases. The process begins with the "Select" phase, a series of rigorous Agency IT portfolio selection activities, followed by the Agency's "Control" process and finally a process to "Evaluate" the outcome IT initiatives. The evaluation process provides essential feedback to enhance the CPIC process and improve the Agency management of IT initiatives.

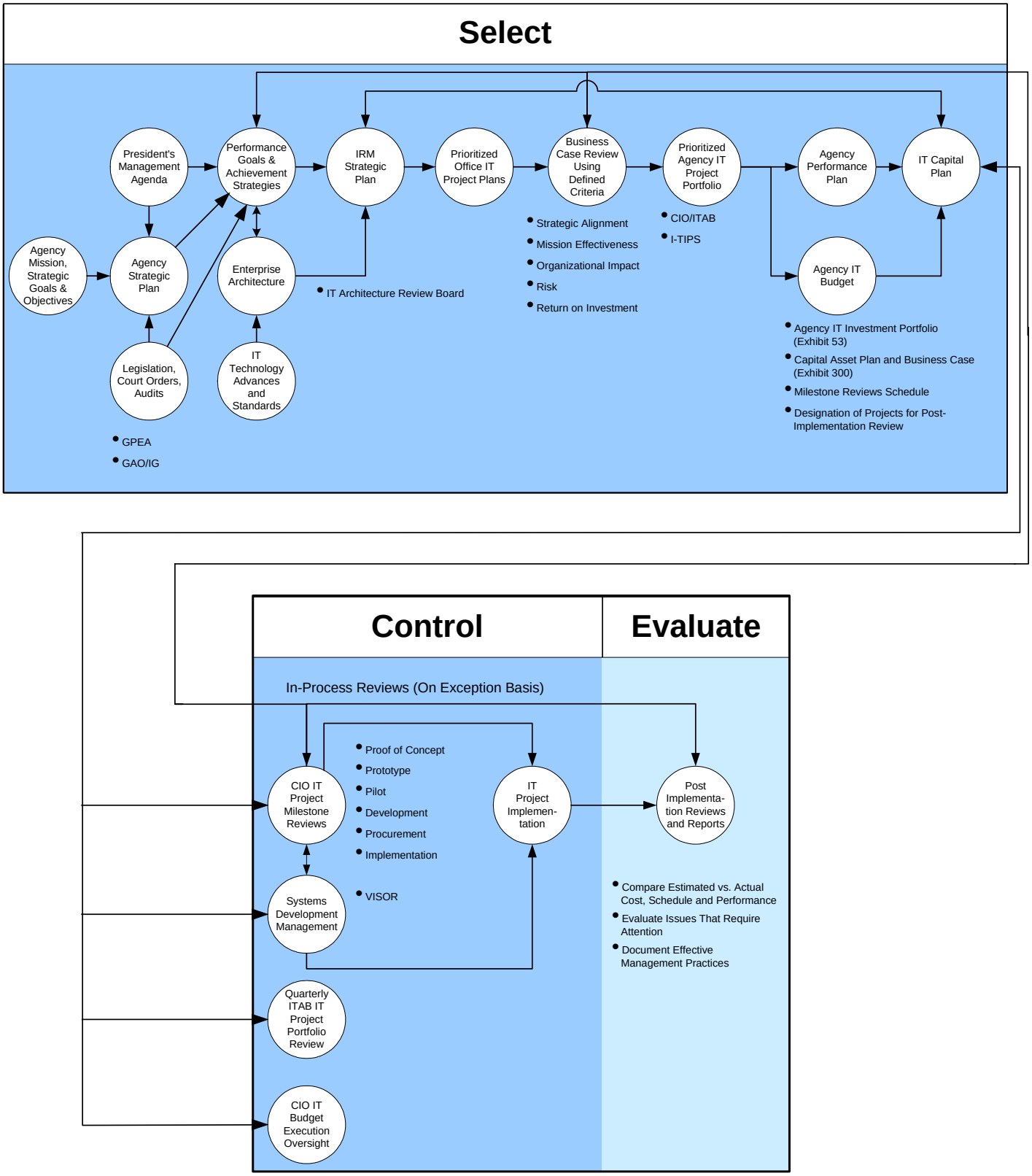


Figure 8: Target Capital Planning and Investment Control Process

Systems Development Management

Advancing technology requires that multiple systems management disciplines for developing application software must be available to SSA practitioners. In response to a need for improvement in the systems development process as the Agency moves to a cooperative processing environment, SSA is putting a new strategy in place. This strategy will update some of the disciplines already in practice, as well as introduce new disciplines.

Software Process Improvement Using the Capability Maturity Model

Developing software using the most efficient and effective processes is essential to supporting the Agency's constantly increasing need for automation. *The SSA software development community needs processes in place to maximize the return on investment that the Agency accrues through the application information systems technology.* Developing and institutionalizing a consistent, disciplined environment will provide the basis for improving work processes and for training staff.

SSA's Systems Process Improvement (SPI) program is following the approach recommended by the Software Engineering Institute (SEI) at Carnegie Mellon University, the developers of the Capability Maturity Model for Software (SW-CMM). This effort is establishing a repository of best practices for all software development projects to be able to tailor and follow. The processes include measurements to enhance the ability to predict time frames and staffing needs on projects.

A recent evaluation of selected high priority projects conducted by the SEI resulted in the achievement of Level 2 of the SW-CMM. This achievement positions the organization to move toward the goal of reaching the quantifiable benefits of higher maturity levels.

Systems Development Process Engineering

Process Assets Library

The Project Resource Guide (PRIDE) is a web-based resource that is intended to be a virtual Project Office. It provides the capability of housing the organization's process assets in a library and delivering specific instruction, guidance and data to SSA management. This information is available to document, plan, monitor and manage an organization's processes and software development projects.

The SPI Team works with project teams and other Systems personnel to author, customize, deploy and maintain processes in PRIDE. The Project Manager (PM) selects the appropriate process from the PRIDE library and appropriate model for a Microsoft Project Work Breakdown Structure (WBS). The PM then customizes the WBS to include activities, dependencies, resource estimates and milestones related to the specific project. This schedule is then stored in an MSP repository. Through

PRIDE, team members have access to procedures, templates and samples of the deliverables for each task.

At the end of each week, team members use the Resource Accounting System (RAS) to record the actual number of hours spent on a particular project or release. These hours are provided to the PM for comparison with estimated or scheduled effort. The project schedule can then be updated to reflect changes in resource utilization, milestone dates or other project data.

Project and Integration Management

Policies, standards and procedures are used to insure efficient management, control and integration of SSA's Information Technology (IT) projects. The primary objectives of these procedures are to (1) provide management information for oversight and decision making, (2) maximize the efficient use of scarce resources, and (3) ensure the use of uniform, proven practices to achieve project objectives.

In conjunction with the need to improve the systems development process, new strategies are in place and underway to facilitate ITS project integration and management. Current, near-term activities focus on projects which users indicate must be accomplished within the fiscal year (not including cyclical and maintenance projects).

Activities already accomplished are listed below:

- Collected performance related data to improve estimation, requirements, and scope definition. Getting the project properly defined at the front end will improve Systems' ability to deliver high quality software on schedule;
- Provided comprehensive project management training to ensure managers have the knowledge to effectively plan and implement projects;
- Instituted the use of a standard project planning and scheduling tool, and a single-common repository for project plans;
- Instituted an automated system to document and track impacting issues and dependencies to mitigate their risks to timely project completion;
- Provided automated up-to-date project resource use information;
- Structured executive-level project status meetings and reports so that potential problems were communicated and addressed effectively; and
- Recruited skilled staff for critical IT shortages.

In addition to these accomplishments, the Office of Systems (OS) has also undertaken the initiative to:

- Institute an effective method of managing and assessing the impact of changes to requirements throughout the life of the project.

Quality Control and Quality Assurance

Quality control (QC) and quality assurance (QA) is an essential element of SSA's comprehensive systems engineering environment. *Product developers and line*

management use QC practices to ensure that products are reliable, maintainable, efficient and meet user needs. The SPI Team has developed a QA process to ensure that the development process is subject to continuous improvement. The process includes procedures for planning QA activities, conducting them and tracking non-compliance items to resolution. QA activities are incorporated into the project's Software Development Plan and related MSP schedule. The QA process has been implemented as part of the process rollout on software development projects.

Systems Validation and Verification

Systems Validation

Systems-level functional and acceptance testing activities of core programmatic, related management information and administrative software releases are performed using the Interactive Validation Environment (IVEN) which is housed in the Enterprise Software Engineering Facility. The environment is comprised of various automated processes that facilitate test design, the management, design, and development of test cases, and the management and execution test runs of target software releases. The environment enables SSA to satisfy application development and change control critical elements as defined by GAO and the SW-CMM and uses the Institute of Electrical and Electronics Engineers' Technical Independence Model for Testing Activity IV and V. SW-CMM requirements for test coverage are satisfied by the institutionalization of automated test coverage tools and practices. The environment provides for independent preparation of test data and independent test procedures as required by external monitoring authorities and the Capability Maturity Model. The environment supports systems testing for mainframe batch, CICS, client/server, and browser-based applications. An integrated validation database provides a test bed of master and transaction files as well as a collection of specialized test data generation and test data alteration tools. The environment also provides capabilities to conduct usability testing.

Systems Verification

Checkpoints in the project lifecycle have been established to ensure that software development items managed under change control are produced. A Systems Release Certification process verifies that all required project activities have been completed at appropriate project lifecycle stages before any software change can be implemented. Software test lifecycle products undergo verification using accepted IT industry methods including inspections and walk-throughs.

Web Testing and Validation

SSA's web-based applications operate in dynamic environments. Test tools complement the manual testing process. Test management and test automation tools increase test coverage and support an efficient validation process. In addition, increased test coverage may reduce the volume of problems discovered in the production environment. Test management tools are used to integrate requirements management with test planning, test scheduling, test execution, defect tracking, and

test analysis. Test automation tools increase regression test coverage and test data documentation.

Systems Life Cycle Management

The management of the systems lifecycle at SSA is currently being embodied in three documentation efforts:

- The Internet Project Lifecycle (I-PLC) has been developed and documented through the efforts of a Technical Work Group (TWG) comprised of representatives from Systems, customer and policy components. The lifecycle has undergone pilot testing by several Internet projects. Modifications have been made to the I-PLC based on the pilot findings and the lifecycle has been implemented on all future Internet projects.
- A flexible Standard Project Lifecycle (S-PLC) has also been developed and undergone pilot testing. The S-PLC is geared toward non-Internet efforts of longer duration and more complicated functionality. One of the techniques that this lifecycle envisions is an iterative systems development approach. In this case, there is a much closer relationship between the requirements definition and analysis and the design; the iterative process can help to streamline the lifecycle.
- The Collaboration Lifecycle has recently been published in PRIDE. Although all of the lifecycles advocate collaboration during business analysis and requirements development, this lifecycle expands that concept throughout the development and testing activities. Projects that follow the Collaboration lifecycle include:
  - Those in which OS and non-OS personnel are jointly developing code to be included with a release of an application; or
  - Projects that require no OS development, but may require consultative or investigative OS participation in areas such as capacity management, environmental testing and architecture.

The Collaboration lifecycle is intended to focus on communication required between development teams. It is also designed to reduce the project management activities that are required by non-OS developers, while ensuring that proper policies and procedures are followed and the project is properly tracked and managed.

These three methodologies constitute somewhat of a departure from the way SSA has designed and developed systems in the past, but build on the best practices of a highly qualified Systems staff. They embrace an interactive team approach to systems development using small integrated teams of people to develop requirements and code.

SSA continues to gain experience with its software development efforts and refines its processes and lifecycle methodology accordingly. The effort being conducted by the SPI Team will result in new or revised processes that are in sync with the guidelines established by the SEI.

Data Administration

SSA's current data administration processes and procedures are geared to support systems development and maintenance in a central file environment. The scope of Data Administration encompasses the service delivery and the administrative systems for the Agency. This environment is characterized by multiple systems that use and modify the same centrally maintained data. Data structure definition is managed by three methods: standard file descriptions, standard specifications that explain the data elements found in the files, and standard data names.

In addition, more global procedures are used in selected projects and involve using data structures as the basis for software system design. These procedures cover:

- Developing entity-relationship models;
- Assigning and defining the attributes of those entities;
- Using the attributed models to load project-specific dictionaries; and
- Integrating the project models into a comprehensive SSA view.

Disciplines include data modeling, information modeling, entity relationship attribute modeling, and repository-style databases.

Architecture Review Board

In 1999, SSA established the Architecture Review Board (ARB) to provide Systems-wide architectural governance to enable project review and feedback. This Board helps ensure that IT resources are used efficiently to support the Agency's vision and strategic planning through integration with the SSA's business requirements. The EA components that comprise SSA's IT architecture and design principles, as well as the technologies and standards that define each architectural component, serve as a basis for the Board's decisions.

The Board also supports legal mandates and Federal guidelines such as:

- The Information Technology Management Reform Act (ITMRA) of 1996, also known as the Clinger-Cohen Act (Public Law 104-106), which assigns agency responsibility for developing, maintaining and facilitating the implementation of an information technology architecture; and
- The Office of Management and Budget's document titled "Management of Federal Information Resources" (OMB Circular *A-130*, revised) provides guidance to Federal agencies on the development and implementation of Information Technology Architectures.

The ARB consists of personnel nominated either by Office of Systems Associate Commissioners or by the CIO. The Deputy Commissioner of Systems appoints the Board Chairperson. In addition to the Deputy Commissioner of Systems, the Deputy Commissioners of Disability and Income Security Programs, Human Resources, Operations, and Finance, Assessment, and Management, as well as the SSA Chief Security Officer (SSACSO), are represented on the ARB. The Board meets bimonthly, with additional meetings scheduled as necessary. All non-mainframe developmental projects are subject to review by the ARB.

Presentations made by Project Managers must include responses to a questionnaire developed by the ARB as well as Systems Enterprise Architecture documentation. The questionnaire reflects the different phases of review as envisioned by the Software Process Improvement (SPI) initiative. Architectural compliance and review by the ARB is an integral part of the SPI initiative. Further information is available at the Project Resource Guide (PRIDE) website and the ARB website.

Now that the additional architectures for data and applications have been developed, the ARB is examining itself and its role in relation to the governance of both data and application designs. As more experience is gained in these architectures, the management policies of the ARB as it relates to these architecture areas will be adjusted accordingly.

Usability

The Usability Center (UC) provides user-centered design and evaluation support service to project teams throughout the Agency. These services include, but are not limited to, documenting user requirements, testing usability and evaluating interface standards. Usability Center personnel work with the Agency's software development teams to ensure that a user interface is easy to use, intuitive, and enhances productivity. The Usability Center has incorporated the Electronic Meeting Facility, which has a staff of trained facilitators who use groupware technology for RAD/JAD sessions, meetings and requirements gathering.

Section 508 Compliance

Section 508 of the Rehabilitation Act of 1973, as Amended in 1998, requires that when Federal agencies develop, procure, maintain, or use Electronic and Information Technology (EIT), they must ensure that it is accessible to individuals with disabilities, unless it would pose an undue burden. Federal employees and members of the public who have disabilities must have access to and use of information and services that is comparable to the access and use available to non-disabled Federal employees and members of the public.

The Section 508 staff works with all components in the agency to assist in the development of procurement requirements for purchasing EIT that is accessible to individuals with disabilities. They manage an intranet-based Procurement Wizard to track all EIT procurements, and assist in determining if the EIT is Section 508 compliant or meets an exception that is allowable by law. The staff also tests and evaluates all of the applications that are developed in-house and works along with project teams and developers to provide consultation, support, and assistance in developing Section 508 compliant and accessible applications.

Configuration Management

Once a life cycle product is developed, reviewed, and approved it is subject to configuration management (CM) control. In order to emphasize the importance of management oversight of systems change, three levels of Configuration Control Boards (CCBs) exist. The higher-level board is chaired by the Deputy Commissioner for Systems (DCS), with the Associate Commissioners (ACs) serving as members.

This board is referred to as the Management Steering Committee with oversight and decision authority over all DCS improvement efforts and disputes between components. Subordinate CCBs exist in each of the principal Systems components. These CCBs are chaired by the AC of the component, with high-level managers serving as members. CCBs also exist at the project level with the authority to approve changes of a minor nature that do not affect commitments to the customers. Efforts are underway to ensure that the CM processes are compliant with the CMM by developing CM standards based on industry best practices.

Data Center Management

Network Customer Service Center

The Network Customer Service Center (NCSC) is a centralized, consolidated call center located in the NCC designed to provide expert technical assistance on initial customer calls. The NCSC staff is responsible for providing problem reporting and resolution services to a wide variety of SSA network customers at various locations throughout the world for numerous LAN/WAN devices, system platforms, COTS software, SSA specialized applications, and Assistive Technologies for Employees with Disabilities (EWD).

NCSC major functions and goals are to:

- Accept all types of initial trouble reports;
- Diagnose and resolve LAN/WAN problems on the initial call;
- Consult internally with more experienced NCSC engineers on the initial call, when necessary;
- Perform problem recordation, reporting, and documentation tasks;
- Provide close management of the Call/Problem handling and support process;
- Perform both real-time voice and electronically posted emergency notifications; and
- Implement and enforce specialized call center policies and procedures.

Other help desk functions contained within the NCSC include:

- Accepting and reviewing problem tickets created by other entities and assigned to the NCSC for vendor dispatch;
- Reporting problems to vendors and initiating vendor service;
- Customer follow-up to ensure that service was delivered and that the reported problem was resolved;
- Escalating service-related issues to vendor and SSA management; and
- Provide self-help intranet site for the customer.

National Network Service Center

The National Network Service Center (NNSC), also located in the NCC, serves as the SSA network monitoring and network operations component. The NNSC houses a variety of automated and manual monitoring systems providing proactive surveillance and exception alerts on SSA enterprise-wide systems. Enterprise systems and devices monitored include NT infrastructure servers, inter/intranet servers, critical application servers, and wide area network communications equipment. In addition, the NNSC is a 24x7 operation that serves as a backup to the NCSC and, as such, is capable of performing many NCSC functions.

Other services provided by the NCSC are:

- Monitoring support for the mainframe production environment;
- Providing specialized monitoring support for projects and pilot applications;
- Providing 2nd level support to SSA network customers for mainframe applications and issues involving CICS transactions, mainframe print traffic, and 3270 session connectivity;
- Problem report intake, documentation, resolution, and escalation; and
- Disseminating widespread outage and national scope, production degradation notifications.

Network Operations Center (NOC) functions contained in the NNSC include:

- Maintaining critical equipment at the Remote Operation Communications Centers (ROCCs) such as core router and switch equipment for backbone communications to the ROCCs;
- Maintaining SSANET communications circuits that service end-sites;
- Maintaining end-site WAN communication devices and LAN equipment;
- Performing 1st and 2nd level LAN/WAN problem determination and resolution steps; and
- Interacting with the WorldCom NOC to report, diagnose, and resolve network communication issues.

Capacity Management

Within SSA, capacity planning is an integral part of the Agency's overall IT planning process.

Methodology

The purpose of capacity planning is to identify the point at which existing resources can no longer support workload requirements. The resource requirement projections, which determine when additional capacity is needed, are based on usage analysis, including computing capacity, main memory, auxiliary storage devices, network capacity, and printing. Over the years the Agency has moved to awarding procurements with longer system life spans. IT procurement justifications have required longer-range projections. To suit this purpose, a well-defined approach for

developing long-range capacity requirement projections was developed. Now, because of rapid technology changes and more flexible procurement strategies, the Agency is moving away from longer procurement life cycles. For example, we are moving to a 3-year cyclical refreshment cycle for appropriate technology needs such as workstation/desktop infrastructures. In these technologies, capacity planning is driven more by obsolescence and market pricing factors.

The Agency's current process to forecast IT capacity requirements uses sophisticated analytical techniques to collect and analyze IT resource utilization data for individual workloads. Each workload is looked at periodically to determine its future requirement. Changes in requirements are based on changes in the functionality of the software, changes in the number of users of the software, and on actuarial data regarding the frequency of the software use. New workloads and workloads under development are estimated based on a comparison of relative functionality to existing workloads, and the rate at which the workloads can be processed by the new technology.

The Capacity Management for server platforms will focus on the measurement of utilization for the servers wherever they are located with the Agency IT infrastructure. Individual requirements will be established for each server based on the function that server performs and the volume of transactions which pass through that server.

Performance and Service Level Management

Well-performing automated systems are required to accomplish timely processing of SSA's programmatic and administrative workloads; SSA's Performance and Service Level Management processes are established to objectively monitor the critical infrastructure and workload performance of these automated systems. Critical infrastructure being monitored includes SSA's server and desktop infrastructure, the local area networks, the telecommunications network which links all SSA sites and connects SSA to the public, and the mainframe infrastructure hosting all of SSA's mission critical applications and resources. Most recently performance management processes have been established for the Electronic Messaging Infrastructure and the Internet infrastructure supporting www.socialsecurity.gov.

Availability, stability and performance are priority tenets in Performance and Service Level Management:

- **Availability** means access. SSA users must have access to SSA IT infrastructure service while office and telephone access is offered. Non-employee access (e.g. data exchange partners and the public) is required at times approaching 24 hours per day, seven days per week.
- **Stability** is the high availability overall, without patterns of even brief periods of outage. An outage may be loss of access or a decrease in performance that renders the service virtually unusable from the user perspective. Any interruption causes losses in productivity time much greater than the duration of the outage. When a member of the public is affected (e.g. prolonged

interview, incomplete 800 number contact), opinions of SSA services are influenced.

- **Performance** is the system's ability to process workloads timely. End user transaction response time is frequency monitored as part of the Service Level Agreements at SSA. Measurements of infrastructure utilization (e.g. CPU utilization and network traffic volumes) are key indicators of how the automated systems are performing. The performance measurements are monitored and reported on a regular (daily) basis. Trends and abnormalities are analyzed so that proactive planning and action can be taken to maintain the expected level of systems performance.

The basic elements of a Service Level Management are in place and Service Level Agreements exist for 23 of the major workloads. In addition, a generic service level agreement of common services exists for all major workloads. Routinely using information produced by systems operations, analysts assess the extent to which the agreements are met. When departures from the standards occur, management notifies the program component and acts to restore the service level. In the future, management will emphasize developing more highly automated and integrated monitoring and reporting mechanisms.

- The **Performance Management System** provides management and technical staff with the reports, tools and techniques needed to determine if performance objectives are met. The objectives are based on current operational objectives, applicable contract provisions, established service level agreements and current industry standards for system performance.
- **Service Level Agreements** are established for significant new system workloads. Development of these agreements begins during the operations planning stage and are well-underway prior to the implementation of the new system. They are finalized after production implementation. This permits actual user behavior, application tuning and in situ factors to be better reflected in the Service Level Agreements.

The Performance and Service Level Management System will be expanded to provide for online exception reporting to monitor and evaluate related individual devices, the overall system and Service Level Agreements. It will provide identification and resolution of problems through the use of early warning exception reporting and through automated interfaces with the existing change management and problem management systems. The Service Level Methodology is shown in Figure 9.

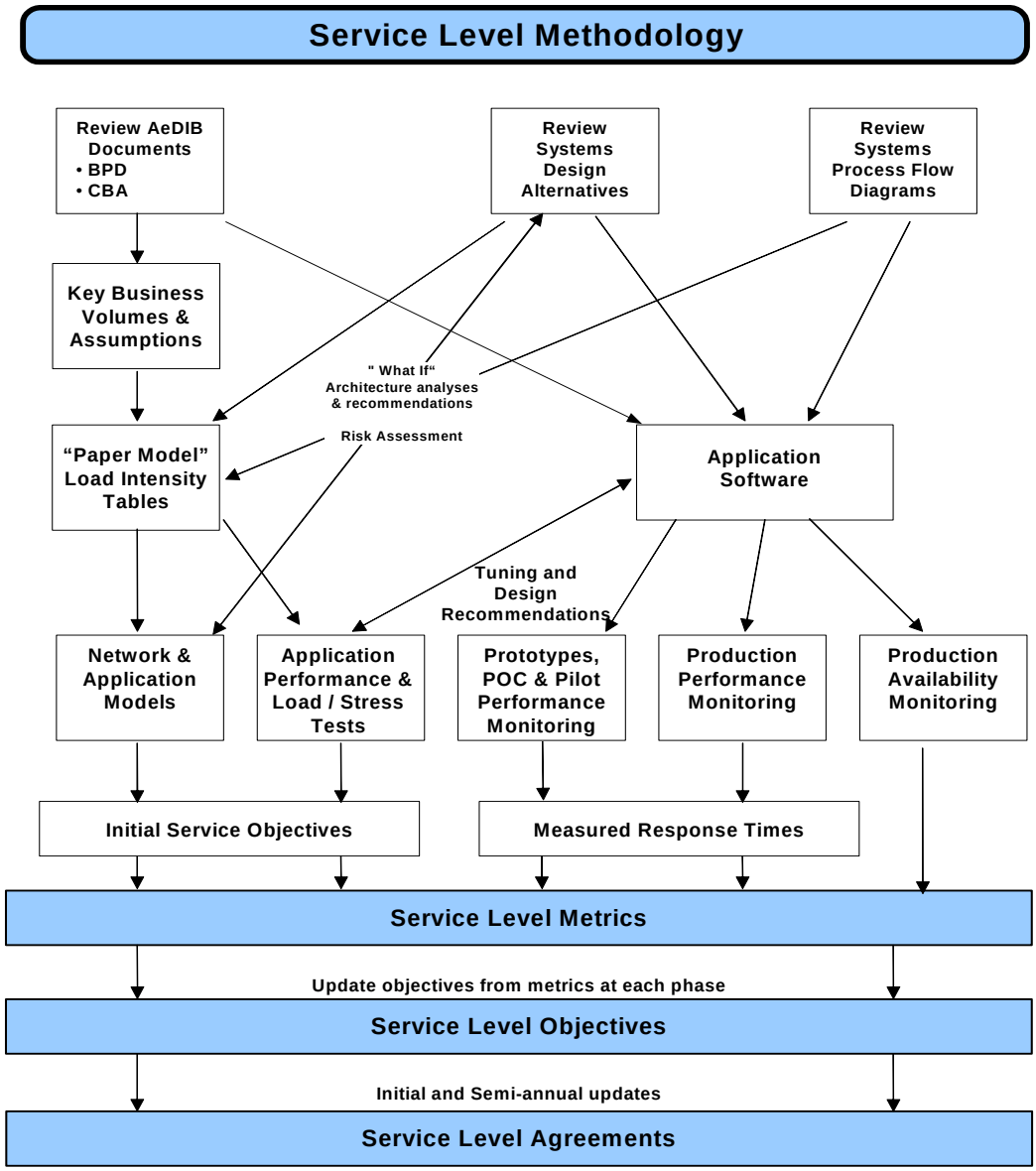


Figure 9: Service Level Methodology

The chart above illustrates the methodology used to develop Service Levels for an application. Key business functions and volumes are extracted from such application documents as the Business Process Plan and the Cost Benefit Analysis. Computer systems architecture designs and computer systems process flow diagrams provide information to the initial workload estimates in a "paper model," or Load Intensity

Table (LIT). LITs provide input to network and application simulation models, and the models project estimated response times. LITs also provide input to application performance test designs and application load/stress tests. The network and application models provide estimates of application response times. Application software must be developed before application performance tests and application load/stress tests can be conducted. Results from application performance tests and load tests provide tuning and design recommendations for the application while it is still in development. When the application software is deployed in pilots and production, the computer resources are monitored and response times measurements are made. Production availability monitoring occurs during pilot and production deployments. Service Level Metrics are a combination of estimated and measured response times from the above sources and Initial Service Objects. Service Level Objectives are updated from Service Level Metrics at each project phase. Service Level Objectives provide initial and semi-annual updates to Service Level Agreements.

Business Recovery

Business Recovery Computing Environment

The Business Recovery Computing Environment Project ensures that SSA will be able to quickly restore the National Computer Center (NCC) computing environment at an alternate site in the event of a natural or man-made disaster. This project supports SSA's mission by providing the computing resources needed to continue issuing checks, taking claims and supporting all the other services SSA provides no matter what may befall SSA's computing environment. SSA has continually improved its backup and recovery procedures.

- SSA maintains and updates the Disaster Recovery Plan for Computer Operations at the National Computer Center, which provides a high-level overview of the Agency's Disaster Recovery Plan for the Agency. This document does not contain sensitive information and is available for public distribution.
- SSA maintains an updated version of Technical Procedures for the Off-site Restoration of SSA's Computer Operations. This document contains sensitive information and its distribution is limited. Copies of this document are also stored at the Off-site Secure Storage Facility and the commercial off-site recovery facility.
- Offices of Systems components regularly review and update the Technical Procedures to meet current operating requirements.
- SSA maintains and updates the Emergency Response Plan for the National Computer Center. This document details procedures for the invocation of the Agency's emergency response. It contains sensitive information and is distributed on a limited basis.
- SSA maintains an Inter-Agency Agreement (IAA) with the General Services Administration for Disaster Recovery facilities and services. This IAA provides sufficient computing resources to allow for the ultimate restoration

of all SSA services should any type of event prevent the SSA from using the NCC.

- SSA identified critical workloads for immediate restoration in the event of a recovery event. SSA identified secondary, or deferred workloads for phase two restoration.
- SSA continues to identify and provide new hardware to support restoration of SSA's continually evolving computing infrastructure.
- SSA conducts annual recovery exercises at commercial off-site recovery facilities to insure the Agency's ability to restore its critical systems and improve the Agency's technical procedures for restoration.
- Equipment and facilities are in place to provide telecommunications between SSA offices and the recovery facilities.
- An internal Disaster Recovery test facility at the NCC is operational. This facility allows SSA to insure all data required to support off-site restoration is backed up and stored off-site. In addition, this facility provides an initial testing vehicle for technical recovery procedures, prior to the off-site exercise.
- SSA continues to explore options to speed the backup, recovery and restoration of computer operations.

Business Continuity and Contingency

An Agency workgroup conducted a business impact analysis, which involved the review and confirmation of critical workloads and priorities. The business impact analysis included a review of the current Agency Contingency (Disaster Recovery) Plan, as well as the Agency Strategic Plan, the Information Technology Architecture Plan and the Government-wide Study on Infrastructure. This last item is included to ensure the Agency has considered and included Government-wide considerations in its plans.

Applied Technology at SSA

Historically SSA has taken a pragmatic and conservative approach to technology innovation. The Agency has relied on mainstream market offerings that typically are also used in other government or commercial sectors, rather than undertaking solutions considered to be leading edge or early market offerings. Yet SSA has had to be a visionary because of the challenges it faces with the large size of our overall business, relative to our customer and partner base. SSA continuously drives the mainstream market place to expand their product sets. Demographic trends, such as growing workloads, the retirement wave and a changing workforce, force a commitment to new levels of technology and early market adoption in appropriate cases. The expansion of our visionary and early adoption strategy will be closely managed in light of SSA's long standing resolve to deliver reliable, secure and scaleable IT services.

With the establishment of future architectures as part of the Agency's EA, the Agency is now more proactive and disciplined when applying new technologies. Business architecture changes now drive application and infrastructure architecture changes. Such changes foster the need to adopt new technologies, but with specific applicability of the technologies to meet business needs.

This new, structured approach is being implemented as the Technology Infusion Process (TIP), with executive oversight provided by the Technology Infusion Board (TIB). The TIP collects information about the research objectives and potential benefits of the technology/business opportunities. The TIB, composed of representatives from SSA business organizations as well as the OCIO and Systems components, determines priorities of research and applied technology initiatives, presents these to the ITAB, and manages completion thereof. The TIB also disseminates information regarding technology efforts underway at SSA or the results from completed projects. The TIB makes recommendation regarding the next steps (e.g., expansion to pilot phase; shut down, etc.) for the project or technology.

The screen refacing initiative is a current example of the Agency's proactive approach to evaluating a new technology. Screen refacing is the presentation of existing mainframe character-based screens in a Web-enabled graphical user interface (GUI). The promise of this technology is improved usability and understanding of existing screen transactions with no application changes at a minimal investment in both time and money.

The evaluation process started with the identification of business needs and critical success factors. After executive management approved the business needs and critical success factors the Office of Systems (OS) performed applied research, consulting with industry experts and communicating with technology vendors, and created an OS-wide workgroup to guide the initiative. The workgroup determined that the technology warranted further evaluation, and identified a core set of requirements and evaluation criteria. Social Security then performed proofs-of-concept with multiple vendors and multiple products, validating that the technology satisfied the business needs, evaluation criteria and core requirements. After further refining the requirements and interviewing product reference accounts, the Agency is developing a working prototype to demonstrate the potential effectiveness to the end-user organization. The next steps will be determined by the results of the prototype.

Other technologies to be evaluated using this approach include:

- Enterprise Portal Proof of Concept,
- Master File Strategy Proof of Concept,
- Internal Use of Web Services Technology,
- Data Archiving Proof of Concept, and
- Management Information Data Mining Proof of Concept.

Technology Trends

Technology is evolving in many key areas. In the communications environment:

- Bandwidth expansions continue;
- Expanding internet and other mobile technologies will lead to more customer controlled interactions; and
- Interagency data exchange will grow as a result of communications advances.

In the area of computing and storage capabilities:

- Server and desktop power continue to increase, allowing for implementation of higher levels of automation;
- Data storage continues to grow at significant cost savings;
- A need will grow for greater levels of operating system support; and
- The concept of grid computing (where computations and information sharing can occur across geographically dispersed environments) will mature, enabling better usage of computing power and data.

The shifts in communications, computing and storage capabilities will allow for greater geographical independence and likely lead to implementation of systems that would then be better protected in event of disaster scenarios. Moreover, citizens and partners will expect service at any time and from anywhere. Expected enhancements to speech recognition and digital pen/ink technologies will offer additional interface channels into IT systems.

Security technologies will continue to develop. The security challenge will be compounded by technology offerings via the Internet or other communications channels. Enhancements to identity systems such as PKI potentially could lead to higher levels of self-service business offerings. Biometric technologies will likely prove useful for our internal employee access control mechanisms.

With the increased focus on service delivery to the public, and partnering with government agencies or the commercial sector, the technology of application design and coding is expected to change. Integration of exiting and future services will be paramount. Webservice technology potentially will facilitate this evolution. The new software development technologies will also grant additional powers to traditional users of IT services. They will be able to create their own IT services somewhat independently of the traditional software development model. This shift will again force an emphasis on integration and management technologies.

The software development technologies will also lead to advanced client interface metaphors that will improve the information supply and elevate human-computer interaction to a "pull" metaphor, rather than the "push" approach of earlier decades. Public expectation will demand that information be available "their" way and no longer "our" way.

Workflow technologies will be enhanced to integrate with information and document management architectures. Movement to an all-electronic data is expected. In the transition phase, as the reliance on paper-oriented media continues, the development of electronic tags, very small devices that store data that can be read or written to wirelessly, could enhance existing systems that rely on traditional bar-coding.

With the increase in collection and maintenance of information, analytics (the process of analyzing data) will become more important. Unstructured data analytics will become more prevalent. Analysis techniques increasingly will address not only structured data, but also text, audio and video information. Advances in this area can lead to a better understanding of business processes or clients, with ultimate efficiencies realized when information is acted upon timely.

The Office of Systems is cognizant of these enhancements and innovative developments in the IT field. It will continue to coordinate and research future technology and its impact on SSA systems in a structured and disciplined manner.

Furthermore, to assist the Agency in understanding and exploiting the development of an Internet-based input channel which would allow SSA clients to deal directly with the Agency's automated systems (rather than an SSA employee as intermediary), OS has established the Electronic Technology Center (eTC). The eTC is a facility specifically designed to demonstrate and evaluate technologies in an Internet environment from the client's perspective. The eTC has been opened for business since September 2000.

The eTC consists of a four-room facility configured with numerous servers, workstations, networking equipment, and a state-of-the-art demonstration room. The entire facility operates on an isolated LAN with a separate Domain Name, Internet Service Provider, and IP address scheme. This enables client connectivity to the Internet through a special SSA firewall and prevents any possible access or damage to SSA's production systems. Through its equipment and connections, the workstations can be configured to simulate data exchange from a residence, school, library, etc.

Chapter 7: IT Human Resources Management

Commitments to SSA Employees

SSA's IT Human resources include about 3600 employees, most of whom (about 3000) are organizationally located in the Office of Systems. The remaining employees (more than 600) are located throughout the rest of SSA's organization, with more than half of them in the Office of Operations.

SSA provides employee training and development at all grade and occupational levels. It ensures that employees are properly trained and provides for opportunities for personal and professional development. SSA is also committed to maintaining a work environment that includes accommodations for employees with disabilities such as TDD and closed captioning services for the hearing impaired. For the visually impaired, PC software enlarges text and graphics on large monitors and additional hardware "readers" are provided to transfer images from hard-copy material onto the PC screen.

Since the early 1980s, Systems has invested considerable resources in building a staff that has the necessary knowledge, skills, and abilities to achieve modernization of SSA's information systems. Time has shown that this has been a wise investment. With advances in technology proceeding at an ever increasing pace, SSA remains committed to maintaining a highly skilled and motivated workforce through continued training, staff development and an effective work environment.

Toward that end, Systems has developed and implemented an IT Workforce Strategic Plan. In order to maintain and enhance the capabilities of its IT staff, the organization implemented a skills inventory survey. The survey assessed the current base of knowledge and skills, identified future requirements, and determined the gaps in skill needs. Workforce strategies and plans have been developed for hiring, training, and professional development to fill the gap between requirements and current staffing, and are an integral part of the IT Workforce Strategic Plan. The information that follows is consistent with that plan.

The Staffing Picture

The Office of Systems talented workforce includes almost 3,000 technical employees who are skilled in a wide variety of computer-related specialties. These skills range from the basic ability to operate a personal computer to an in-depth knowledge of SSA's mainframe operating system. Other employees are skilled in the intricacies of the Internet, relational database management systems, and data communications in

LAN environments. Technical employees are adept at using a structured methodology for the phases of the systems development life cycle and complying with appropriate standards and guidelines. The supervisor to employee ratio continues to be 1:11.

In FY 2003, the Full-Time Permanent (FTP) attrition rate was 5.8 percent, or 165 losses. While more employees in the workforce have begun to reach eligibility for Federal retirement or have accepted the Agency's early-out retirement options, the number seeking computer system positions in the private sector remains low. Approximately one-half of Systems' yearly attrition rate is the result of employees accepting regular retirement. The Office of Systems has been able to offset these losses by targeting most of its replacement hiring authority towards the recruitment of highly skilled technicians from private companies or recent computer science college graduates. Systems also has used nationwide recruitment efforts to improve its workforce diversity.

The Office of Systems remains proactive in intensifying its recruitment activities. Current projections indicate that Systems is at the beginning of a retirement wave that will witness 43 percent of its workforce, or 1,235 employees, reaching retirement eligibility by 2007. For planning purposes, Systems is forecasting that the number of employees accepting regular retirement will steadily grow from an actual 2.4 percent of the organization in FY 2001 to over 4 percent by 2007. These projections indicate a potential loss of nearly 500 FTPs over this five-year period, along with the experience, knowledge, and technical skills of these employees.

The Office of Systems recognizes that losses of this magnitude, in such a short period of time, cannot be offset by an intensified recruitment effort alone. It must be coupled with strategies being implemented in the workplace, such as succession planning, establishing best practices, and improving the rate of retention.

The figure titled *FY 2002 Losses and Hires* highlights the placement of Systems' FTP hiring by workload in FY 2002. The majority of the FTP hires (119 of 142) in FY 2002 have been assigned to the Agency's highest priority initiatives.

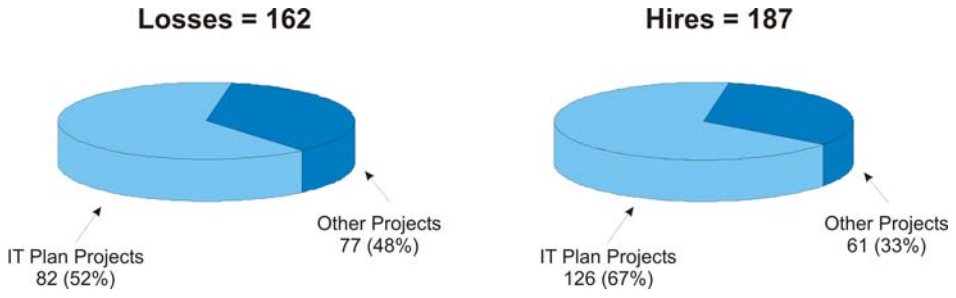


Figure 10: FY 2002 Losses and Hires

The Office of Systems workforce distribution in FY 2003 is depicted in the figure titled *FY 2003 Estimated FTEs*. These resources were used to provide ongoing systems and network maintenance support, and to carry out the Agency's critical IT

Plan and reengineering initiatives. Future resource estimates will be adjusted to reflect the impact of legislative changes or new initiatives as a result of new legislation. In addition to the above in-house resources, Systems employs over 500 contractor personnel. While contractor personnel will continue to support some workload functions, the need to recruit and maintain a well trained in-house technical staff will continue.

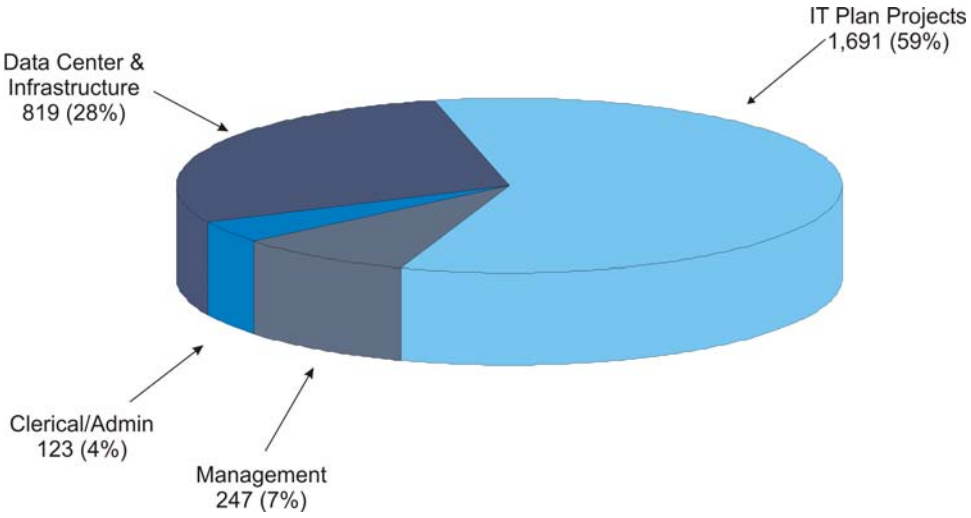


Figure 11: FY 2003 Estimated FTEs

Future Skill Needs

The future skills needed by SSA's Systems' workforce stem from environmental forecasts and assumptions, and the implementation of the target architectures. As a result of the intensive training program in place, Systems employees have achieved a proficient level of competence with desktop software and the Microsoft Windows workstation, server and network operating systems. A cadre of LAN and e-mail administrators has been trained in each Systems component and the development of employees as Microsoft Certified Systems Engineers has been supported and promoted. As new versions of the Microsoft desktop and server operating systems and Microsoft Office Suite of applications are released, we continue to ensure that Systems employees are trained in the skills needed to use this new technology in the most effective and proficient way possible. Additionally, as we continue to move away from the token-ring environment, Systems employees will need to improve their skill in using the Ethernet environment. As the mainframe environment is upgraded with new versions of the mainframe operating system, Systems employees will be trained to use the new features and capabilities of the operating system.

Environmental forecasts drive the planning needed to recruit new personnel and to train the SSA workforce in new skills.

Another key skill needed to achieve the projected environment is that of distributed application program development. SSA needs programmers who are skilled in using modern software and software engineering tools. Employees need to be skilled at working in both the mainframe and cooperative processing environments. Skill in Internet/Intranet web page design and application development is another important emerging skill area. As Web browser technology has evolved, Internet/Intranet usage has skyrocketed. The Intranet is an ideal vehicle for disseminating information to and collecting information from employees. The Internet is also now being used as a major source of program information for the public. Use of the Internet/Intranet will expand significantly. Systems must increase the pool of staff with Internet-related skills to meet the Agency's vision for customer service. Video conferencing and multimedia demonstrations are now being used for meetings, presentations and training throughout SSA. This requires expertise in multimedia development tools and media design concepts. Other areas that will likely take off in the upcoming years are Voice over IP and wireless networks. Systems employees will need to upgrade their skills in these areas in order to put SSA in the best possible position for the future.

Distributed systems will increase network complexity and will require SSA to turn to sophisticated Local Area Network/Wide Area Network design tools. This requires skill in understanding network traffic flows, and modeling these flows in network design tool languages. New skills for distributed systems network design will enable SSA to make a smooth transition into using the full potential of the IWS/LAN as well as the WAN environment.

Future Skill Areas	
ALC	Network Technology
COBOL/CICS	Object-Oriented Programming
Communication Design	Open Systems Interconnectivity
Computer/Network Security	PC Support and Maintenance
Configuration Management	Project Management
Data Modeling	Quality Assurance
Data Warehousing	Relational Databases
Database Administration	Software Testing
Distributed Application Development	Software Validation
Electronic Business	Solaris
Electronic Mail	Systems Analysis and Design
Enterprise Support	Team Building
GUI Development Tools	Technical Documentation
Image Processing	Voice over IP
LAN Management	WebSphere
Multimedia	Web Application Development
Network Management	Wireless Technology

Table 6: Future Skill Areas

Table 6, *Future Skill Areas*, shows some of the more important skills that will become even more important over the next 5 years. SSA is focusing on these future skill areas to support the target environment. It is financially beneficial to train existing employees in newer technologies. *A significant portion of technical training is devoted to training existing employees in new skills.* Periodically, SSA needs to

recruit experienced employees with highly technical skills to deal effectively with new technology.

MANAGEMENT SKILLS

Most of SSA's Systems managers are technically oriented, having come up through the ranks of the Systems organization or from technical jobs in the private sector. Some have SSA programmatic backgrounds. Most possess strong supervisory and management skills, and most are trained to be professional project managers.

Systems managers must stay current with new technology and be aware of new and emerging areas of technology to better lead their technical personnel. Because of the limited amount of hiring that will be done, managers will have to adopt new and innovative methods of training and motivating their staffs to perform at higher levels of productivity.

Technical skills are critical for most employees, but functional skills such as planning, staffing, organizing, delegating and communicating are critical for managers. Some of the new skill development for managers is focused on improving leadership, project management and interpersonal communication skills.

In January 2003, Systems began a Management Leadership Curriculum for middle and senior managers. The curriculum includes skill areas necessary for effective management and leadership such as planning, problem solving, communicating, presenting and motivating management teams.

Currently Systems has implemented an initiative to develop a Team Leader Curriculum. This curriculum will cover skills that team leaders will need to guide their teams effectively.

Over the past several years, Systems has expended considerable effort training technical employees to function in the cooperative processing environment. Systems devotes an equal amount of effort to training its software development Project Managers. The January 1999 report of the Government Chief Information Officers Council states that the largest skills gap in the information resource management arena occurs in the area of project management.

Systems has instituted a curriculum of professional courses that trains managers on the best project management skills and techniques. The courses selected contain proven techniques from *the Project Management Book of Knowledge*. The courses cover basic project management skills along with team building, estimating techniques, risk management and project tracking. This training will ensure that software development Project Managers in Systems are skilled in industry best practices.

A current Systems-wide initiative will require additional training for virtually all Systems managers. *The Systems Process Improvement (SPI) initiative is a major Systems effort that uses the Capability Maturity Model (CMM) as its base infrastructure.* CMM is a five-level industry standard process improvement methodology. CMM, as well as other initiatives under the SPI umbrella, will guide

the new development and tailoring of project management and project team training. This effort will be extensive.

Plan for Meeting Future Skill Needs

SSA's vision of the future anticipates that technological changes will continue to occur at a dramatic rate. The introduction of even more advanced technology requires innovative thinking, a new way of viewing processes, and proficiency in using new products. In addition, predictions are that there will be too few people trained in information systems to satisfy growing needs in both the public and private sectors. The gap between the demand and the supply of skilled professionals is growing. These factors force SSA into competition with private industry for retaining skilled systems personnel and challenge SSA to develop current employees to their full potential.

Continuing attention to the following will ensure that skills needed to support the target architecture are maintained:

- Skills and skill levels needed;
- Training;
- Career paths;
- Employee development;
- Mentoring and coaching;
- Rotational development; and
- Retention and recruitment.

One mechanism used for employee development is the Systems Rotational Program (SRP), which has been in place for over 10 years. Systems employees ranging from grade levels GS-3 to 13 are selected each year to participate in the SRP. Participants choose two or three assignments in other components that they believe will enhance their knowledge and experience. This gives them a broader perspective of Systems functions and improves job performance on return to their home component.

SSA is committed to providing its employees with training, development and career advancement opportunities.

Due to budget constraints, outside hiring to meet specialized systems personnel needs will continue to be limited. Basic skills training is offered to help prepare lower-graded employees for advancement. Special attention is given to developing career paths for employees who have been in clerical or computer equipment operator positions for a number of years. Systems has established Computer Assistant and Computer Systems Analyst trainee positions at the GS-5 to GS-7 level that are used to promote staff who demonstrate an aptitude for computer skills.

Systems recognizes the need to give entry-level technical employees a foundation of knowledge about their position, organization, mission, projects and responsibilities as well as other information to help them comfortably and productively work in the Systems environment. Systems components match seasoned employees with new employees for mentoring and coaching. Systems believes that mentoring will play an

important role in passing on business knowledge and developing needed skills. A Mentor Guide is under development and will be available to all mentors. A seminar on Mentoring for Systems mentors will be developed once the guide is approved. Currently, guidance on mentoring for mentors and mentees is included in post recruitment briefing sessions.

As part of a continuing effort to develop strategies to satisfy skill needs, Systems conducted a management study in 2002 of the current skills of Systems employees. An online application was developed to gather data on employee skills from branch managers and report on skills at the aggregate level.

Based on Systems' initial findings and the data collected, the decision was made to enhance the tool for future use. As a result, the application was modified to capture information about retirement eligibility, and the list of competencies and skills surveyed was expanded. Skill levels (basic, intermediate and advanced) were added to provide a more accurate picture of the breadth and depth of skills possessed by employees.

More importantly, functionality was added to capture future skill needs in addition to current skills. Mangers are asked to identify their future (within 3 years) skill needs based on anticipated workloads and process and technology changes. The data collected on future needs along with the data in the skills inventory can be used to generate a variety of gap analysis reports.

Another Systems management survey was conducted in 2003 with the following objectives:

- Take a snapshot of the competencies and skills of Systems technical employees
- Collect information on future skill needs
- Perform a gap analysis between current skills and future skill needs
- Track skills lost due to retirement
- Use gap analysis results to improve Systems' human capital strategy

The data collected will be further analyzed and evaluated in light of other information such as attrition rates and contractor support. The resulting comprehensive gap analysis will be used to develop appropriate IT workforce planning strategies. Systems plans to update the skills inventory and future needs data annually to better link staff requirements and workforce strategies.

Employee Training

A top training priority is to prepare Systems employees to perform in the constantly evolving Information Technology environment. *The Systems Technical Training Program (STTP) provides a flexible approach for maintaining high skill levels for both technical staff and managers.* During the last several years, the infrastructure of SSA's computer systems has transitioned from a primarily mainframe environment to a cooperative processing environment with increased use of the Web. The STTP has been continually modified to respond to changes and to train Systems employees

in the concepts, software, hardware and tools of the new environment. Courses related to the cooperative processing environment were added to the set of technical courses offered to Systems employees. These courses focus primarily on Microsoft Windows and the Microsoft Office suite of products. Additionally, training programs in developing web applications and in working in the DB2 environment have been developed and provided to employees. A series of courses covering security-related topics for Cisco, Microsoft, Solaris, UNIX, the Internet and the network were offered to employees, and the STTP was also augmented with courses related to Section 508 and accessibility. Most of the over 400 classroom training courses provided by the STTP to Systems employees in FY 2002 taught skills related to the new environment.

Additionally, an analyst training curriculum has been developed to provide a technical foundation and appropriate skills for Systems' analysts. The curriculum provides training in basic information technology concepts, basic programming skills, a methodology for planning, analysis, and requirements development, JAD techniques, the Systems environment, concepts related to data modeling, validation, usability and SSA's business processes.

Systems has three training facilities equipped with 16 to 20 personal computers and LANs to accommodate the increased need for training. Additionally a new facility dedicated to WebSphere training was recently constructed. These facilities continue to be in constant use for hands-on training courses related to the new environment.

The primary purpose of the STTP is to leverage the cooperative processing environment and associated technologies to provide state-of-the-art training and training information services. Carried out in a client-focused manner, the program enables employees to be more responsible for their training and development. Using a variety of delivery approaches, the STTP provides the necessary technical training on an ongoing basis. As a result, the STTP is dynamic—ever improving to meet the needs of a changing environment.

Systems training comprises both broad-based concepts of the new ITA environment as well as specialized technology applications.

The newer technologies demand intensive training, which includes courses that build the conceptual foundation for the new environment before presenting tool—or product-specific training. The STTP defines a set of core courses for all Systems employees. These core courses present a conceptual picture of the working environment as well as teach how to use several basic PC software packages with an emphasis on Microsoft Windows and the Microsoft Office suite. Technical staff receive an additional set of core courses that provides a more technical introduction to the environment.

With a well-developed conceptual foundation firmly in place, training then concentrates on building specific skills. A set of technical skill categories, or areas of competency, has been defined and courses required for each competency area have been developed. The competencies include:

- Analysis and design;

- Computer security;
- Database technology;
  - DB2 Administration;
  - DB2 Application Development;
  - Oracle Administration; and
  - Oracle Application Development
- Development languages and tools;
- Mainframe Application Development and Operations;
- Network technology;
  - Cisco-Related Administration;
  - Microsoft Windows Administration;
- PC Application Development;
- PC and Workstation Support and Maintenance;
- Project Management;
- Technical Management; and
- Web Development.

Employees will be trained in those specialized hardware and software processes and tools that support a particular job or project.

The STTP will continue to be enhanced and training efforts will be redirected as needed to optimize the information technology infrastructure and leverage the IWS/LAN investment. Continuous re-education of Systems employees has become a necessity. A Presidential Executive Order signed on January 11, 1999, establishes a government-wide policy of continuous education for employees involved in information technology services. This has been the policy of the Office of Systems for almost two decades. Systems' technical training program and educational opportunities ensure that highly skilled professionals maintain the high standards of public service that defines Social Security today.

Systems employees can stay abreast of the latest hardware and software technology developments through various technical research services. These services include access to select web-based resources and analytical reports that highlight industry projections and trends. In addition, access to technical books-online is currently being offered to Systems employees.

E-Learning

E-Learning is an online training delivery system that offers over 350 web-based technical training courses to employees at their workstations. E-Learning, which was initially a local area network (LAN)-based application in 1995 and a server-based application in 1996, is now web-based and is available to all SSA headquarters employees in Baltimore, as well as field office employees throughout the United States who may be interested in Information Technology (IT). E-Learning courses

are primarily designed to enhance the technical skills of IT professionals. Some examples of the skill categories available through E-Learning include:

- Applications development;
- Cisco;
- Communications and Networks;
- Computer security;
- Database technology;
- Internet Development;
- Mainframe Software and Tools
- MCSE curriculum;
- Microsoft desktop applications;
- Project management; and
- Windows curriculum.

The expansion of E-Learning nation-wide has contributed to the ability of information technology professionals, beyond the Office of Systems, to take advantage of quality training at their workstations.

E-Learning enables employees to take *just-in-time* training when it is needed, supplement their classroom training as needed and learn at their convenience. Systems will continue to modify and expand the library of Web-based courses to correspond with the Agency's current technological needs. Systems will continue to research the use of multimedia technology (e.g., audio, video, and speech recognition) for E-Learning as the computer architecture allows. This research is of particular importance relative to providing technical training to employees with disabilities. Given such increased, flexible, and easily accessible training opportunities, employees will be encouraged to develop a habit of continuous education in keeping with taking more responsibility for their own training and self-development.

Graduate-Level Training Program

The Graduate-Level Training Program (GLTP) was established in 1989 to provide experienced Systems professionals in key positions of critical need, with the opportunity to expand their technical knowledge and skills in areas directly related to their function at SSA. These areas include client/server technologies, database management/administration, information assurance, information technology management, operating systems, software design and development, systems analysis, telecommunications, or web applications development. The program is designed to give employees high-level academic training to ultimately support and promote continued growth and improvement of Systems.

The GLTP continues to be an important element of the STTP. Based on the training budget for each fiscal year, three to five employees enroll, full-time, in an information systems or computer science program under the Office of Systems'

GLTP. *Employees enroll in specified programs at local academic institutions such as Johns Hopkins University, Loyola College, the University of Baltimore, and matriculated programs at universities in the University System of Maryland.* After a year of graduate-level study, participants return to work with knowledge of new techniques in systems design and development, and new ideas on how to manage in an environment that relies on automated work processes. This program also gives Systems employees an opportunity to interact with their private sector counterparts in an educational setting, helping them to bring new perspectives to their jobs. Several former program participants are now Project Managers for major software redesign projects.

Recruitment Strategy and Employment Incentives

Recruitment Strategy

As the Agency faces the challenges of a new millennium, our goal is to address information technology challenges by developing a strategic approach to recruitment that enables Systems to obtain needed technical skills and competencies in our human capital resources. Advanced planning is critical to this process. The Office of Systems has implemented a Skills Inventory Survey to assess the current skills of our technical employees, project our known future skill needs and to assess any projected gaps. Having a recruitment strategy and recruitment staff focused on workforce strategies and recruitment, and on meeting skill needs, enables us successfully to target our efforts in today's increasingly competitive IT market.

To meet the future technical needs of our Agency, the Office of Systems must maintain the ability to recruit and retain both entry-level and experienced employees. The Deputy Commissioner for Systems established a Recruitment Staff, which reports directly to his immediate office to emphasize the critical nature of recruiting qualified personnel who meet the high standards of the Office of Systems. By providing focused attention and financial resources to this staff, we can achieve more effectively our human capital resource strategy as defined in our IT Workforce Strategic Plan. As part of that strategy we continue to refine our recruiting process and best practices to ensure success in sourcing talented IT candidates to meet the challenges of SSA's information technology needs.

Our Recruitment Strategy includes several initiatives to optimize recruitment and enhance our current successful retention efforts:

- Forecast recruitment needs in advance;
- Develop hiring goals;
- Implement a more aggressive advertising/marketing campaign;
- Utilize a comprehensive college recruiting and entry-level recruitment plan;
- Initiate an internal SSA recruitment effort to attract SSA employees with SSA program knowledge;

- Design specific approaches for obtaining the hard-to-find technical skills, i.e., expanded use of recruitment bonuses, higher than minimum salaries, increased advertising budget;
- Increase use of external and SSA Developmental programs and the Student Career Experience Program as recruitment tools for future Systems employees.

Compensation

Attracting new personnel with the technical skills required by the rapidly changing IT environment has become increasingly difficult. Analysts predict the labor market will remain highly competitive so the recruitment challenges SSA presently faces will remain an issue the organization will face for the foreseeable future. As baby boomers begin to retire and private industry salaries continue to rise, skilled IT workers will be at a premium.

To assist Federal Agencies in their competitiveness, the Office of Personnel Management has attempted to address pay comparability with a new IT pay scale and hiring incentive. Good recruitment, which entails getting the right candidates with the right skills in the door, involves more than just money. It involves exposure, timing, a sales pitch utilizing the right materials and finally a competitive benefits package.

One of the functions of the recruitment staff is to monitor IT compensation in our geographical area by survey data and by personal survey at job fairs. To enhance our efforts to meet the competition and market, we utilize recruitment bonuses, retention bonuses and above minimum salary offerings. We market our employment opportunities at job fairs, USA Staffing, and with newspaper ads. We have fully utilized quality promotional materials at job fairs and on university campuses and have developed a website to advertise Systems positions, the organization and SSA benefits. In addition, we work to increase our exposure by creating a strong presence on University campuses and in the experienced hire job market.

Entry-Level Commitment

Because we recognize that OS will be facing a substantial retirement wave in the next 5 -10 years, we give conservative but focused priority to our future needs by specifically targeting FTEs for entry-level hiring. In each of the past 4 years, we have set aside 25–30 % of our potential hires for entry-level positions. We utilize various hiring authorities to recruit entry-level employees including: the Outstanding Scholar, the Administrative Careers with America postings, the Federal Career Intern Program, Veterans Readjustment Act Appointments and Schedule A appointments for persons with disabilities.

Career development for these new hires is critical to our success. Most entry-level hires are placed in career ladder positions with extensive training outlined in Individual Development Plans that focus on developing technical skills related to the specific job assignment. Additionally, entry-level hires attend group training in a set of core courses covering soft skills, SSA's business processes and SSA's computer

environment. In the last 3 years, the Office of Systems has moved to target more of our entry-level hires to college graduates who have Information Systems (IS) or Computer Science (CS) degrees. We recruit these talented individuals with our commitment to their training and personal development. By targeting IS/CS majors, we are able to better tailor individual technical training the candidates need to perform well in their positions. IS/CS candidates are more valuable to us because of the specialized skills they already possess thus enabling us to focus our training and development dollars on their personal technical training needs directly related to their positions. Our investment is better spent and we are showing strong commitment to their personal skill and competency development. We recruit most IT/CS candidates utilizing above minimum salary offering because of the special skills they bring to the Agency. We continue to strive to be the "Employer of Choice" for graduating students in the IT field.

Recruitment Focus

Our staffing plan now includes the option of hiring both experienced and entry-level employees at any time during the year rather than just in the last quarter. To meet our need for quality entry-level candidates throughout the year, we attend job fairs in both the Spring and Fall. Many of the Fall job fairs focus on Information Technology. In addition, we target schools nationwide to increase our diversity. To improve interviewing of out-of-state candidates we incorporate some distant on-site visits and we are exploring the use of video interviewing to increase our geographic reach to more schools and to reduce increased costs. Attendance at job fairs is instrumental in establishing a strong presence on the university campuses. Further, it fosters a strong working relationship with university career services staff and allows us a unique opportunity to market our organization directly to students and to collect candidate resumes.

We anticipate that Internet usage will continue to grow, with an even greater emphasis on Web recruiting. In addition, the anticipated shortage of new graduates with diverse cultural backgrounds in computer science and related fields makes college recruitment programs important to the hiring strategy.

Workplace Incentives

SSA has numerous workplace incentives in place, which we highlight extensively in our marketing of System's employment opportunities. One of the most valued by today's job seeker is work tour flexibility. We market flextime, and choices between two alternative work schedules (AWS-5-4-9 and 4/10) as opportunities to vary a work schedule to adjust a person's work tour to his/her lifestyle and the contemporary workforce. Other valued benefits include: our onsite fitness center, credit union, employee association, post office and onsite day care centers at the main complex and Metro West building. These services augment the benefits for our current workforce as well as provide incentive to prospective employees.

Support Services and Competitive Sourcing

SSA will have a continuing need to contract for IT support services. In general, SSA serves as the systems integrator for most developmental projects and operational functions. However, skilled contractor resources are often needed to supplement SSA's staff because there continues to be a critical shortage of experienced, technically qualified personnel available to meet the Agency's needs for new programmatic and administration/management information software applications while simultaneously maintaining current systems. The SSA workforce is not expected to increase significantly in the foreseeable future; however, the workload continues to grow. Even with the stated ASP goal of recruiting, developing and retaining a high-performing workforce, maintaining appropriate skill levels will require supplementing the SSA personnel with contractor resources.

Furthermore, many of SSA's employees are eligible to retire in the next five to ten years. According to the ASP, up to 59 percent of SSA's current workforce will either retire or leave the Agency for other reasons. The retirement of key systems personnel will have an adverse impact on the development and maintenance of programmatic and administrative/management information systems. In addition to the loss of personnel due to retirement and attrition, SSA can expect to face the challenge of training current employees in the new technologies planned for implementation during this timeframe and recruiting new staff with highly specialized skills. Federal agencies could find it difficult to compete with salary levels offered in the private sector. Technical changes and new technologies require new innovative thinking, proficiency using new products, and new techniques. SSA is in competition with other Federal agencies and private industry to hire and retain employees skilled in these new technologies.

Technology services are required to: 1) accomplish Agency strategic initiatives; 2) provide full software life cycle support; 3) provide technical support for software engineering and database activities; 4) perform analytical and research activities; 5) conduct cost benefit analyses; 6) conduct independent reviews; 7) support software process improvement and software engineering management activities; 8) provide highly specialized skills related to current and advanced technologies not available to SSA; and 9) transfer private sector technical knowledge to SSA.

In addition, the President's Management Agenda has established Competitive Sourcing as one of five management initiatives. A number of Information Technology functions are commercial in nature. Over the next few years SSA expects to conduct competitive sourcing studies under procedures of the newly revised OMB Circular A-76. The results of these studies may change the percentage of work contracted. That percentage may go up or down depending on the results of the competitive sourcing studies.

Chapter 8: Budget Perspective

This chapter of the IRM Plan provides a brief discussion of SSA's overall budget and the major areas in which funds are spent.

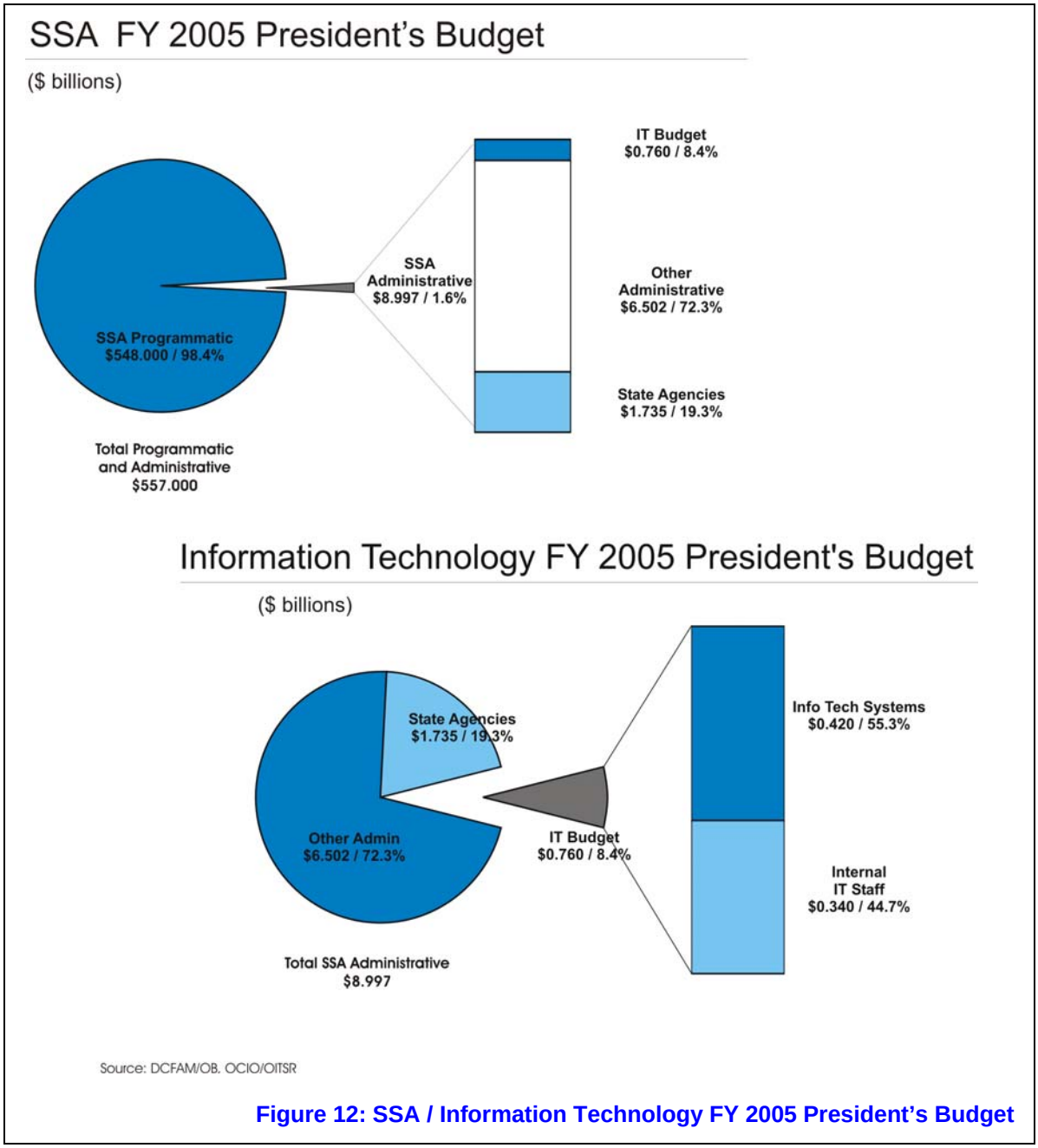


Figure 12: SSA / Information Technology FY 2005 President's Budget

The FY 2005 President's budget, depicted in Figure 12, includes almost $9 billion for administrative expenses. The Information Technology (IT) budget, at $760 million, represents 8.4 percent of the Administrative budget. Approximately 55 percent of the IT budget, or $420 million, is allocated to ITS spending. (In addition to the new budget authority of $420 million, we will have $45 million of anticipated carryover from prior year unobligated balances and $3 million in reimbursables for a total of $468 million in ITS spending. This amount is reflected in Figure 13.) ITS spending supports investments in strategic automation initiatives, financial management systems, IT infrastructure, telecommunications, office automation, enterprise architecture and IT security. The remaining 45 percent, or $340 million, is used for employee salaries, benefits and related expenditures.

The Budget Outlook

The chart below depicts the budget outlook for the upcoming years. As major new systems supporting the disability process are rolled out and implemented across the nation, the infrastructure costs to support the new systems will increase. If the total IT budget is to remain level or is only slightly increased, this will constrain the amount of money that can be invested in agency priorities in the future.

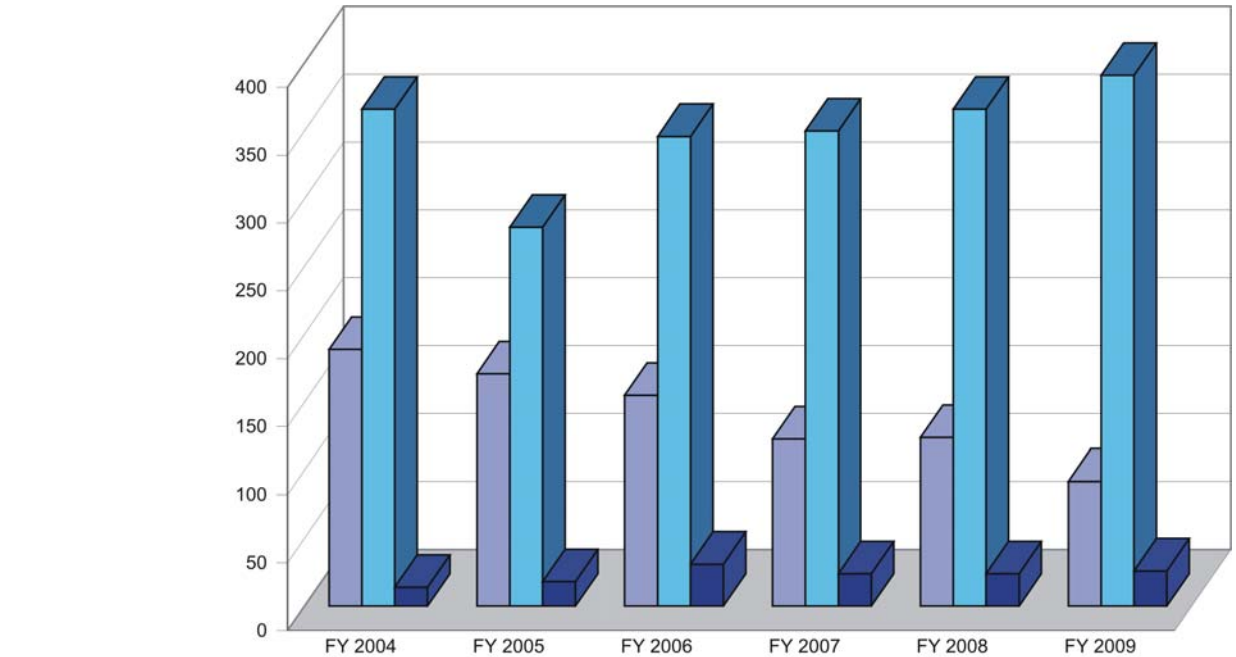


Figure 13: The Budget Outlook

Appendix

Summaries of Current and Target Architectures

Business Process Architecture

Information flow/Relationships of Core Business Processes

Agency planning documents define SSA's five core business processes:

- Enumeration;
- Earnings;
- Claims;
- Postentitlement; and
- Informing the public.

It is through these core business processes that SSA delivers its services to the American public—services that are based on long-standing as well as recent legislative requirements and broad Federal government policy. Major legislative initiatives over the years, which have dramatically affected SSA's workloads, have not changed the basic business processes.

The figure titled *The Social Security Administration's Core Business Processes*, found on the next page, reflects the complexity of the interactions among the processes. Then, a brief description of each process coupled with an illustration of its interactions broken out from the overall figure follows.

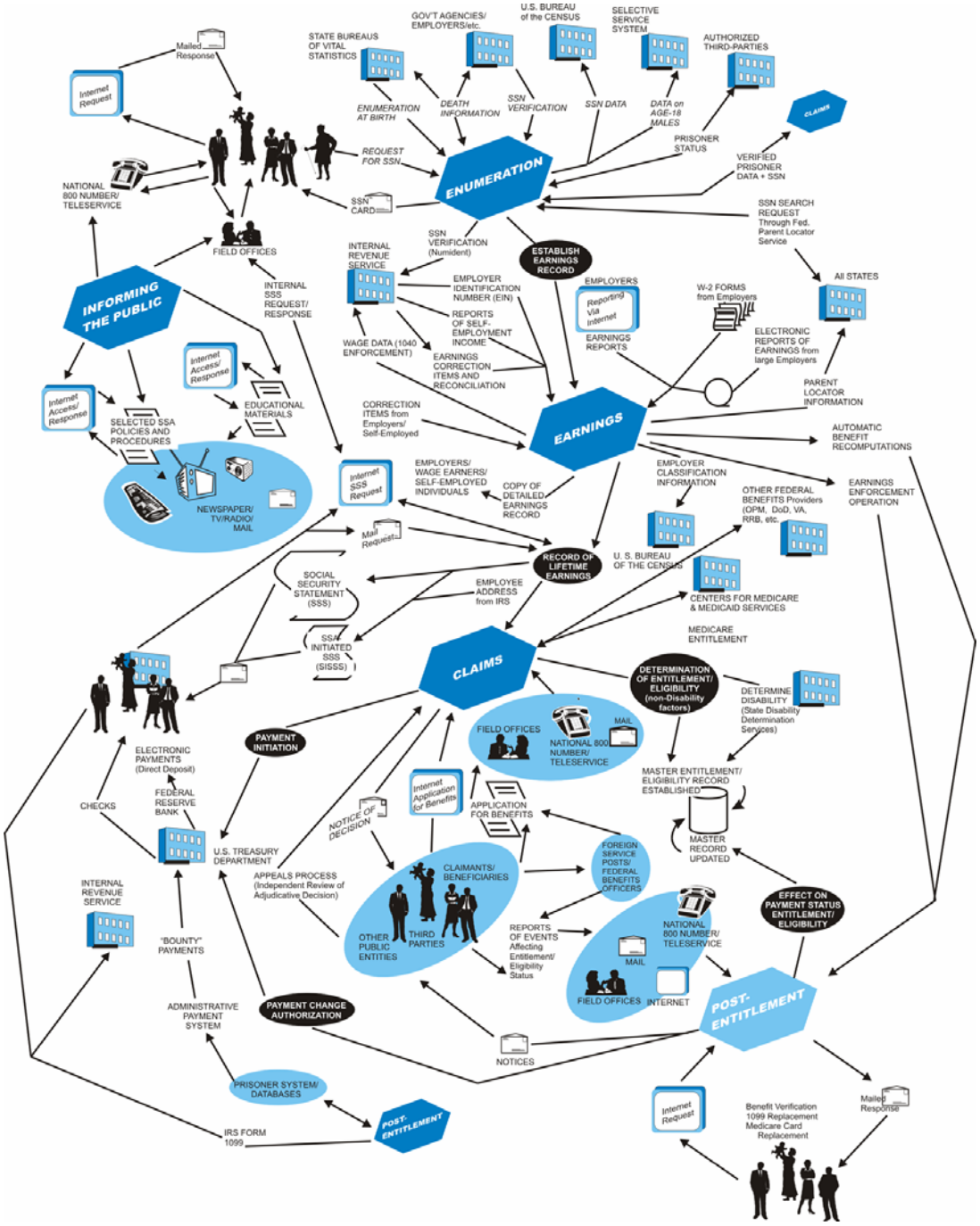


Figure 14: The Social Security Administration's Core Business Processes

Enumeration

Enumeration is the process by which SSA assigns Social Security Numbers (SSN) to identify workers and beneficiaries, issues replacement cards to people with existing numbers, and verifies SSNs for employers and other government agencies.

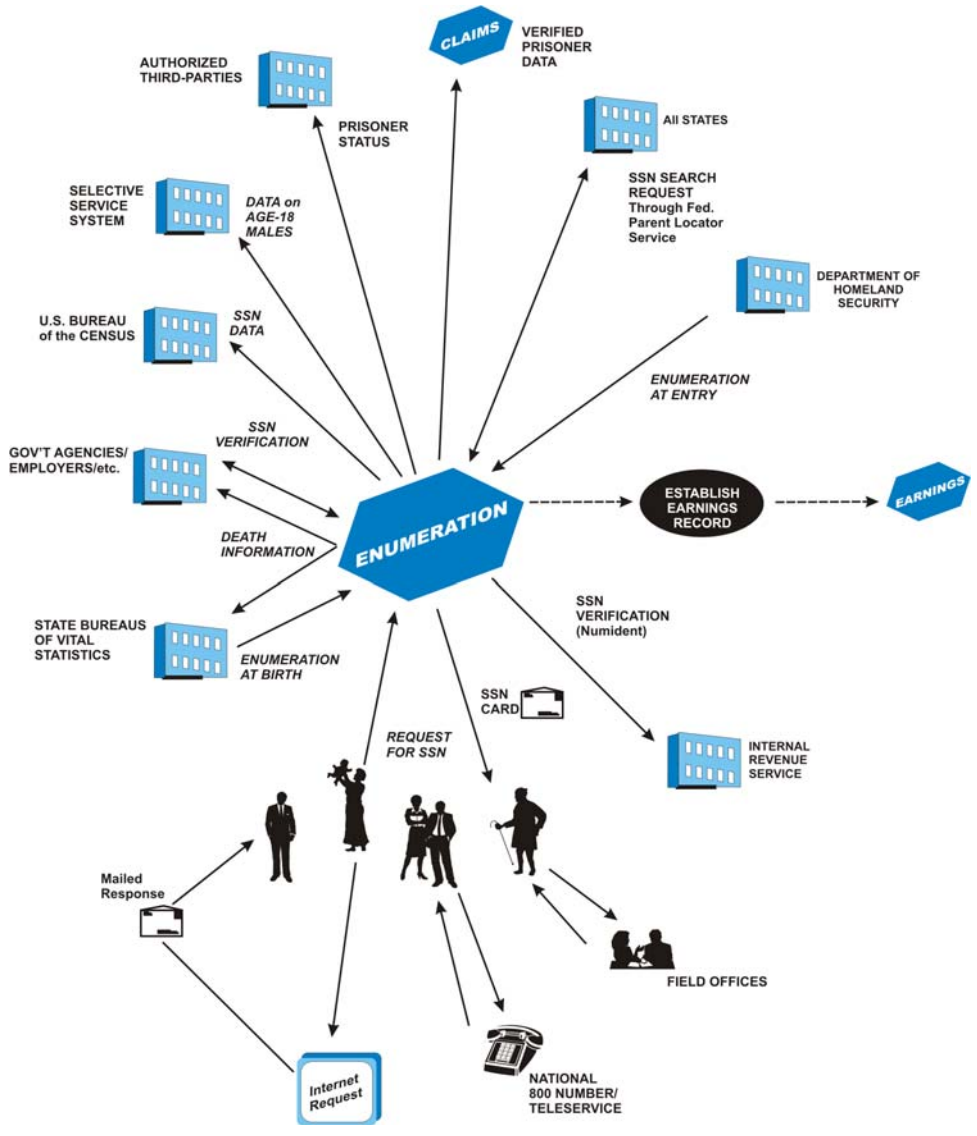


Figure 15: Enumeration

The SSN is used to record earnings covered by Social Security and/or Medicare and to process and pay claims for Social Security and Supplemental Security Income benefits. An SSN may be needed to report other income to the Internal Revenue Service (IRS) and is required by IRS for any individual claimed as a dependent on a

tax return. Countless other organizations, both public and private, also use the SSN for identification and administrative purposes.

An SSN is obtained by submitting an application and documentary evidence of age, identity and U.S. citizenship or legal alien status. Local offices are the primary points for accepting applications because of the need to examine documents to verify identity. Parents may apply for SSNs for their newborns at the time they register the birth at the hospital. Hospitals forward the data needed to assign SSNs to State vital statistics offices, which in turn key and transmit the data to SSA. Before a new SSN is assigned, the applicant's identifying data is compared to the existing database to ensure that the individual previously had not been issued an SSN. Enumeration at Entry, which is the Department of Homeland Security (DHS) collecting the enumeration information from persons over 18 with Permanent Resident Cards and forwarding it to SSA, is a process as distinct as Enumeration at Birth.

As a service to the public, SSA verifies the validity of SSNs (that the name, date of birth and number match existing records) for employers for payroll purposes, and for government agencies to ensure the accuracy of information used in other Federal and State benefit programs. SSA also offers SSN verification service to State Motor Vehicle Administrations for purposes of verifying information used to issue drivers licenses or identification cards. In small numbers, SSNs may be verified by calling SSA's national 800 telephone number or a local office. There is also a paper process for handling verification requests of 250 or less. Large volume requests are mailed to SSA on magnetic tape for batch processing or transmitted electronically to SSA through automated data exchange systems.

Through the Enumeration process, SSA handles almost 18 million requests a year for new and replacement social security cards.

Earnings

Social security benefits are based on an individual's earnings as reported to SSA. Reports of earnings are submitted annually by every employer liable for Social Security and Medicare taxes, including self-employed workers. Through the earnings process, SSA establishes and maintains records of individuals' lifetime earnings. The Agency uses this data to determine work history (i.e., insured status) for entitlement to retirement, survivors, disability and health insurance benefits, and to calculate benefit payment amounts.

Employers submit wage reports to SSA on paper, electronic or magnetic media. The process for recording wages is an annual operation. Paper submissions (i.e., W-2 forms) are processed primarily in SSA's Office of Central Records Operations' Wilkes-Barre (Pennsylvania) Data Operations Center where they are electronically scanned. The data is transmitted to central office where, along with the reports submitted on electronic and magnetic media, it is validated further and updated to the Master Earnings File. To ensure completeness of earnings data, wage items are

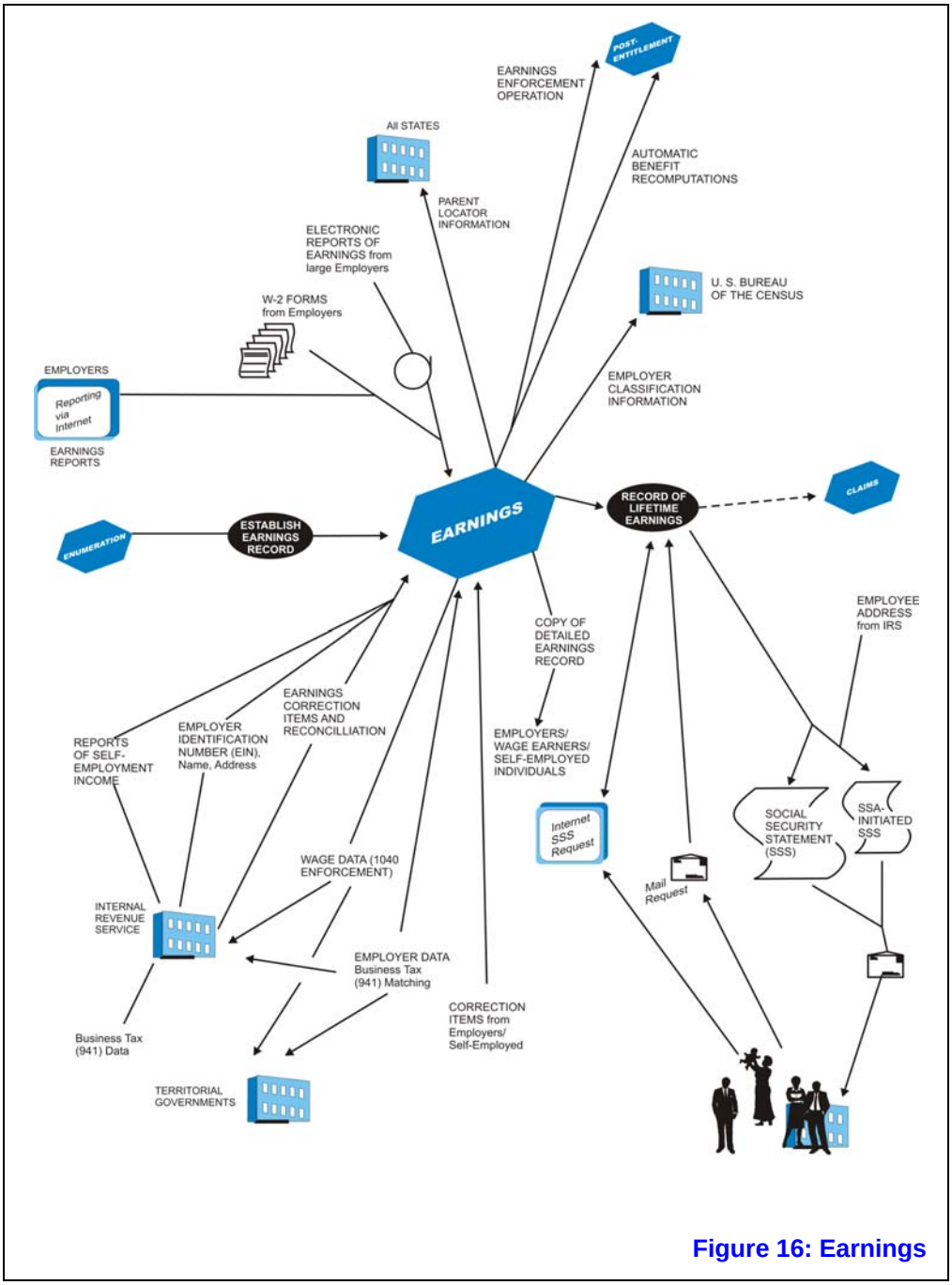


Figure 16: Earnings

matched yearly against tax data reported to IRS.

Workers, employers, or the IRS may request corrections to an earnings record. Individuals contact SSA in person, by telephone, through mail or the Internet. Local offices and processing centers are typically involved in the more complicated correction cases, as well as in those identified in connection with claims for benefits.

In FY 2003 SSA's Earnings process handled 257 million earnings items from employers and self-employed persons.

In addition, since 1988 SSA has offered a *Social Security Statement* on request to members of the public. A *Statement* contains a worker's earned credits and an estimate of benefits earned based on past work history. These statements are automatically mailed to a number of persons each year. SSA now mails an estimated 136 million statements annually to all eligible individuals. The *Statement* was formerly known as a Personalized Earnings and Benefit Estimate Statement, or PEBES.

Claims

To become entitled to benefits (i.e., payments) under the Retirement, Survivors and Disability Insurance (RSDI) program or Supplemental Security Income (SSI)

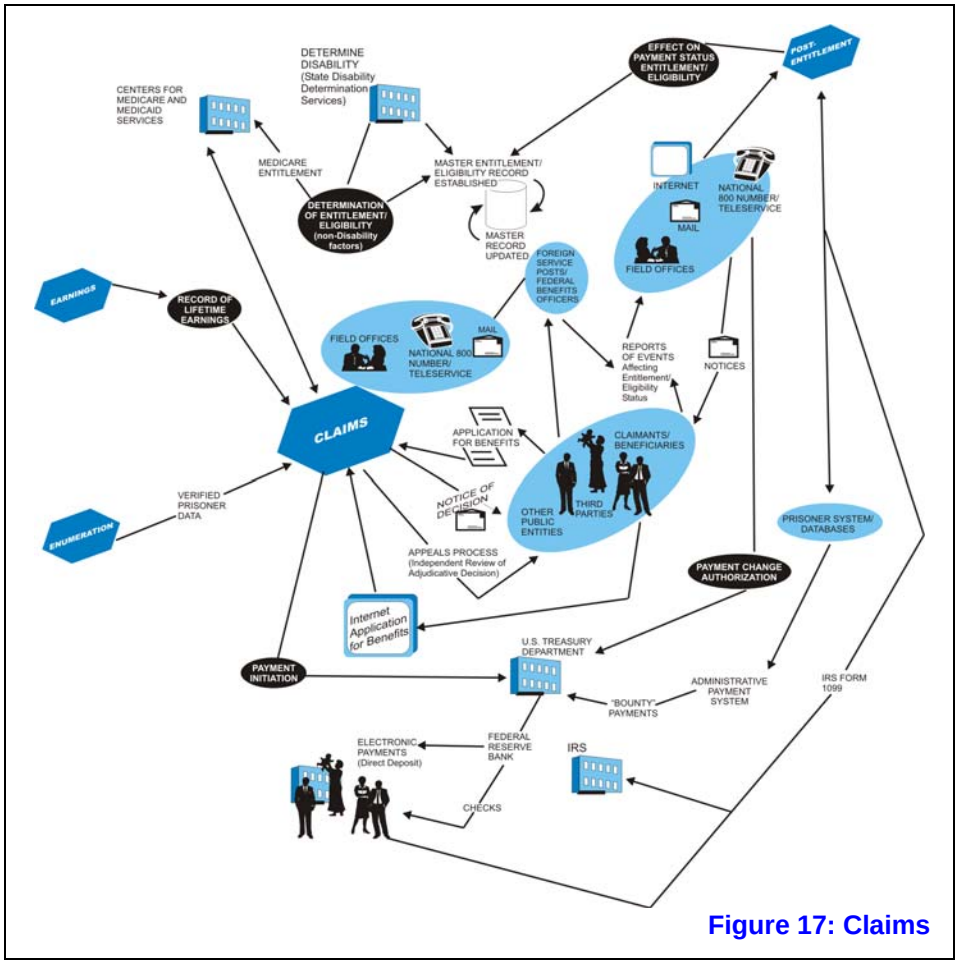


Figure 17: Claims

program, an individual files an application and submits certain proofs of eligibility. The claims process comprises the actions that SSA takes to determine an individual's eligibility for benefits. It begins with a claimant's initial contact with SSA and carries through payment effectuation, or the three levels of administrative appeal that a claimant may request.

The process for determining eligibility for benefits involves certain basic functions that are consistent across each program:

- Outreach and information;
- Intake;
- Evidence collection;
- Determination of eligibility;
- Notification of award or denial;
- Initial payment; and
- The appeals process.

Eligibility requirements vary considerably by program and type of benefit, but all require access to the SSN and earnings databases both to determine eligibility and to compute a benefit amount.

With regard to disability claims for both the RSDI program and the SSI program, in addition to being eligible for the program, it must be determined that the applicant is disabled. The medical determinations are made by State-administered Disability Determinations Services (DDS). State DDSs are staffed by employees of each State, but are funded by SSA. There are 55 DDSs which include all 50 States, the District of Columbia, Guam, Puerto Rico, the Virgin Islands, and the Federal DDS.

Finally, any claimant has the right to appeal the decision made on an individual's claim for benefits. This usually occurs when the Agency decision on the claim is unfavorable to the claimant, i.e., benefits are denied. If pursued after a local reconsideration process, an appeal is handled through SSA's Office of Hearings and Appeals (OHA). OHA maintains an independent structure of hearings offices throughout the country. Through these offices, claims are readjudicated and can result in reversing an earlier denial of benefits or affirming the original decision.

In FY 2003 over 7.5 million RSDI and SSI claims were processed.

Postentitlement

Once an individual becomes entitled to RSDI or SSI benefits, any change in circumstances that affects the amount or continuation of payment needs to be reflected in SSA's records. Non-disability eligibility redeterminations for SSI are mandated for each individual at least every 3–6 years. To accomplish this, records meeting criteria which classify potential errors are selected annually. About 2 million records are selected for this operation. In addition, the operation runs monthly to catch new cases and those records which have changes to their records requiring immediate contact. Total selections for redeterminations/limited issues are close to 3 million records annually. The postentitlement (PE) process encompasses the

actions that SSA takes after an RSDI or SSI claim is processed. The process is designed to ensure continuing eligibility and timely and correct benefit payment. Examples of PE activity include processing changes of address, non-receipts of payment, changes of payee and reviews of payee accounting information, benefit recomputations, overpayment recovery, changes in relationship such as divorce or remarriage, benefit-terminating events such as death, certain age attainments, and reviews of continuing eligibility.

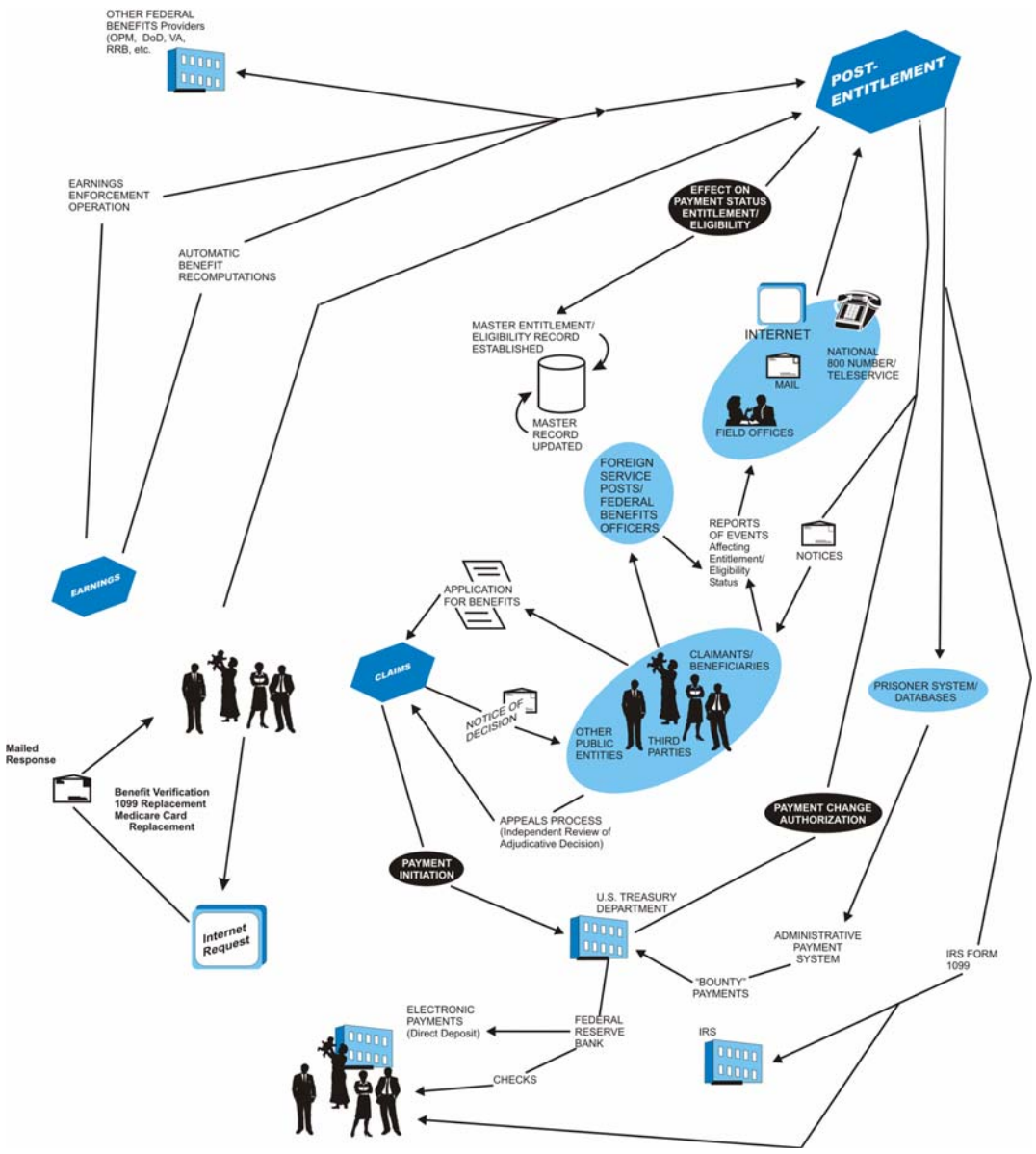


Figure 18: Postentitlement

PE activity is initiated by beneficiaries, recipients and third-parties, and is also generated from internal processes based on existing Agency database information. Employees throughout SSA—in local offices, teleservice centers and central records operations—and in the State DDSs are involved in various aspects of the PE process. As in the claims process, should a beneficiary or recipient be dissatisfied with SSA's action on the individual's benefits, an appeal can be initiated through the Agency's independent appeals process.

Almost 102 million postentitlement actions were processed in FY 2003.

Informing The Public

This business process involves SSA's extensive public information activities as well as the statistical and other program data SSA provides to support research and policymaking throughout the government and in the private sector. Most activities falling within this core business process relate to or are derived from one of the other programmatic-related processes.

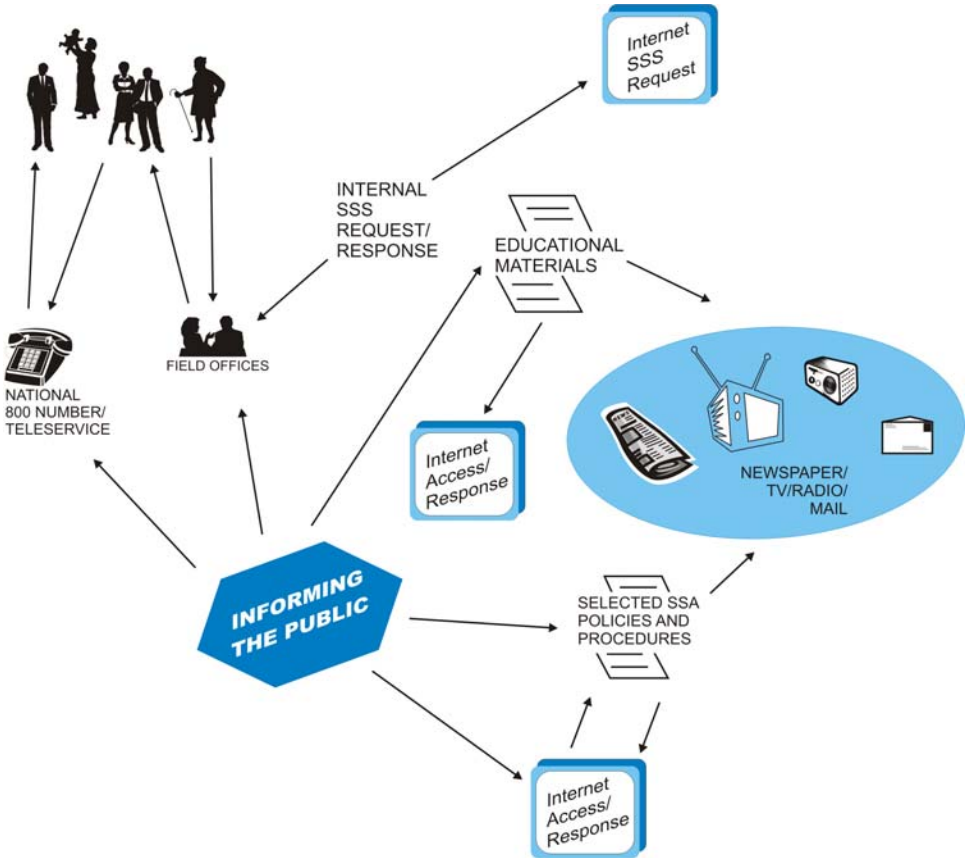


Figure 19: Informing the Public

Key Support Processes

Key support processes fall under two major categories—Administrative and Management Information Systems, and Information Technology Infrastructure.

Administrative and Management Information Systems

In addition to SSA's core processes, the Agency relies on a variety of administrative processes to ensure the continuity of its operations. Such support processes include, but are not limited to, payroll (i.e., the time and attendance system); workload tracking and control systems; accounting, budget and travel systems; employee

health and safety services; building operations; and any number of other systems and processes having to do with continuing operations.

Program Policy Process

Supporting all of the SSA core business processes is the key process of program policy and instruction development and dissemination (known as the Program Policy Process). Re-engineered in the mid 1990s, the SSA Program Policy Process has evolved into a comprehensive set of procedures and systems to identify, research, author, and distribute rules, regulations, instructions, explanations and guidance on all SSA programs and services. The generation of key management information is also facilitated. The process touches almost every component in SSA, either as an information provider or as an information user.

The Program Policy Process is supported by an extensive set of electronic tools, databases and systems. These include but are not limited to: QuickPlace collaboration sites, , MS Outlook, several Oracle DBMS', the Instructional Authoring System (for POMS, HALLEX and the TSCOG), the PolicyNet Reference area, the Program Policy Archive System, the Policy Implementation Planning System, Medicare Online, and the E-DIB Operating Guide Online.

Information Technology Infrastructure

SSA relies on an information technology infrastructure to support virtually all of its programmatic, administrative and management information processes. Essential features include the Agency's processors (hardware), systems software and telecommunications system, as well as its facilities, transportation, uninterruptible power supply (UPS) services, and general business continuity (backup and recovery) processes. Together they provide the means by which SSA is able to provide service on demand to the general public, the Agency client population, other government entities, large and small corporations, and individual businesses.

The Internet serves as an additional channel of programmatic communication for virtually all types of public and third party contact. This includes support for systems development and maintenance of all Internet, Intranet, and Extranet applications that provide access to SSA for any e-customer that wants to use any e-business programmatic functionality the Agency provides.

Application Architecture

Application Software

Application software in use at SSA is categorized as programmatic, administrative, and management information. Software applications that support workload functions related to the delivery of client services required by law or regulations are classified as programmatic. All other software supports services used to manage the Agency including its workloads, personnel, payroll and financial transactions.

Figure 20 below defines the application software boundaries and interfaces, and identifies software common to multiple systems. The figure shows the relationship among the primary architectural components. These include, from right to left:

- SSA's business-critical data that are entered and retrieved through database access software;
- Key business applications (interactive and batch) with their process control front-end software;
- Support applications (Print Manager, Mail Delivery, Notices, etc.); and
- Presentation functions that provide security and network management for customers interacting with the system.

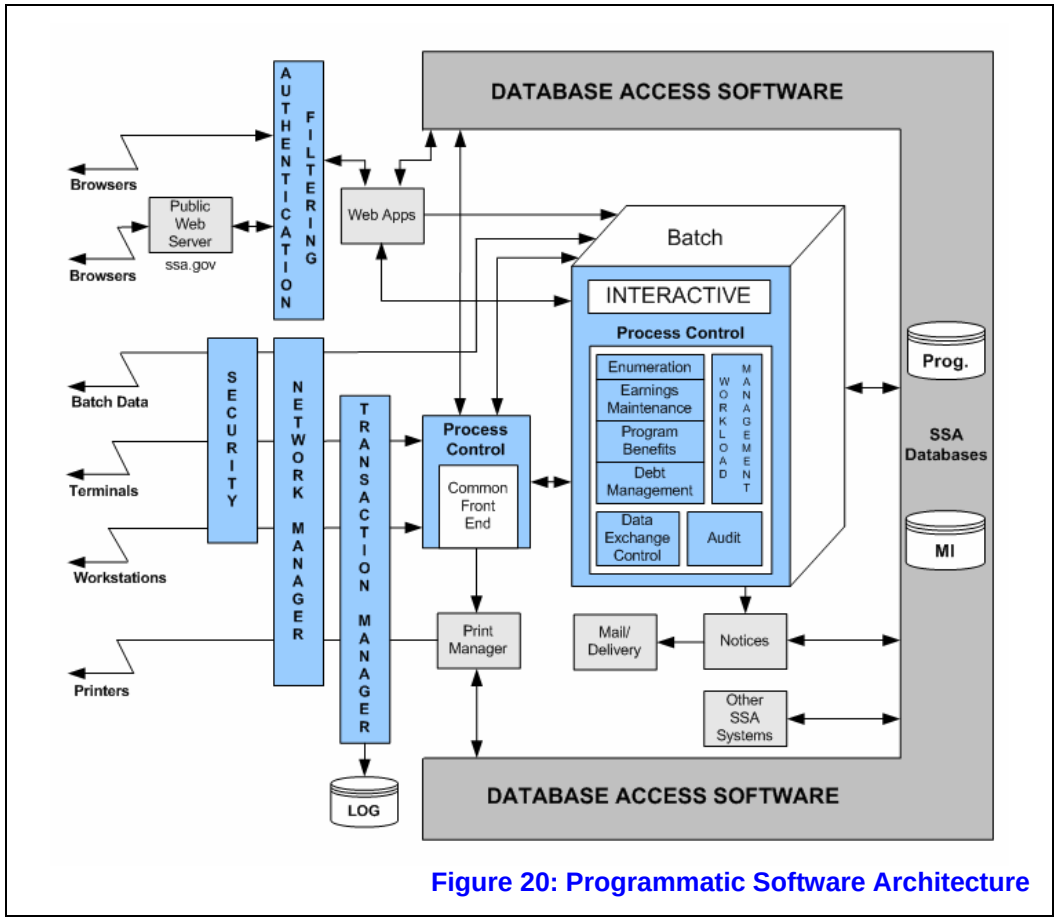


Figure 20: Programmatic Software Architecture

This design which has guided the Agency's systems development for the last decade has been enhanced to accommodate SSA's latest business vision which is providing electronic service delivery using web-based applications. The diagram shows how Internet users interact with the Agency's traditional business systems. This is done through the Public Web Server and Authentication Filtering to access web applications. These web applications, in turn, can access the Agency's key business applications and data as required. This architecture ensures a high level of security while eliminating the need to duplicate business logic and databases for web-based applications.

Programmatic Systems

SSA's IRM Strategic plan calls for continuing attention to the enhancement of the functionality, efficiency, and maintainability of our programmatic software applications. SSA has no immediate plans for the wholesale replacement of these applications. The Agency considers such an undertaking to be much too costly, fraught with risk, and essentially unnecessary. Rather, SSA intends to continue with a balanced program of functional enhancements, targeted new development, and regular technical improvement. SSA's approach is evolutionary, not revolutionary.

Strategic Goals for Programmatic Systems

The SSA strategy for programmatic applications is designed to achieve the following strategic goals:

- Systematically reduce the number of programmatic transactions that are rejected or alerted for manual attention to *increase the level of automation;*
- Incorporate new system security technologies, as appropriate, to further protect SSA's programmatic applications and the sensitive, personal data that these applications use and create, thereby *enhancing system security and privacy protections;*
- Provide automated *client self-help capabilities* (such as use of the Internet) to enable SSA clientele and authorized business partners to deal directly with our automated systems;
- For those cases where initial input transactions are rejected, *integrate with local support systems* to help SSA operations personnel effectively control, manage, correct, and reprocess the rejected or alerted workload items;
- *Support paperless processing* in all SSA field components and State Disability Determinations Services (DDS) offices; and
- Regularly maintain and periodically *improve the efficiency and maintainability of programmatic applications.*

A sizeable portfolio of system development and software enhancement projects has been established to achieve these strategic goals. These projects are identified in the SSA Systems Work Plan, along with summary data that quantify the projected return on investment (ROI) and work-year costs for each. The matrix included as Table 7 below provides examples of the kinds of initiatives that will be undertaken to achieve each of the strategic goals. Note that the example initiatives are categorized within the five major functions common to all software applications: Input, Retrieve, Process, Store, and Output.

Programmatic Application Goals	Programmatic Automated Processing Functions INPUT → RETRIEVE → PROCESS → STORE → OUTPUT				
1) Increase level of automation	*Enhance input data collection, data editing*	*Provide access to additional data types*	*Provide additional processing logic*	*Improve integrity of stored data*	*Improve clarity of exception output messages*
2) Enhance system security & privacy protections	*Adopt next generation application access controls (e.g, PKI)*	*Incorporate DBMS administered multi-level database access controls*	*Conduct periodic security audits of all sensitive applications*	*Adopt certified data storage technologies*	*Transmit outputs using appropriate encryption techniques*
3) Provide client self-help capabilities	*Provide Internet-based input channel*	*Provide access to additional stored data*	*Isolate input presentation functions*	*Store partially completed input data*	*Improve clarity of user output messages*
4) Integrate with local support systems	*Provide automated input path from local support systems to programmatic applications*	*Provide automated data retrieval path from local support systems*	*Integrate local & programmatic pre-release testing processes*	*Identify stored transactions & results created by local support systems*	*Write programmatic output directly into local support systems*
5) Support paperless processing	*Provide document scanning; Provide logic to locate & extract structured data from scanned images*	*Provide document image indexing capability*	*Provide workflow control logic for PSC & DDS operations*	*Store scanned images & associated indices; Provide foundation for storing other non-structured data*	*Create output using paperless recording media*
6) Improve software efficiency and maintainability	*Isolate input presentation functions extracted from processing applications*	*Provide isolation layers to insulate processing applications from database technologies*	*Restructure & document code; adopt reusable software modules/ objects*	*Provide isolation layers to insulate processing applications from database technologies*	*Adopt standard output message and language libraries*

Table 7: Initiatives to Achieve Programmatic Application Goals

Increased Automation

Since the development of the first computer-based programmatic applications in the early 1960s, SSA systems components have been driven by the strategic business objective to automate functions that were previously performed by SSA employees.

The success of SSA's automated systems and its workforce of skilled knowledge workers have enabled this agency to assume ever-increasing workloads without massive increases in the SSA labor force. SSA programmatic automation goes far beyond the collection and storage of data for subsequent retrieval by employees in the SSA field offices. Custom developed software logic makes complex determinations of programmatic entitlement and eligibility, automatically computes monthly benefit amounts and withholdings, generates personalized award certificates, letters and other automated notices, and much more.

While a significant portion of the programmatic business functions have been effectively automated, we continue to push for further automation gains. Because Social Security legislation is additive in nature, new systems requirements are continuously being added as extensions to programmatic requirements that have built up over the years since 1937. Failure to keep pace with these new, additive requirements would result in steady erosion of the overall automation rate.

Currently, the relative volume of programmatic transactions rejected or alerted by the automated systems is actually quite low—less than 5% for the majority of system transaction types. That is, more that 95% of the SSA programmatic transactions are processed to completion without the need for human intervention beyond the entry of input (event) data into the automated transaction processing systems. But, when dealing with the volume of transactions that occur in the SSA operating environment, small reject percentages translate into very large numbers. These large numbers consume a significant percentage of the available human work hours in any given operating day. If we are to make a greater percentage of our workforce hours available for dealing with the public, the amount of time spent on the entry of input data and the resolution of rejected transactions must be reduced.

For the past several years, we have been reengineering the 'front-ends' of our transaction processing systems to adopt real-time data entry methods (particularly, a common point for data entry and the resolution of data input errors). While this effort is largely complete, there are several reasons for focusing on the input processes:

- There are substantial payoffs still to be realized; a significant percentage of the total number of rejected transactions is caused by invalid input data.
- Improving the input processes is less difficult than dealing with the other causes of programmatic exceptions (such as extending the already complex transaction processing logic or eliminating inconsistencies in previously stored historical data).
- The input processes are the most amenable to the new and evolving information technologies, such as object-oriented design, graphical user interfaces (GUI), the Internet, natural language, voice translation and synthesis.
- It is the portion of the overall process that is most seen and best understood by end users (and, as a result, the area most addressed by user service requests and employee suggestions).

In addition to improving the programmatic input processes, work will continue on extending the level of automation within the transaction processing systems that run centrally at the SSA National Computer Center (NCC). The following table identifies a number of currently established software projects that are designed to enhance the programmatic input processes and/or increase automation in the transaction processing systems:

Application Software Projects	Automation Objectives
Annual Wage Reporting	Extend the highly successful program for automating employer annual wage reporting (from paper reports to magnetic media or Internet reporting).
Title II Redesign (Attorney Fees)	Generate IRS Forms 1099 for fee amounts paid to attorneys representing title II claimants.
Implement Railroad Retirement and Survivors' Improvement Act	Modify existing claims and postentitlement systems to modify and extend automated adjustment of title II benefits based on RRB entitlement.
Automated Job Stream Notice Improvement	Extend existing software logic to automatically generate client notices with clarified language, improved sequence of explanatory paragraphs.
Integrated Disability Management System	As a result of Ticket to Work legislation and other postentitlement disability projects, develop new system capabilities to automate control of continuing postentitlement disability functions, including those related to assisting

Application Software Projects	Automation Objectives
	disability beneficiaries in their attempts to return to work.
SSI FORD Court Case	In automated notices generated by the SSI System, provide more detailed information explaining the derivation of payment amounts.
OHA Automation—Digital Recording Capture	Automate the capture, storage and retrieval of audio recordings for Office of Hearings and Appeals
OHA Automation—Video Teleconferencing	Automate the capture, storage and retrieval of video recordings for Office of Hearings and Appeals
QA Modernization	Develop a modern, reusable QA Architecture to support migration of the antiquated, high-risk legacy QA systems, respond to needs for dynamic study definition and execution, improve timely detection of erroneous payments and expedite corrective actions initiatives.
Distributed Online Correspondence System (DOCS)	Extend and refine the DOCS system to further assist SSA field components in building their own client notice templates and notices from a database of standardized language.
Increased Title XVI Automation	Improve productivity, e.g., reduce internal work hand-offs and multiple contacts with beneficiaries.

Enhanced Applications Security

Systems security is a top priority for the Social Security Administration. All new programmatic applications are designed and developed with effective security protections as a mandatory requirement. Internal change control reviews and the enterprise-level Architecture Review Board (ARB) reviews all include careful examination of the security and privacy protections provided by the application design. Prior to production release programmatic applications are thoroughly tested for possible security weakness. Additionally, existing applications are regularly subjected to security audits and independent penetration testing. As new security technologies and protection methods are adopted by the Agency, programmatic applications are modified, as necessary, to provide compatibility with such new methods.

Generally speaking, the SSA enterprise architecture thinking calls for isolating applications from the security components that protect the applications and their associated data. The underlying security tools and support technologies are part of the IT infrastructure that applications use as a platform for transaction processing. (See "Infrastructure Architecture" beginning on page 136 for detailed information about the SSA security infrastructure.) This isolation helps to establish clearly defined security layers that avoid the mixing of application and security code in the same execution space. SSA also typically will select general-purpose security solutions over application-specific methods that are more vulnerable to security penetration. This type of functional isolation is fundamental to the notion of 'compartmentalization' that is an essential characteristic of an effective system security strategy.

Even with such separation and isolation it is sometimes necessary to modify applications in order to implement such architectural changes. For example, in our current mainframe environment, all applications must be registered to the TOP SECRET security management tool, identifying the databases and files that they are authorized to access. As the SSA system security architecture continues to evolve,

adopting new technologies that provide increased protection, the SSA programmatic applications will be modified, as necessary, to take advantage of these new protections.

For example, SSA's next generation Internet-based applications are being designed to rely on a new commercial off-the-shelf (COTS) client authentication subsystem that will be used to identify authorized clients for E-government transactions. Additionally, current prototypes and other experiments using public key infrastructure (PKI) technology may lead to a new security component that will be used by programmatic applications.

The following table identifies a number of currently established software projects that are designed to enhance system security and/or privacy protections:

Application Software Projects	Security / Privacy Objectives
WebSphere Pilots—Client Authentication	Develop next generation Internet architecture using WebSphere Access Manager as the underlying tool for Internet client authentication.
Comprehensive Integrity Review Process (CIRP)—Data Mining	Extend the existing CIRP to use the Intelligent Miner tool to assist the discovery of fraud.
e-Vital	Extending automated data exchange with State agencies will require expanded use of existing system security solutions and the possible adoption of new security solutions for new exchange partners.
GSA E-authentication	Provide authentication and credential management services to citizens, government agencies, businesses and other institutions as an enabler of secure, authenticated transactions.

Local Support System Integration

Over the years, SSA local and regional offices have developed a variety of applications to help them deal with the workloads that are created for and by the automated programmatic systems. For example, the central transaction processing systems deliver many different types of processing exceptions, alerts and development requests to the field offices for investigation and follow-up manual actions. Employees with software development knowledge in these offices have developed various types of automated support systems to help them control and process these workloads. The local support systems range from simple information look-up tables to fairly sophisticated workload control systems and various types of 'screen scraping' applications that match and combine data to build input transactions to be re-entered into the central transaction processing systems.

In recent years, the field operations components have worked together to select the 'best of breed' from these locally developed support systems. The selected systems are now being refined to serve as regional or national standards for selected support functions. A collection of projects has been established to support these regional efforts.

We expect that in the near future, additional projects will be established to more tightly integrate these local/regional support systems with the central programmatic systems. This will help to more broadly establish a multi-tier application architecture (that will be reflected in both our short-term and longer-range target application architectures).

Visitor Intake Process (VIP) is one of the currently established software projects that deal with the development and refinement of locally developed programmatic support systems. VIP will upgrade a locally developed application used to help manage district office visitor queries and the assessment of visitors to field office representatives. The VIP data are also used to create workload measurement reports identifying workloads not previously reported.

Client Self-Help Capabilities

The most visible category of client self-help projects is the development of an Internet-based input channel that allows SSA clientele to deal directly with the Agency's automated systems (rather than an SSA employee as intermediary). SSA has several successful implementations already in production and high-priority work continues on extending this capability to the full range of client-initiated programmatic transactions. Three broad types of Internet applications are being constructed:

- The simplest of these applications use static or active server pages to provide clients with information about SSA and the various programs that the Agency administers.
- The second category (and the most common) is server-based applications that act as interactive front-ends to the existing programmatic transaction processing systems. These applications allow clients to file a claim for benefits, request an earnings statement, or a variety of other services by entering information online. The Internet applications communicate with the programmatic online or batch processing systems and return response information to the client's personal computer screen. (In some cases, completion of transaction processing is asynchronous and the completed output product is delivered later from an existing batch processing system.)
- The third type of Internet application is a completely new application that is developed specifically for Internet users. In these cases the process typically runs online as a server application.

In addition to the applications that deal with SSA claimants, beneficiaries, SSI recipients, and their authorized representatives, there are many self-help applications that support employers and other types of SSA business partners. For these clients, the Agency makes use of existing programmatic online or batch processing applications wherever possible. Internet-based front-ends allow these trusted third parties to enter input directly into existing programmatic data exchange systems, bypassing SSA human intermediaries.

There are also several disability-related Internet services that were recently added. The Integrated Social Security Benefit Application (ISBA) now allows claimants for title II disability benefits to complete their application online. ISBA filers also can complete and submit the Disability Report (SSA-3368) online. The Office of Systems will soon make the complete suite of disability report forms available via the Internet.

While the Internet is the most visible type of client self-help application, there are other types of systems that also provide highly effective and efficient services to SSA business partners. These applications use more traditional data exchange technologies, such as system-to-system interchange, electronic file transfer, and shared network access. These types of systems are very productive in situations where the external business partner has a substantial investment in automated systems and databases and prefers to generate transactions out of their automated system (rather than manually entering data via the Internet).

Over the next several years SSA expects that a significant amount of programmatic application work will be focused in the area of expanded self-help capabilities. Primary attention will be focused on use of the Internet, but other types of data exchange will expand as well. This is particularly the case in our dealings with employers and State agencies.

The following table identifies a number of currently established software projects which deal with expanded self-help capabilities for clients and business partners. (**Note:** Many of the cited software projects support more than one strategic goal.)

Application Software Projects	Client Self-Help Objectives
WebSphere Pilots	Development of second-generation software applications for client-entered postentitlement transactions (using the WebSphere J2EE-compliant web development tool set).
Representative Payee Accounting	Provide volume providers with the ability to submit SSA-623 accounting reports as Internet transactions.
State Online Query (SOLQ)	Provide States with online capability to obtain SSA enumeration, earnings, and benefit information.
Title XVI Account Status	Provide Internet-based capability to obtain title XVI bank account, identification, overpayment, and Medicare information from SSA master files.
Electronic Wage Reporting	Provide capability for small employers to submit annual wage reports as Internet transactions.

Paperless Processing

SSA has a long-established strategic goal to reduce reliance on paper forms for conducting programmatic and administrative business functions. In the automated programmatic processes, considerable progress has already been made in achieving this goal. The Paperless Processing Center Project has established the foundation for the elimination of the paper claims and the vast majority of Program Service Center (PSC) functions are now conducted without use of these folders. Operations personnel in the field components have a variety of online and batch information retrieval paths for obtaining 'master record' data stored in the central databases. Internet initiatives have established the basic applications structures that will be needed to eliminate paper applications in the title II and title XVI claims processes.

While considerable progress has been made, important work remains to be done. For example:

- Additional experimentation and prototype system development is needed to determine the specific methods to be used for electronic signatures.

- We need to gain much more first-hand working experience in using digitized images of various types of technical documentation material (particularly medical evidence) in order to establish system requirements such as display resolution, color replication, page flip rates, simultaneous viewing of multiple pages, etc.
- Audio and video recordings of hearings and other types of evidence are obviously feasible from a technical standpoint, but essentially untested from an operations perspective.

There are significant cost considerations that need to be addressed as we move forward to eliminate reliance on paper documents:

- Additional direct access disk storage (and off-line archival storage) for the recordation of additional transaction history and non-structure data types, including scanned images, video and audio recordings. A commercial off-the-shelf content management tool will also be required to effectively store and manage the tremendous volume of digitized records that will result from the elimination of paper records in the SSA programmatic processes.
- Additional wide area network (WAN) and local area network (LAN) bandwidth is needed to support the movement of very large unstructured data records between storage nodes and workstation devices.
- Backup (and possibly redundant) mainframe and server computing capacity may be required to provide the kind of 'non-stop' system architecture that will be needed when offices begin to rely totally on automated systems and records for day-to-day workload processing.
- Additional local support technical staff (either in-house or contractor personnel) may also be needed to provide for very rapid return to service response in the event of inevitable equipment failure.
- OHA will need additional IT equipment for its hearing rooms to deal with the electronic folder, digital recordings and video teleconferencing. An Automation Planning Group has been convened to identify the specific needs.

Many of these issues are being addressed as SSA moves ahead with implementation of the Accelerated Electronic Disability (AeDib) project. The technical decisions that are reached as part of the AeDib effort will have a significant impact on the structure of programmatic application target architecture. The following table identifies a number of currently established software projects that deal with the support of paperless processing:

Application Software Projects	Paperless Objectives
Paperless PSC	Complete installation of the Paperless PSC infrastructure and continue enhancing the software applications.
Accelerated Electronic Disability (AeDib)	Move partners in disability claims adjudication/review to a "folderless" process by connecting legacy systems to an electronic folder.
OHA Case Processing and Management System	Development of a case processing and management system for OHA that will be integrated with the electronic folder. This is one of the five components of AeDib.

Software Efficiency and Maintainability

In addition to the projects intended to enhance application functionality, SSA will also conduct a variety of software engineering efforts to improve application efficiency and maintainability. These projects are part of the ongoing efforts we make to keep our automated processing systems current to reduce maintenance and improve performance.

Software improvement projects come in all sizes and focus on a variety of technical objectives; e.g.,

- Existing application code may be modified in order to upgrade an underlying COTS software product used by the application. Upgrading the software development tool set or the database management system (DBMS) is often necessary because the software vendor no longer supports the outdated product. In other situations an underlying infrastructure product (such as a new operating system release) will provide efficiency benefits that justify minor adjustment of production applications.
- Selection of a new enterprise standard for a commonly used software function can require modifications to applications that were developed using some other software product. Converting such software applications may be cost-justified based on the resulting savings in license fees and other technical support costs that result from the elimination of redundant support products.
- Similar cost savings can also be realized by software improvement projects that replace many small, but functionally similar applications, with a single application processor.
- Occasionally, software maintainability may be improved by a project that does not involve modifying the application code itself. The effort to document the existing programmatic application systems is a good example of such a project. This effort will produce the existing application architecture documentation needed to meet Clinger-Cohen requirements. The availability of this architecture will also pay dividends as part of the ongoing management of software applications.

The following table identifies a number of currently established software efficiency and maintainability projects:

Application Software Projects	Efficiency and Maintainability Objectives
Title II Redesign	Complete the development of a new title II transaction processing application that will replace the existing title II postentitlement 'object programs'.
Representative Payee Accountability Phases 2 and 3	Improve and restructure the existing title II and title XVI Representative Payee Accounting application leading up to the combination of these two separate systems and their associated databases.

Additional Target Architecture Information

For additional information about the development of target architecture definitions for the SSA programmatic applications, refer to Chapter 3 of this document.

Administrative Systems

In contrast to the programmatic systems, SSA's administrative systems support the management of SSA's human, financial, and physical resources. SSA's administrative systems directly support 3 of the goals of the President's Management Agenda:

- Strategic Management of Human Capital,
- Improved Financial Performance, and
- Budget and Performance Integration.

In addition, the SSA strategy for administrative and management information applications is designed to achieve the following strategic goals:

- Develop an incrementally implemented enterprise level Administrative Business Architecture (ABA) that facilitates the integration of disparate administrative source systems and recognizes data created in such systems as a corporate asset. The ABA will act as a framework for adding new capabilities as well as enhancing or replacing existing administrative systems.
- Develop a robust Management Information Architecture (MIA).

There are a number of software applications, running on a wide variety of platforms and architectures, in support of these goals. Many were written in-house; others are commercial off-the-shelf (COTS) or government-developed off-the-shelf (GOTS) products, which SSA either implemented "as is" or modified to meet the functional requirements of the associated business processes. In some instances, administrative business processes are being supported through an Application Service Provider. These various systems were developed, improved, and redeveloped over the past 25+ years in response to specific business process needs. Many were developed by SSA's Office of Systems (OS) with internal development staff and/or contractors; others were developed by the business components responsible for the function. Examples include:

- *Online SSOARS* which is the management information (MI) arm of SSOARS. This is a mainframe query tool developed by SSA's Finance Office.
- *Third Party Payment System (TPPS)* which provides SSA's field and regional staffs the capability to write "checks" for administrative and programmatic payments. This is a mainframe CICS application developed jointly by OS and SSA's Finance Office.
- *Benefit Certification and Accounting System (BCAS)* which provides automated support of the business processes associated with the certification and accounting of benefit payment data sent to Treasury. Presently there are both a title XVI and a title VIII BCAS. Planning is underway for a title II

BCAS. Each is a mainframe application developed by OS with contractor support.

- *Financial Interactive Voice Response System (FIVR)* which provides SSA employees and vendors access to the status of payment (e.g., travel reimbursement, vendor invoices) through use of interactive voice response technology. The application was developed jointly by OS and SSA's Finance Office with contractor support.
- *Administrative Payment Information Network (API Net)* which provides employees with an alternative means of accessing the payment status data available through FIVR. This web-based application was developed by OS.
- *Social Security Administration's Streamlined Acquisition System (SSASy)* which supports SSA's acquisition business processes. This COTS solution was implemented by SSA's Acquisition Office with contractor support.
- *Financial Information System (FIS)* which provides budget execution tracking support for SSA's field and regional offices. It is a Web application developed by SSA regional offices.
- *Federal Personnel/Payroll System (FPPS)* which processes core personnel transactions and the biweekly payroll process. These are outsourced to another Federal agency serving as an Application Service Provider.
- *Mainframe Time and Attendance System (MTAS)* which processes time and leave records into the payroll process. It is a mainframe GOTS significantly modified by OS with contractor support.
- *Human Resources Management Information System (HRMIS)* which provides administrative management information on human resource transactions. It is a mainframe application developed by OS.
- *Official Union Time Tracking System (OUTTS)* which is a system used to track time spent by employees on official union business. It is a mainframe application developed by OS.
- *Training Online Nomination* System *(TONS)* which is a system used to process requests for authorization of training nominations. It is a mainframe GOTS modified by OS.

These applications represent many of the administrative business processes supported at SSA. But there are many other similar processes and applications running on SSA's computing platform.

For example, the Office of Systems creates and maintains numerous data extracts from its programmatic data bases that support SSA's statistical, research and policymaking functions. The Office of Policy uses these data as the basis for:

- Research,
- Policy analysis,
- Numerous publications,
- Fact Sheets,

- Analysis of proposed legislation,
- Information for OMB and congressional staffs,
- Information for higher monitoring authorities, and
- Research data sharing with other Federal agencies.

Administrative Business Architecture

The collection of applications described above has served their customers well over the years within the limits of each application's individual business process domain. Recently, work has been done to integrate some of them, particularly with SSOARS for financial accounting purposes. While somewhat successful, the amount of work required to accomplish those efforts, coupled with the growing need to support COTS offerings and entrepreneurial development, underlines the need for a different approach. One major pillar in that approach must be a standard framework which provides a structure for all future administrative systems development, regardless of software/hardware platform or location of development support.

SSA is just beginning to embark on the development of the Administrative Business Architecture (shown below) which will provide that framework. This architecture will be integrated with the MI Architecture as displayed pictorially on page 126. The following factors will guide the development of the Administrative Business Architecture:

- Administrative applications must acknowledge all potential customers (e.g., employee/manager self-service) rather than just the traditional business process specialists; and
- Administrative applications must improve productivity or otherwise provide value-added service (i.e., to the business process specialists of the particular business domain; to end users (employees/managers); and/or other users of the data created (data supporting other business processes or management information).

- The need to leverage COTS, GOTS and application service provider solutions to support the automation of SSA administrative business processes. In implementing such solutions, SSA recognizes the need to minimize customization so as to leverage best practices, reduce costs/risk and maintain a future upgrade path.

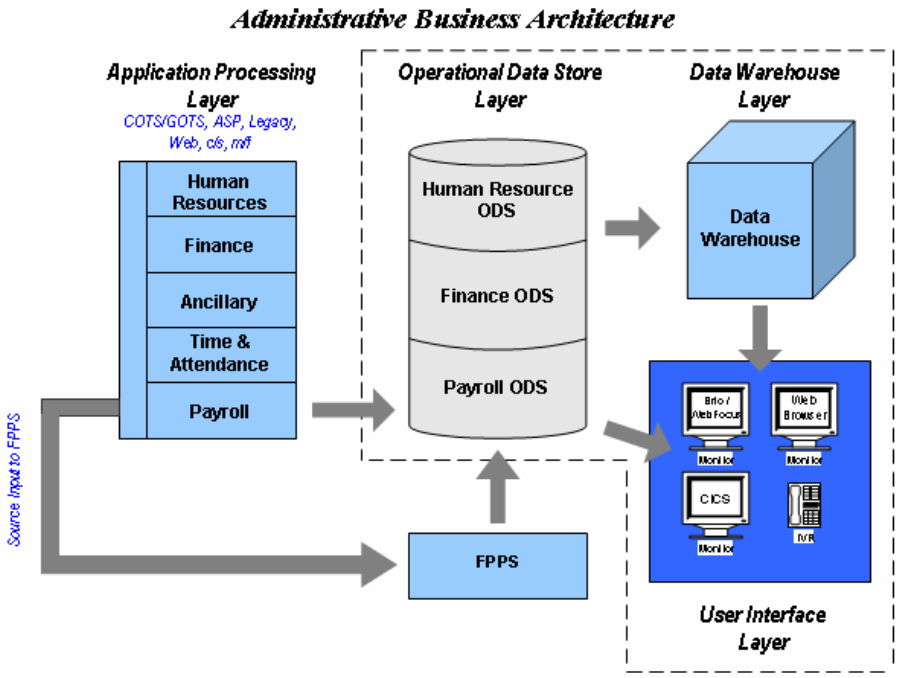


Figure 21: Administrative Business Architecture

- Integration of functions and data across formerly separate business processes is increasingly important. Data created in one administrative business process is frequently required elsewhere in the enterprise to support the processing of other administrative transactions or as administrative management information to support the management of human and financial resources.
- The ABA will work in concert with the Management Information Architecture to ensure the availability of administrative data as a corporate asset and the effective delivery and presentation of such data. This will be accomplished through the implementation of consistent data definitions and data structures, and the use of similar Business Intelligence tools. The ABA will provide standard data definitions and usage rules, thereby allowing users throughout the Agency to leverage administrative data to meet the Agency's tactical, operational and strategic reporting requirements. The physical structure of the ABA will rely on components such as operational data stores and the data

warehouse, as well as standard reporting tools that comprise the Management Information Architecture.

- OS, departmental development teams and external solution providers will form alliances to take advantage of all available resources and leverage the specific skills of each.

The ABA represents a long-term commitment to the continuous improvement of systems supporting the processing of administrative workloads as well as technologies to effectively deliver timely, accurate and relevant information concerning such processes. The ABA will be developed as an enterprise solution, facilitating the integration of disparate administrative source systems and to recognize data created in such systems as a corporate asset. While the ABA is a long-term strategic initiative, it will be implemented incrementally. This will enable SSA to continue to leverage its legacy applications while gradually replacing or subsuming them with new technology. Using this approach, the ABA will provide a framework for enhancing or replacing existing administrative systems, as well as adding new capabilities through the integration of COTS products as components of the ABA as these products mature in the Federal market.

Initial efforts are focused on:

- **Social Security Online Accounting and Reporting System (SSOARS)**
  This initiative replaced the previous Financial Accounting System with a COTS solution. While seeking to leverage the new technologies available in the marketplace, the initiative was also driven by the need to be compliant with established standards governing financial accounting systems in the Federal sector. A competitive acquisition process led to the selection of Oracle Federal Financials. The broader scope of the Oracle Federal Financials product over the predecessor FACTS system provides more integrated financial management software and replaces or subsumes cuff systems such as FIS. Additionally, SSOARS web technology allows greater access to financial data in SSA field offices.
- **Third Party Payment System**
  The Third Party Payment System (TPPS) Release 3.0 has replaced the predecessor client/server application and local databases maintained in approximately 1500 sites nationwide. The application supports the issuance of checks for emergency beneficiary payments as well as payments to both employees and vendors. TPPS Release 3.0 provides a single data entry of programmatic payments to ensure that Immediate Payments (IP)/Emergency Advance payments (EAP) are appropriately generated and correctly recorded on all systems of record.
- **Travel Manager**
  TM Release 8.1 was implemented in support of SSA's long-range vision to develop a fully integrated, electronic, paperless Travel Management System that integrates with the Agency's accounting system. This Web-based release serves SSA employees located at headquarters offices in Baltimore, Maryland,

Washington, D.C., and Falls Church, Virginia, and in 10 regional offices and approximately 1,400 field and hearings offices throughout the United States.

- **Benefit Certification and Accounting System (BCAS)**
  BCAS Release 3.0, completed the automation of the title VIII/title XVI Certification and Accounting process being used at SSA. Requirements definition is underway for BCAS title II. BCAS supports the Division of Benefit Certification and Accounting (DBCA) in certifying and accounting for payments made through the Department of Treasury.
- **Payroll Operational Data Store**
  The Payroll Operational Data Store (ODS) initiative replaced the legacy database that housed payroll data and generated SSA's official Payroll Analysis Recap Reports (PARR) and Full Time Equivalency Tracking System (FTETS) reports. The Payroll ODS reduces staff workloads by providing timely payroll information which can be joined with staffing reports to accurately determine component labor costs.
- **Human Resources Management Information System (HRMIS) Replacement**
  HRMIS is the core legacy application supporting the capture and reporting of human resource data. The replacement strategy will provide the means of transitioning support of these workloads to architectural based solutions. The objectives include upgrading the technology, improving data capture, delivering management information consistent with the MI Architecture and establishing the means of integrating external sources of human resources data (e.g., short-term best of breed initiatives, Application Service Provider).
- **Human Resources (HR) Operational Data Store (ODS)**
  This initiative provides for improvements in the access to, and processing of, data from HRMIS. It represents an initial step toward HRMIS Replacement and the delivery of administrative data under the Management Information Architecture.
- **Short-Term Best of Breed Initiatives**
  The Agency continues to look for opportunities to leverage COTS, GOTS and Application Service Provider offerings in the management of its administrative business processes. Consideration was given to commercially available enterprise human resources solutions; however, it was determined that the Federal market for such COTS solutions required further maturation. While waiting for a viable long-term solution, the Agency is expediting a few short-term initiatives to acquire Best of Breed COTS/ Application Service Provider solutions to support critical workloads (e.g., recruitment).

Management Information

Management information (MI) is the full range of data and information that SSA staff at all levels needs to manage the workloads, programs and resources for which they are responsible. MI is developed and produced as an integral part of programmatic and administrative processes, as cost-effectively and unobtrusively as possible.

A major initiative is underway to improve MI throughout the Agency. The SSA Unified Measurement System (SUMS) and Managerial Cost Accountability System (MCAS) effort is to improve the quality, consistency and access to information used by managers and analysts throughout SSA to manage work and account for resources. SUMS/MCAS will provide access to information needed to meet changing business requirements, support process reviews and comply with government standards for cost accountability. To accomplish these goals, the systems that collect MI must do so in a consistent and flexible manner. This project involves modifying current systems as well as creating new methods for capturing information on workloads throughout the Agency.

MI is addressed from several perspectives at SSA to support the different levels of management. It can be categorized as workload management, work measurement, and general management information. An additional MI focus is to migrate new and existing systems to the MI architecture. This is shown on page 126.

Workload Management

Workload Management is the operational MI required to manage day-to-day programmatic operations. Detailed and summary workload information for managers and staffs in the field offices, teleservice centers and PSCs is monitored. Specific events are tracked through the claims' life cycle. This ensures that cases are worked in a timely manner. Workload management is also used to identify workloads requiring special attention and workflow problems. Work that is transferred from one office to another may also be tracked.

There are Workload Management Systems (WMSs) for specific programmatic application areas. WMSs are an integral part of the programmatic project effort and generally coincide with new releases of programmatic software. Workloads are categorized as received, cleared and pending. Summary and detail listings and online queries are available to field offices. Standard reports of clearances and pendings are also available to the area directors, regional offices and field offices.

Work Measurement

Work measurement is the summary MI that quantifies the work that needs to be done to achieve the Agency's objectives. This includes work performed in the field offices and DDSs. The primary components of work measurement are workloads, work sampling, processing time and work hours. Work measurement information supports a variety of management functions:

- Estimating resource needs;
- Justifying budgets and staffing requests;
- Planning for recruitment;
- Determining cost of workloads, functions and programs administered by SSA;
- Assessing productivity of SSA components;
- Allocating staff;
- Accounting for SSA's performance to upper management; and

- Analyzing operations, process and productivity changes.

Work measurement is a critical management tool. It produces data for all types of work activity and at all levels of management. This includes managers in the budget, human resources, integrity reviews, policy and operations areas. There are several systems that support work measurement.

The work measurement systems provide SSA managers with an integrated, summarized view of work measurement data. These systems receive programmatic and MI data on workloads, processing times, work sampling and time and attendance from numerous sources. Summarized data from these sources are edited, formatted and stored. Regional Office, PSC and Central Office users are able to retrieve and manipulate data and produce ad hoc reports.

General Management Information

Several systems provide summary and strategic level MI that is used for activities such as trend analysis, quality assurance and summary level reporting. Overall MI requirements are defined as an integral part of the programmatic project effort. These systems produce various MI reports associated with earnings, title II and title XVI claims processing, the national 800 telephone number network, and debt management.

Management Information (MI) Architecture

The figure, *Management Information Architecture*, depicts a completely new look from the way MI has been delivered in the past. Formerly, MI systems were designed independently from the programmatic and administrative systems that feed them

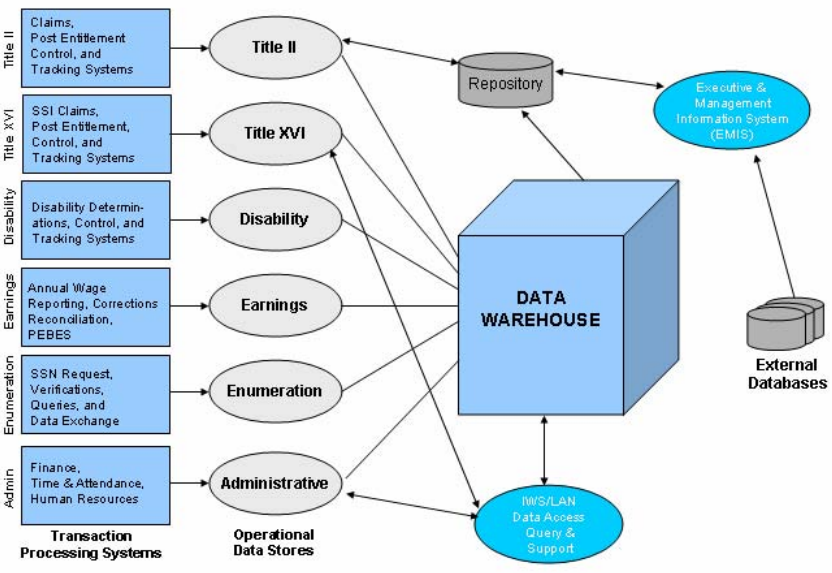


Figure 22: Management Information Architecture

data. Each new system had a unique design, so that customers frequently had to access many different systems to obtain the information they needed. With the establishment of the MI architecture, all significant new MI development will be delivered through this infrastructure. Standards have been developed so that the type of data to be stored determines which portion of the architecture will house it. Additionally, there will be standardization of the access methods to the data as well as its delivery mechanisms.

The MI Architecture, depicted in Figure 22 above, consists of four components: Operational Data Stores (ODS), Data Warehouse, the Repository, and the Executive and Management Information System (EMIS). Data extracted from both the programmatic and administrative transaction processing environments is organized and stored in ODS. These are designed along functional lines (e.g., disability, title II, title XVI, etc.). ODS are structured and stored on the mainframe using DB2 as their Relational Data Base Management System. The MI architecture is being developed incrementally. Initial releases have occurred as shown in the shaded sections of the diagram. Additional releases are planned in each of the functional areas until the architecture is completely implemented.

The ODS data is then extracted using software tools and structured in a Data Warehouse, managed by Oracle operating on high-end data base servers. The data is organized and summarized at different levels to support various types of queries and Online Analytical Process needs. Historical data is also managed by the Data Warehouse. Because of the volume of data needed to support the decision making process, data will be archived and made available when historical information is needed.

The target MI architecture is supported by an active, robust and fully functional repository that manages the metadata for those elements housed in other architecture components.

The EMIS serves as the delivery mechanism for the architecture, giving the MI customer direct access to Agency mission critical information to support their daily decision making, planning and oversight activities. Hard data (i.e., measurements, counts, processing times) will be provided through connectivity to the Data Warehouse, ODS, and other key data bases. Soft data (i.e., Agency goals, plans, and strategies) will be provided through various techniques made available through web-enabled technologies.

This architecture is accessible through the IWS/LAN. Users of the architecture will be able to extract, query and manipulate data with COTS access tools. The data access capabilities are designed to support open ended access tools to meet the different needs of SSA's diverse MI customers.

Technology such as Operational Data Stores, Data Warehousing, the Repository, and the EMIS provide more efficient and timely management information and decision support capabilities to SSA management at every level.

Data Architecture

SSA's data architecture consists of three major components, as illustrated in Figure 23 below. The central component is the data; the other components provide support functions dealing with the data. SSA classifies its data holdings within three major groupings: programmatic, administrative, and management information (MI). The programmatic group is made up of data that are collected (or generated) to support SSA's programmatic mission. Programmatic data entities are clients, legal representatives, business partners, etc. The administrative group consists of the data used to run the Agency and manage its personnel, budgets, physical plant, etc. MI data are produced to measure performance characteristics of both programmatic and administrative processes.

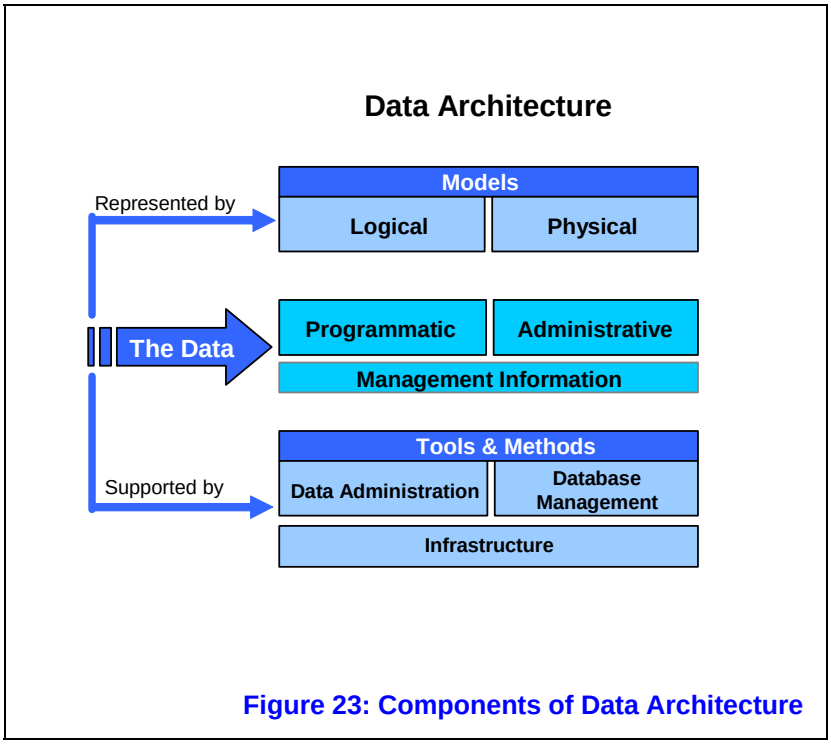


Figure 23: Components of Data Architecture

The second major component of the SSA data architecture consists of the models that represent existing and planned collections of data. There are logical and physical data models. Logical data models are typically developed early in the life cycle development process to help define and document 'what' data are needed to support a planned new software application. (In Enterprise Architecture terminology, logical data models illustrate the planner, owner and designer views of data.) Physical data models represent the database manager's view of data and illustrate 'how' the data are to be physically stored to meet update and retrieval performance requirements.

The final component is the collection of tools, storage infrastructure technologies, and operating methods that are used to support data administration and database management. Tools include commercial off-the-shelf (COTS) products such as data modeling packages, data dictionaries, and database management systems (DBMSs).

Infrastructure includes various types of physical storage devices as well as operational support such as database backup and recovery, disaster protection, and archival storage.

Figure 24 below further illustrates the component structure of SSA's Data Architecture, within the architectural subdivisions established by SSA's Enterprise Architecture (EA) Framework:

- The upper one third of the diagram depicts data administration functions related to the creation of logical data models. The SSA Data Resource Management System (DRMS) is shown as the central support tool for the data administration processes. The labeling on the right-hand edge indicates that detailed information about these functions is provided in the EA Data Architecture (Data Administration Sub-architecture). Summary information is provided on page 130 of this document.

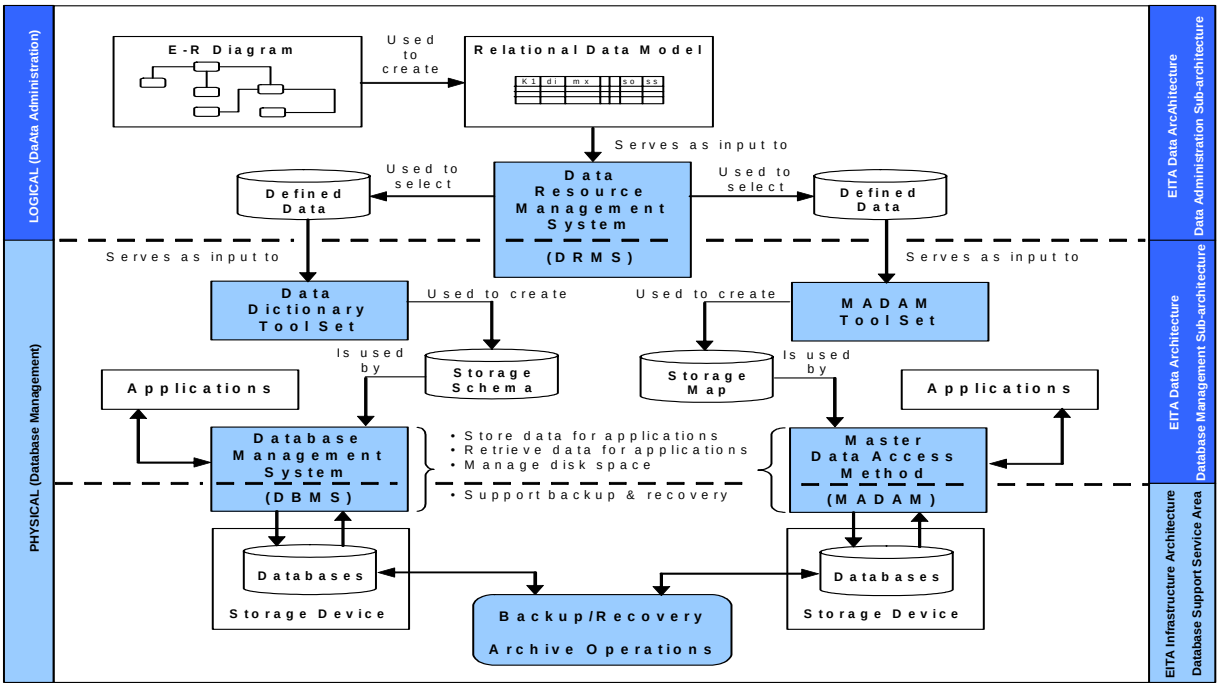


Figure 24: Assignment of Data Management Functions to Architectural Components

- The middle section of the diagram depicts data base management functions related to the creation and management of physical databases. The DRMS is shown as a shared support asset for these processes, but the primary support tools are database management systems (DBMSs). Two broad categories of DBMS and DBMS-like tools are shown (1) COTS DBMS packages and (2) the SSA developed Master File Access Method (MADAM). The labeling on the right-hand edge indicates that detailed information about these functions is

provided in the EA Data Architecture (Data Database Management Sub-architecture). Summary information is provided beginning on page 132.

- The bottom one third of the diagram depicts database support technologies and functions provided by SSA's Office of Telecommunications and Systems Operations (OTSO). The labeling on the right-hand edge indicates that detailed information about these functions is provided in the EA Infrastructure Architecture (Database Support Service Area). Summary information is provided beginning on page 136.

Data Administration Sub-Architecture

The Data Administration Sub-architecture consists of an integrated set of IT technologies and life cycle procedures that support the SSA Data Administrator in achieving the following strategic objectives:

- Promote discipline in the creation of new databases and the expansion of existing databases and 'master record' files;
- Ensure that all parties involved in the application development process understand the true meanings and definitions of the data that they intend to collect, use and store;
- Provide tools and data services that facilitate application development and maintenance;
- Promote standardization in data definition and usage (such as, naming conventions, determining valid data values, data formatting);
- Avoid the creation of redundantly stored data (except in cases where the physical database design process indicates that *planned redundancy* is necessary for performance reasons); and
- In partnership with SSA security officials and database management staff, ensure the integrity and security of SSA's valuable data resources.

To realize these objectives, the Data Administrator and Division of Enterprise Architecture and Data Administration (DEADA) staff work with users and application development teams to identify the specific data that will be needed for successful system implementations. During these work discussions, various data models are developed to illustrate concepts and document target data requirements. Logical data models are created using a combination of COTS software products and in-house developed support tools and procedures. These tools and methods constitute the Data Administration Sub-architecture.

Existing Data Administration Sub-architecture

SSA's existing Data Administration Sub-architecture is illustrated by Figure 23 on page 128. The life cycle products created using the Data Administration technologies and procedures are the logical data models specified by the EA Framework. Table 8 below shows the technologies currently used for the creation of these data models.

Data Administration Function	Support Technologies	Life Cycle Product(s)
Development of the semantic data model for an implementation segment or the enterprise; i.e., the 'owner's view' of data.	Computer Associates' *AllFusion Erwin Data Modeler*	Entity-Relationship (E-R) Diagrams
Development of the logical data model for a target database; i.e., the (application) 'designer's view' of data.	For relational database implementations: Computer Associates' *AllFusion Erwin Data Modeler*	Relational data models of target database tables
	For application implementations based on SSA's Master File Access Method (MADDAM): The SSA Data Resource Management System and SSA-developed utility tool set.	MADAM Record Specifications
Storage of data models and logical data element definitions.	The SSA Data Resource Management System (DRMS) that uses Allen System Group's *ASG-Manager* as the underlying DBMS.	DRMS query responses and generated record specifications.

Table 8: Components of the SSA Data Administration Sub-architecture

Target Data Administration Sub-architecture

SSA's data administration plans call for broadening the role of the DRMS, on an incremental basis, as new business functions are automated and existing application systems are replaced. Presently, the DRMS houses all of the programmatic data element definitions and selected data definitions for administrative and management information systems. The eventual goal is to enable the DRMS to serve as a common access channel to all SSA data element definitions and usage (including locally developed software applications). The following list identifies the major functional capabilities and design characteristics of our Target Data Administration Architecture:

- **Provide DRMS Access to Administrative, MI and Local Data Definitions**—As noted above, the eventual goal is to establish the DRMS as the common repository for all SSA data element definitions. Given the scope of such an undertaking, it is likely that an interim architecture will be employed during what is likely to be a lengthy transition period leading up to the realization of the eventual goal. The interim architecture most likely will establish middleware bridges between the DRMS and other SSA data dictionaries and meta-data repositories to enable the DRMS to index these data element definitions and *point to* the physical storage location of the detailed meta-data.
- **Use DRMS to Manage Data Models**—The DEADA technical staff plans to investigate the possibility of using the DRMS as a central repository for the various logical data elements developed and maintained for SSA business processes and associated applications.
- **Record Application Data Usage**—In order to facilitate software application maintenance, the DRMS will be used to identify the specific data elements

used by the various software entities (programs, modules, objects) in the SSA application inventory. This will significantly reduce the amount of time required to identify the applications that need to be changed for a new piece of legislation or a revised user requirement. It is expected that a COTS product, linked with the DRMS, will be used to read application source code to extract data usage information.

- **Replace Underlying Database Engine**—The DRMS currently uses Allen Systems Group's ASG-Manager product as it's underlying database engine. For a variety of reasons, ASG-Manager may not be well suited for our longer-term DRMS plans. The possible replacement of ASG-Manager will be thoroughly analyzed before embarking on the functional expansion of the DRMS.

Database Management Sub-architecture

The database architecture is made up of a combination of commercial Data Base Management Systems (DBMS) and specialized in-house developed software. Most of the Agency's data required by mission-critical applications is managed by Computer Associates CA-IDMS DBMS and SSA's in-house developed file management utility referred to as the Master Data Access Method (MADAM). In recent years, SSA has added two leading Relational Data Base Management Systems (RDBMS) to its architecture to support: distributed processing; the use of Commercial Off-the-Shelf (COTS) software; enhanced management information; a broader range of data access capabilities; and, in general, to provide more flexibility. The two RDBMS are Oracle on the UNIX platform, and IBM's DB2 on the OS/390 platform. The current architecture is depicted in Figure 25 below.

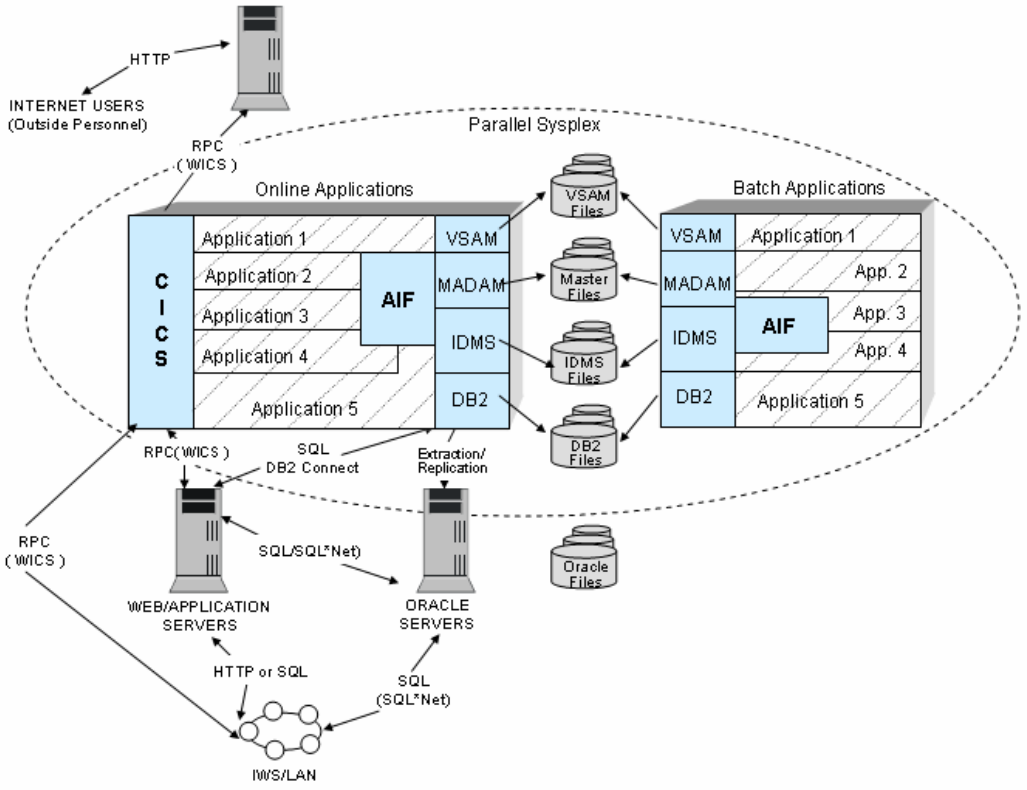


Figure 25: SSA's Database Architecture

MADAM, CA-IDMS, DB2 and Oracle each have their unique purpose within the database architecture. The MADAM software is used to support SSA's very large Master Files containing title II, title XVI, Earnings and Enumeration data. CA-IDMS is used to manage pending data for the Master Files, along with several of the legacy management information databases. Oracle is used for distributed applications that either benefit from the data being located closer to the user (non-centralized) or have departmental (non-enterprise) data requirements. DB2 is used for distributed or mainframe applications that either require or would benefit from a centralized enterprise RDBMS server on the mainframe. In addition, many of the COTS packages require a specific RDBMS, generally either Oracle or DB2, to operate efficiently.

Several different methods are used to access data within the architecture. Both Oracle and DB2 utilize the industry standard Structured Query Language (SQL) as the data access vehicle. An in-house developed interface utility called the Application Interface Facility (AIF) is used for access to programmatic CA-IDMS databases and online access to the MADAM-controlled Master Files. The AIF creates a generic interface layer between the application software and the CA-IDMS or MADAM software. Access to the Master Files from batch is accomplished mostly via direct MADAM calls although some of the batch access is through the AIF. Access to management information CA-IDMS databases is performed through CA-IDMS's native data manipulation language.

While most of the data access requests continue to come from mainframe batch processes or Customer Information Control System (CICS) transactions; several of the new or reengineered applications are being implemented as distributed applications. In some cases, processing is being distributed and special software is required to access the data. Access from IWS/LAN workstations to Oracle database servers is provided by SQL*Net which supports SQL calls either embedded in applications or housed in one of several ways including Stored Procedures and Open Data Base Connectivity (ODBC). Access from IWS/LAN workstations to the mainframe-based DB2 is handled via a middle tier platform running the DB2 Connect Enterprise Edition product. Similar to Oracle, SQL calls to DB2 can be embedded in application code or housed in Stored Procedures, ODBC, or some other standard data access middleware. Legacy data that requires client/server type of access from IWS/LAN workstations is being supported via Remote Procedure Calls (RPC) using SSA's developed Workstation Initiated CICS Servers (WICS) utility.

A number of tools have been acquired or developed to help control, administer and automate portions of the database administration workload. These tools help support key areas including: data modeling, data repository, management of data structures, performance tuning and database monitoring.

With the recent inclusion of RDBMS in the database architecture, the opportunity to improve both the development of databases and administration of SSA's data is being pursued. A step-by-step set of procedures was developed to help define the database development process and more importantly minimize the risk of bypassing key tasks. An intense data naming and modeling standards process was setup to carefully analyze any new data being stored in RDBMS to prevent redundancy of data definitions and inconsistencies among various databases.

Future Database Management Sub-Architecture

SSA expects that the future database architecture will look similar to the current architecture as depicted in the current database architecture diagram. The major difference will be a substantial increase in the number of databases and the amount of data supported by DB2 and Oracle. RDBMS will play a more prominent role in the database architecture and become the first choice for new or reengineered applications requiring databases.

With much of SSA's mission-critical data controlled by the in-house developed software MADAM/AIF and the aging CA-IDMS DBMS, efforts will be made to determine what portions of the data could be managed by DB2. The decision to move any data to DB2 will be made only after studying conversion issues, resource costs, performance impact and future requirements.

As SSA moves forward with developing applications for the Internet, data security and 24/7 data availability will become major challenges. The availability issue is being addressed on the mainframe through use of IBM's Parallel Sysplex architecture. This architecture allows multiple instances of a DBMS to operate on multiple boxes producing a single DBMS image. When a failure occurs to a given DBMS instance on one box, the remaining instances automatically take over the workload. This architecture also provides the ability to share data across multiple mainframes and perform parallel processing whereby all processors in the Sysplex are available for use. The current status is: MADAM software takes advantage of Parallel Sysplex technology today through the use of VSAM Record Level Sharing (RLS); the Agency has begun the process of moving DB2 databases under this environment and this technology is under consideration for CA-IDMS databases. Similar functionality will be made available for Oracle implementations via Oracle's Parallel Server technology.

Solutions for data security issues are becoming available in the marketplace. SSA will continue to closely monitor this area for new developments.

The forthcoming need to support large objects, images, sound and video will require SSA to consider the use of non-structured, object-based data types found in Oracle and DB2. This may be in the form of Binary Large Objects (BLOBs) or possibly even Extensive Markup Language (XML).

SSA is beginning to consider the use of Microsoft's SQL Server for small departmental-type applications requiring a database. A key characteristic of this type of application would be one that is not required to adhere to the full software development life cycle (SDLC). As SQL Servers begins to push into the departmental arena, it is expected that Oracle will be used to handle the Agency's mid-range database needs with DB2 continuing to be the choice on the mainframe for large databases. In addition to Oracle at the mid-range level there will likely be DB2 UDB databases implemented for COTS packages with specific DB2 requirements (i.e., IBM's Content Manager).

In support of the Internet and Intranet we will begin to see database connectivity changes. DB2 Connect will not be needed for web applications running under IBM's WebSphere and Net8 will replace SQL*Net for Oracle connectivity.

Tools that demonstrate a substantial return-on-investment and are key to improving support required of the database architecture will continue to be acquired as needed. If the vendors deliver on long-term promises of a consolidated tool set for Oracle, DB2 and SQL Server, SSA will pursue such tool sets.

Further improvements to the database architecture will be accomplished via the creation of a metadata repository that will provide the ability to track the data the

Agency collects, the meaning of the data, where it is used and eventually be a key instrument for the development of applications and databases.

Infrastructure Architecture

The architecture definition for IT Infrastructure consists of logical and physical diagrams for 15 infrastructure service areas along with supporting narrative descriptions. It also includes a database of detailed component information including make, model, version of the IT hardware and software infrastructure products currently used by SSA. All of this infrastructure information is accessible via the SSA Intranet. Discussion of the service areas follows.

The logical diagrams, which are the focus of this section of the IRM Plan, define the current strategic level infrastructure support functions for all of SSA's systems activities. As such, SSA would not expect them to change often, and when they do, it would be as a result of an executive decision to pursue a significantly different path. As described later in Chapter 6, Transition Strategy, SSA is establishing a formal process for reviewing the enterprise architecture and setting targets for its pieces. This process is just beginning, so none of the infrastructure service areas have approved target architectures at the present time.

The 15 service areas do not represent 15 distinct and separable functions or structures. Instead, they fall into several logical groups, which often connect and occasionally overlap. Figure 26, *Service Area Relationships* on page 137, is one approach to depicting these complex relationships.

The relationships between the service areas, and hence the boundaries between them, will continue to be refined as the Agency proceeds to define the target architectures.

There are a couple of key entities upon which the infrastructure architecture is built. SSA has built a hybrid centralized/distributed node infrastructure to support its many direct-service offices and processing centers nationwide. The two primary support locations are as follows.

- The **National Computer Center (NCC)** is SSA's centralized location for IT processing. It houses most of the processing platforms, technical applications and resources needed to support the Agency's computer business applications.
- The **Remote Operations Control Centers (ROCCs)** are remote nodes located in Pennsylvania, New York, Illinois, Missouri, California, and Alabama. These centers house servers, applications and additional resources needed to support the SSA business applications that run outside of Headquarters.

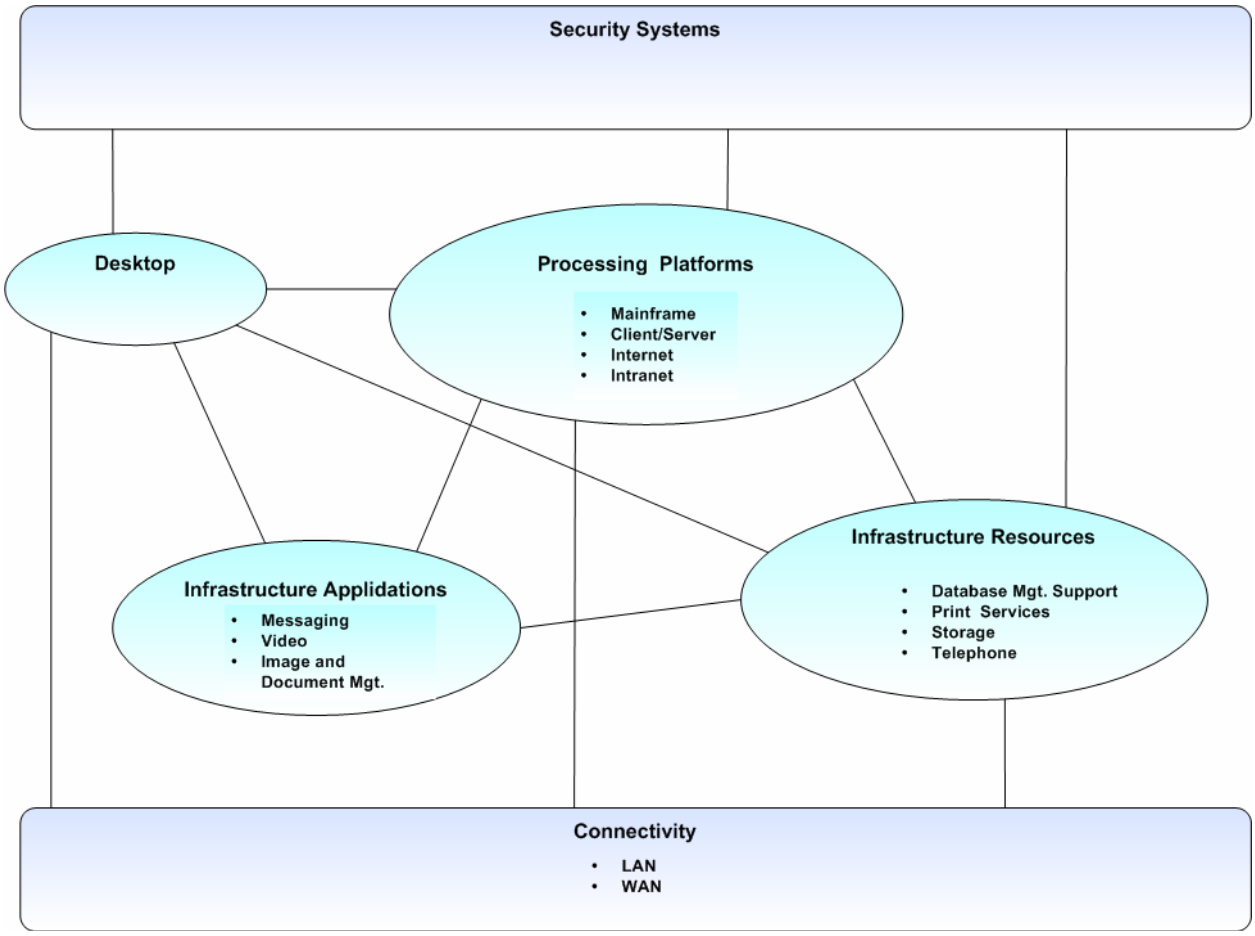


Figure 26: Service Area Relationships

The relationship between the NCC and the ROCCs, and the platform where any particular application or resource resides, is continually evolving. As the Agency develops the target architectures over the next several years, this will be one of the key issues it will address.

Client/Server

Service Area Definition

The Client/Server service area defines the hardware/software infrastructure and processes required to support the applications and functions that reside on a variety of non-mainframe servers and are accessed directly from the desktop.

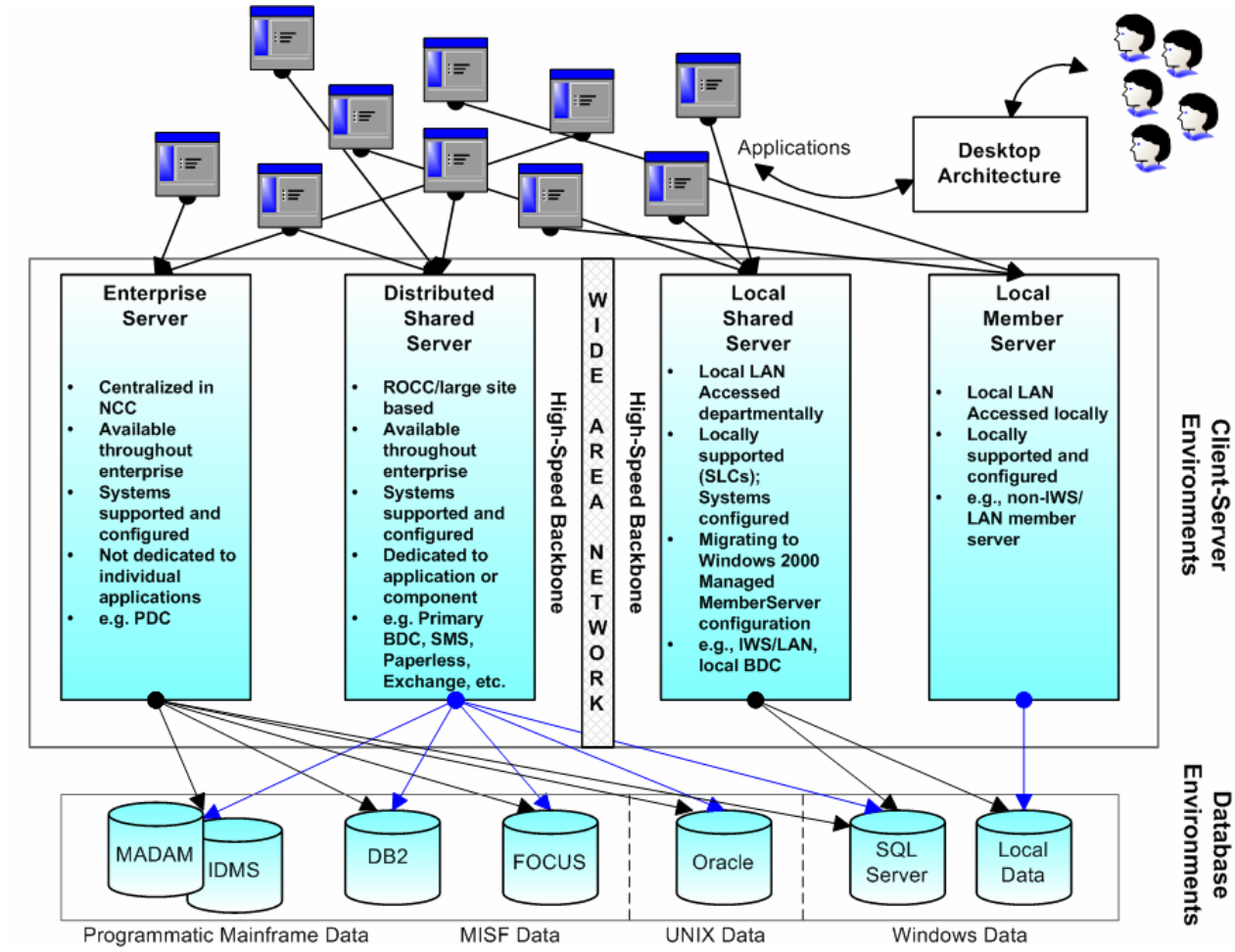


Figure 27: Client/Server Architecture

Current Architecture

There are four environments depicted in the logical diagram, which are differentiated by their physical locations and by who configures and supports them. First, the Local Member Server and the Local Shared Server are managed by staff in the office where they reside. Local servers refer to those servers that are physically located with all the components locally attached, in the case of the a single segment site such as a field office, or in the case of a multi-segment site, with components located on the building backbone. Conversely, the Distributed Shared Server and Enterprise Server are a suite of servers which are remotely controlled and operated by Office of Systems (OS) personnel.

Access to the client/server processing platform is only available from the Desktop architecture. There is no direct, end user interaction with any of these environments.

The **Local Member Server** environment is almost entirely managed by the local office staff. OS is responsible for loading the base image on these servers, providing the operating system and security software footprint to connect to the network. From that point on, local staff provide the support and services necessary to manage them on a daily basis, including support for any locally-installed applications. Applications available in this environment are intended for local use only, and any devices needed by the applications are available on the LAN.

The **Local Shared Server** environment is in a state of transition. In the original IWS/LAN architecture, the local shared server is the Backup Domain Controller (BDC). However, OS is now in the process of replacing this device with a new local shared server called Managed Member Server (MMS). This server is configured and maintained by OS. Local staff are not permitted to add any new software, but the Site LAN Coordinator (SLC) is responsible for all backup and recovery operations. Everything that runs on this server is intended for customers locally attached to the network.

The **Distributed Shared Server** environment is strategically placed where there is sufficient bandwidth and within a managed facility to provide a high level of service. The software is managed and fully supported by OS, and all backup and recovery operations are performed by OS as well. The applications and services available from these servers are available throughout the enterprise. The servers are large site based, generally located in the ROCCs or on the Building Backbone. They are engineered for the higher speed network services.

The **Enterprise Server** environment is located at the NCC. The applications and services are available to the enterprise, and not dedicated to any particular application. They provide access to the Mainframe and Intranet architectures. These servers are fully managed by OS, on a 24/7 support basis, including full backup and recovery operations. They are also engineered for the higher speed network services and are placed in the highest security environment.

The diagram shows the **Database Environments** (within the Database Management Support service area) with which each server may interact. However, there are performance issues that must be considered. The proximity of the database relative to the requesting server is important and may affect performance. The database and the requesting server should be on the same high speed network because once the request crosses the network boundary, there may be performance degradation. In fact, any hardware device that is frequently accessed should be co-located with the server requesting that device.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. The Client-Server architecture is relatively stable. At this point in the development process, it does not appear that the SSA client-server

architecture will change much at the logical level, but rather, at the physical implementation level. These changes will largely be driven by the potential changes in the ROCC structure, as well as evolutionary upgrades for the existing products and associated hardware, in particular the Microsoft Windows platform, including the Active Directory services.

Transition

SSA is currently planning to implement Infrastructure File Servers, software and services that form the "core" of the Agency's client-server architecture. These devices assume the Windows roles of Domain Controllers, SMS Infrastructure devices, Dynamic Host Protocol (DHCP) servers and other functions that support the workstations and file servers "underneath" them in the Windows architecture. These devices are physically located in the ROCCs. In addition, the Server Consolidation project will replace all backroom NT 4.0 backup domain controllers, user ring file servers, enterprise network management servers and application member servers with Windows 2000 Managed Member Servers with comparable functionality.

SSA is waiting for the release of Windows.Net Server before resuming Active Directory research and development activities. Windows.Net Server is expected to introduce several enhancements that will result in a much more manageable Active Directory, particularly when implemented in an environment such as SSA's. Windows.Net Server is currently projected to be released in the Fall of 2002.

When implemented, Active Directory will allow systems to delegate every day systems tasks to personnel more suited to this activity. This will also permit us to eliminate the third party product now used to manage NT user accounts security.

Migrating to Windows 2000/XP will provide a number of features that the Agency should leverage, namely:

- Better Mobile Computing Capabilities—Windows 2000/XP includes features that will allow the Agency's mobile users to connect easily to our network remotely and to connect to SSANET when they are based in the office;
- Distributed Administration—The Active Directory includes a feature to delegate routine tasks to personnel suited to the activity. In addition, we will be able to eliminate some of the third party products we are currently using to manage NT security;
- Better Client Management—Windows 2000/XP has several features that simplify client software installation thus lowering the Agency's total cost of ownership for our computing resources;
- Smart Card Support—The Agency is exploring the use of physical logon mechanisms to authenticate users of our systems; Windows 2000/XP has native support for these systems; and
- Remote Installation Services—Windows 2000/XP will enable SSA to install an entire desktop image from a remote server, again reducing the Agency's total cost of ownership for the desktop.

Database Management Support

Service Area Definition

The Database Management System (DBMS) Support service area defines the hardware/software infrastructure and processes required to operate all of SSA's DBMSs, which house all of the information used to process the Agency's critical workloads.

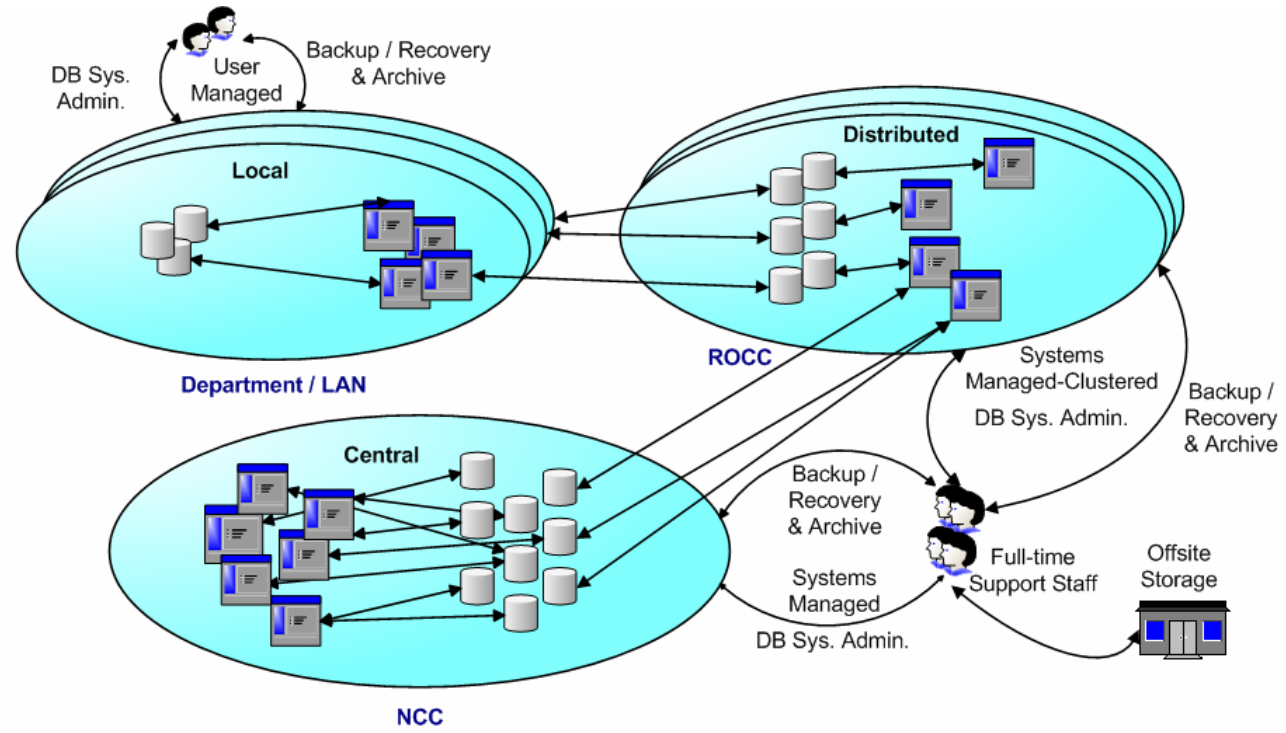


Figure 28: Database Architecture

Current Architecture

This section describes the logical environments that are depicted in the Database Management Support logical diagram.

The **Central** databases housed in Baltimore on the central IBM mainframe computers are Computer Associates CA-IDMS and IBM DB2. All new applications are using DB2 for the database management system (DBMS). Activity against the databases comes from CICS transactions, batch programs, and from distributed applications via DB2 Connect. Some applications are in a data sharing environment that provides added reliability, better performance, and no single point of failure for the application database access.

The **Distributed** databases supported in Baltimore and the SSA ROCCs by the Office of Systems are Oracle on mid-sized Hewlett-Packard (HP) computers using HP-UX, a UNIX operating system. Activity for the distributed databases comes from

client/server applications as well as application servers. Many applications are supported on a high availability cluster where two machines back up each other and in failure situation will immediately pick up the workload of the failing machine. A unique distributed database platform IBM DB2 UDB on Solaris is implemented in support of the COTS package IBM Content Manager.

Local applications are supported with MS SQL-Server on a Windows 2000 operating system. This platform supports the "collaborative" (non-Office of Systems) applications developed at SSA. Workload balancing is used to provide better response and avoid a single point of failure.

Many local application databases are also built and managed by local staff in offices throughout SSA. The two primary DBMSs used for these applications are MS SQL-Server and Microsoft Access. Access is supported as a software tool within the Desktop architecture, but in either case the actual databases developed in these local applications are entirely administered by local SSA staff.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. The Database architecture is relatively stable. At this point in the development process, it does not appear that the SSA Database architecture will change much at the logical level, but rather, at the physical implementation level. These changes will be driven largely by the target Data and Database architectures described earlier in this chapter, ongoing server consolidation, and evolutionary upgrades to the existing products and associated hardware.

Transition

SSA is committed to growing and managing a shared database server infrastructure in order to effectively manage Oracle and 3rd party software license costs. The number and size of new applications targeted for this environment are growing quickly. Also, in outlying years, SSA is committed to standardizing onto fewer UNIX platforms by recompeting the Oracle database server platform in FY 2005/FY 2006. By consolidating UNIX vendors, the Agency will benefit from a more targeted skill set and a more focused administrative requirement.

During FY 2004 additional DB2 applications will be migrated to the data sharing environment for added stability. The Office of Systems will continue to rollout major releases and maintenance to the DBMS products on all platforms.

Desktop

Service Area Definition

The Desktop service area defines the hardware/software infrastructure and processes required to provide virtually all SSA and DDS employees with a robust computing platform at their workstations.

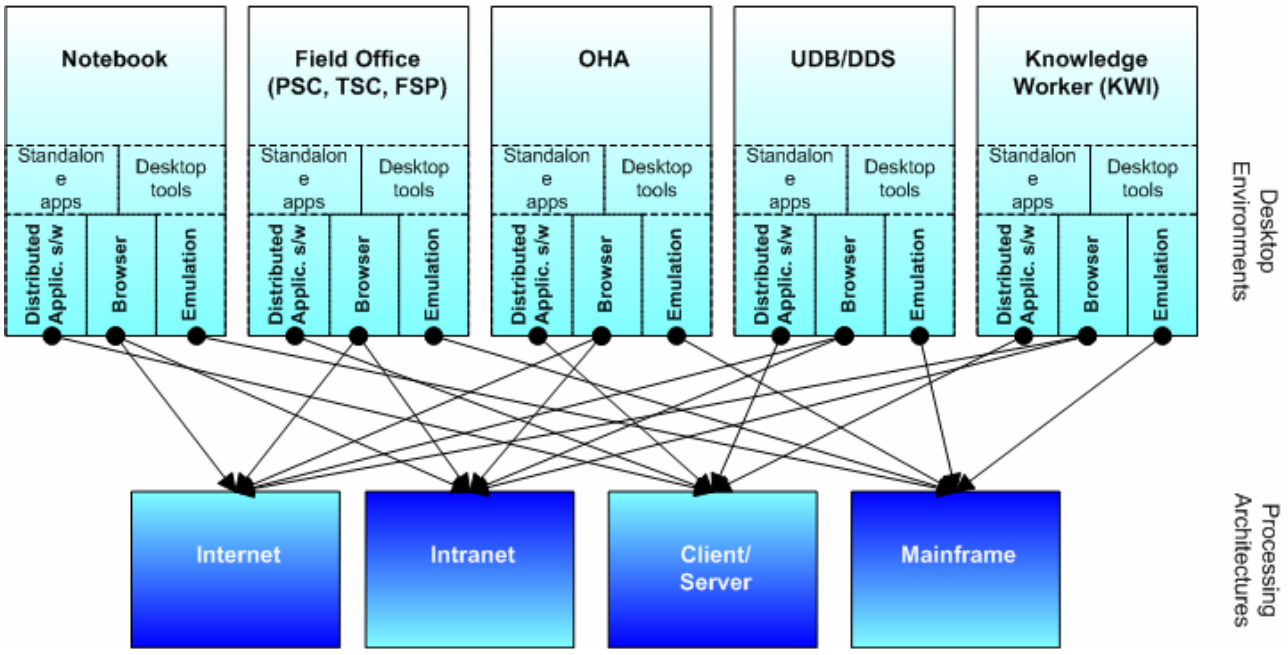


Figure 29: Desktop Architecture

Current Architecture

There are four major, distinct environments in the Desktop architecture, each of which may connect to the defined processing architectures as shown in the figure above.

The **Field Office (FO)** configuration was the first one developed for the original IWS/LAN, and it still provides the desktop for SSANet's many field offices. It is also the baseline for three additional closely related configurations: the Program Service Center (PSC) configuration, the Teleservice Center (TSC) configuration, and the Foreign Service Post (FSP) configuration, which are each built as a FO configuration with additional environment specific applications included.

The **Office of Hearings & Appeals (OHA)** configuration includes specific applications and tools developed to meet the business needs of OHA. While this configuration has some of the same pieces as the FO configuration, the file structure, start menu and desktop are unique to this environment.

Similarly, the **Universal DDS Backbones (UDB)** configuration has been developed to meet the needs of each of the states' Disability Determination Services. Both the OHA and the UDB configurations include applications that are not found on the FO or FO-based configurations.

The **Notebook** configuration has been developed to provide laptop users with remote access to SSANet through the Virtual Private Network and SmartCard technologies.

Lastly, the **Knowledge Worker** configuration is primarily used by non-direct support employees (e.g., policy analysts, applications developers) located at SSA Headquarters or in the regional offices. It is purposely not "locked down" as are the other configurations, acknowledging the wide variance in user requirements in this environment.

Within each configuration there is also a specialized Employees with Disabilities (EWD) sub-build for employees who require those tools on their desktops.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. The Desktop architecture is relatively stable. At this point in the development process, it does not appear that the SSA desktop architecture will change much at the logical level, but rather, at the physical implementation level. These changes will largely be driven by the stated SSA goal of converting existing client/server applications to browser-based technology, the acknowledged 3- to 4-year technology refreshment cycle, and evolutionary upgrades for the existing products and associated hardware, such as the MS Windows platform.

Transition

SSA is encountering the same dilemma that many other IT organizations are facing; namely, as the Agency's desktop infrastructure matures beyond three years, should workstations be repaired or replaced? We have adopted Gartner and GIGA recommendations for a three-to-four year technology replacement cycle for desktops, and are currently in year 3 of the original replacements for approximately 26,000 sub-733 MHz desktop machines.

In addition, we have begun deployment of a nationwide software configuration upgrade to replace Windows NT, NS/Elite and MS Office Suite. The new configuration includes Windows 2000 Professional, PCOMM and MS Office XP.

Electronic Messaging

Service Area Definition

The Electronic Messaging service area defines the hardware/software infrastructure and processes required to provide e-mail and other related services to SSA and DDS internal users.

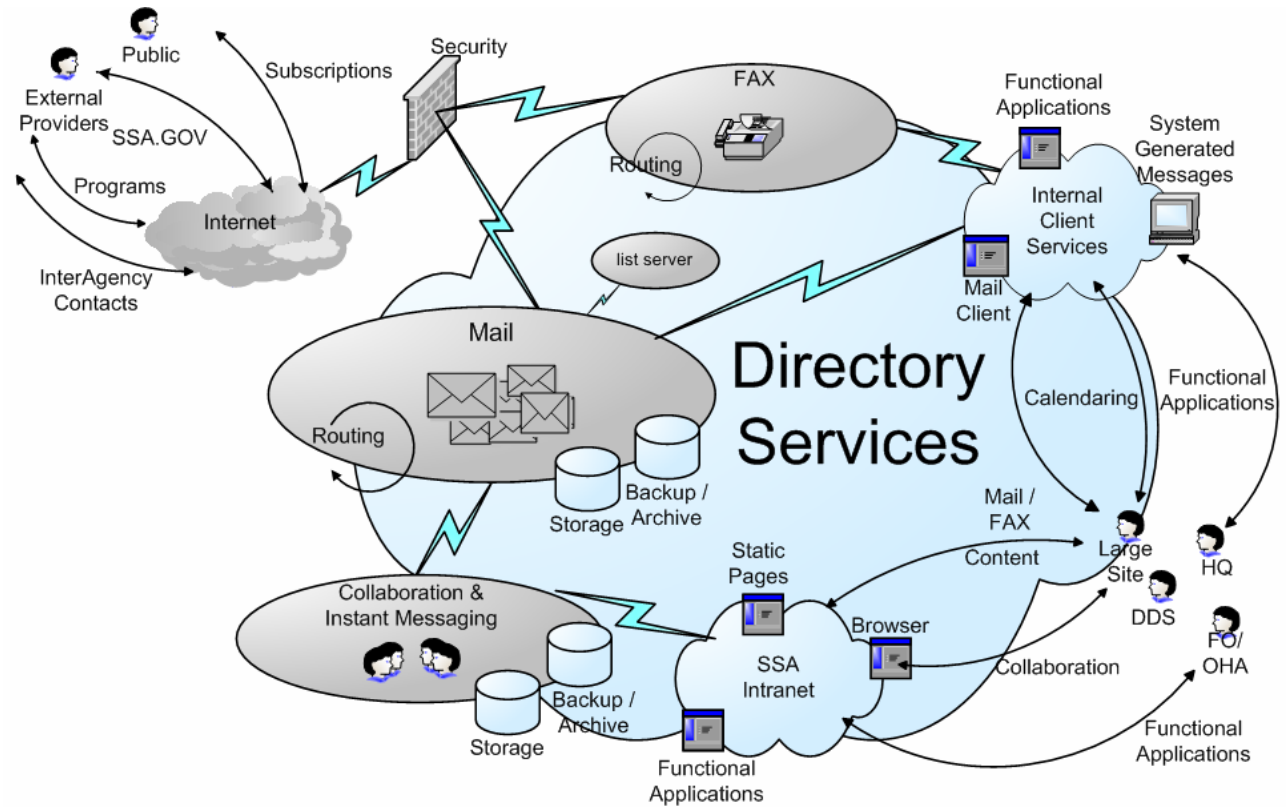


Figure 30: Electronic Messaging Architecture

Current Architecture

This section describes the logical environments that are depicted in the Electronic Messaging logical diagram.

The **Messaging** environment includes all types of asynchronous electronic messages that travel both inside SSA's network as well as over the Internet. Today, virtually every SSA and DDS employee is an e-mail user. E-mail has become a primary means of communication and documentation within and between operating components. The e-mail Architecture has the following 5 basic components or services:

- Database of users and addresses;
- Client/user interface tool;

- Mail generation, storage and routing facilities;
- Internet connectivity for mail outside the SSA network; and
- Mail archive and disaster/recovery storage facilities.

SSA's e-mail environment has approximately 80,000 users. Each user has a mailbox that is accessed via desktop software. Today, users can create mail, address it to any number of recipients, attach nearly any type of electronic file (e.g., documents, presentations, etc.) and send it across SSA or anywhere in the Internet. E-mail behavior is extremely variable and the demand for, and on, the e-mail architecture depends on the employee's position and their level of familiarity and sophistication with the e-mail tool.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. At this point in the development process, it does not appear that the SSA Messaging architecture will change much at the logical level, but rather, more at the physical implementation level. These changes will largely be driven by the Client/Server and Intranet architectures, the Microsoft Active Directory implementation, and evolutionary upgrades for the existing products and associated hardware such as the Microsoft Windows platform.

Transition

Various, significant upgrades to the Electronic Messaging architecture will take place over the next several years. These include: migrating Microsoft Exchange 5.5 infrastructure to Exchange 2003; piloting and deploying Exchange 2003 software and hardware to the SSANet environment, including DDS support and SSA's Internet Mail infrastructure; overseeing and applying corrections/fixes if required to the Exchange 5.5 hardware and software until all offices are upgraded to Exchange 2003; and overseeing and applying corrections/fixes as required to the Outlook Client software.

Upgrading SSA's messaging infrastructure at the communication hub Exchange sites, DDSs and other large sites will meet the requirements for the anticipated upgrade to Windows 2003/Exchange 2003 as well as for the increase in the demand for electronic messaging capabilities. Exchange 2003 enables SSA to better manage the growth of this traffic, provide better availability of e-mail services and consolidate the number of servers required to support this function. The upgrade to the e-mail system will result in better utilization of available bandwidth. In addition, upgrading the e-mail system provides SSA with the current version of messaging software in concert with the Agency's upgrade to Windows 2003. The upgrade also enables SSA to consolidate and significantly reduce the number of SSA servers that support e-mail.

SSA will pilot several Exchange 2003 configurations in conjunction with the Windows 2003 Active Directory pilots. Since Exchange 2003 must be installed in a

Windows 2003 Active Directory environment, the pilot schedule is completely dependent upon the Windows 2003 pilot schedule.

Additional electronic messaging functionality will be researched and tested for use in the SSA environment as follows:

- Many vendors provide **faxing** add-on capabilities to Exchange 2003. SSA is currently evaluating several products for integration into Exchange 5.5 as well as Exchange 2003. Integrated faxing will allow the desktop user to seamlessly send and receive facsimile documents from their e-mail client.
- Microsoft **Outlook Web Access** has been significantly enhanced in Exchange 2003. Used for remote, home, roving and occasional users, Outlook Web Access provides Web browser access to e-mail, scheduling (including group scheduling), contacts, and collaborative information stored in Exchange folders.
- SSA is designing a **Secure Mail** process which will facilitate the transmission and reception of encrypted mail and attachments. This project will address agency-wide, *internal* use of secure email and limited, *external* use of secure email with targeted business partners, e.g., other governmental agencies. This project will not employ Public Key Infrastructure (PKI), S/MIME, digital certificates or digital signatures.

Finally, until recently, internal user-based messaging was the largest infrastructural messaging workload. However, the architecture of the future must be expandable and scaled to accommodate some of the following initiatives promoted in SSA's Service Vision:

- direct outgoing communications with the public (e.g., news, notices, surveys);
- incoming public correspondence from www.socialsecurity.gov users including: interfaces to sophisticated e-mail and customer relationship management applications;
- messaging as a delivery vehicle for medical evidence requests and replies;
- internal and external document faxing using the messaging system routing capabilities;
- an infrastructure for secured (e.g., Public Key Infrastructure) messaging over the Internet;
- applications-callable mail service utilities for employee notifications (e.g., travel reimbursement advice, motor pool reservations, systems problem management ticket alerts, personnel actions, etc.);
- Internet accessible e-mail for mobile employees; and
- impending National Archives and Records Administration records retention criteria for e-mail data.

One project designed to meet these needs is the Electronic Medical Evidence / Public Key Infrastructure (EME/PKI) pilot. In this project, external medical providers send encrypted medical evidence to internal DDS offices. The messages—and medical

evidence attachments, are encrypted using digital certificates. Similarly, the external medical providers can digitally "sign" their message to prove to the DDSs that the message is authentic.

Imaging and Document Management

Service Area Definition

The Imaging and Document Management (IDM) service area defines the hardware/software infrastructure and processes required to capture, store, retrieve and archive images and documents. This service area also defines automated workflow systems that are incorporated through both COTS and SSA developed applications.

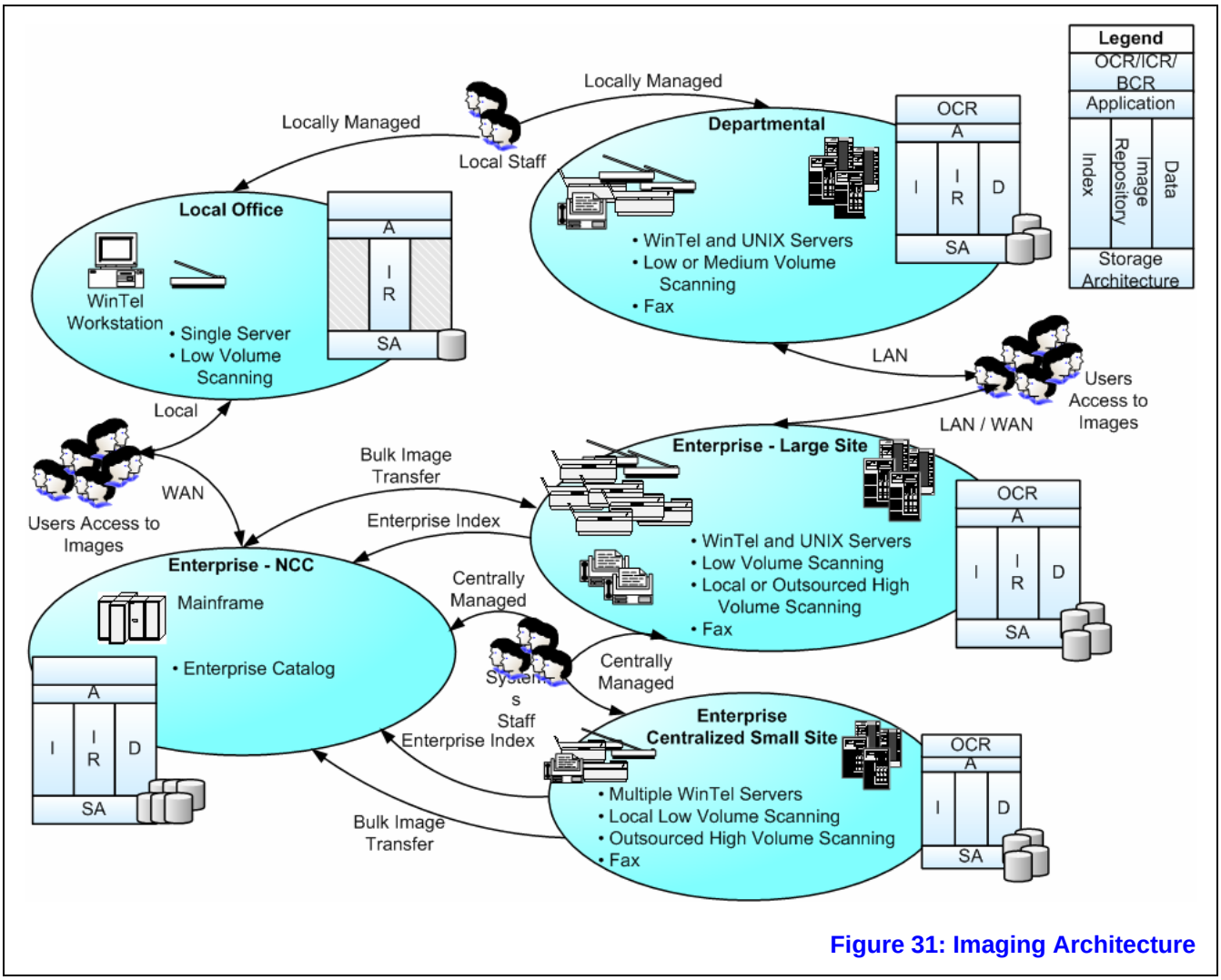


Figure 31: Imaging Architecture

Current Architecture

Figure 31 depicts the logical configuration of the existing and planned imaging and document management (IDM) systems in SSA. All are based on the Client-Server and Local Area Network (LAN) infrastructures and are compatible with the hardware, software, and client-server processing platform supported in this environment. Features of SSA's client-server architecture range from advanced client

operating systems, electronic data storage, data distribution, and integrated mail services to integrated fax services. Within the SSA network (SSANet) there are three environments supported by the Imaging and Document Management service area. They are Enterprise NCC, Enterprise Large Site, and Departmental. The last, Local Office, represents single-user or small-group scanning devices installed and supported by operations staff.

At a minimum, all IDM systems incorporate a scanning application, an image repository and a storage architecture. The primary differentiators for the various logical groupings are whether the systems are centrally managed by OS, whether they provide network access for their users, whether they support high volume or bulk image input, whether they incorporate optical or intelligent character recognition for text or bar code recognition for automated indexing technologies and separate indexing and data repositories. All of these factors are displayed in the diagram above.

With the exception of the Enterprise Large Site environment, all others represent planned, not implemented, architectures. The IDM system supporting the AeDib project will define the standards, configuration and products that are represented by the **Enterprise NCC** system. The IDM system acquired in support of the eFOIA project will define the standards, configuration and products that are represented by the **Departmental** system.

The Paperless Processing Center (PSC) System represents the **Enterprise Large Site** IDM architecture. It consists of a document management/imaging system built upon the client-server/LAN architectures. A combination of commercial-off-the-shelf (COTS) software and in-house programming was used to develop the Paperless system. SSA undertook the Paperless PSC project beginning in September 1993 to support the Agency Strategic Priority, "Begin to Turn SSA into a Paperless Agency by Establishing Electronic Folders".

The primary goal of the Paperless PSC project was to define an enterprise-wide solution, within the context of document imaging and paperless processing. Paperless PSC also addresses the storage, management, retrieval and routing of document images and electronic forms. Computer output, which represents the majority of the processing centers' paper workload, is being electronically downloaded into the paperless system. Incoming mail is being imaged and electronically routed throughout the process.

The implementation of the National Paperless PSC Software began in June 1999. To date, all 6 RSI PSCs, along with ODO and OIO are operating under the National Paperless PSC System. Since the initial implementation, there have been several software releases to address enhancements in both functionality and performance.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. The Imaging and Document Management architecture is one of those areas and will thus have a formally approved target before the end of

FY 2003. One key factor that will be considered in the development of the target architecture is the unique requirements of the fast-track AeDib project. But at the same time, consideration will always be given to the applicability of the architecture across the enterprise, i.e., to a wide range of applications which require this functionality.

In the short term, architectural changes may be at the physical level, based on basic evolutionary improvements, keeping current with vendor software and hardware releases.

Transition

The target architecture for Departmental and Enterprise NCC IDM environments will be defined during FY 2003 as part of the eFOIA and AeDib projects respectively. Minimal changes to the Enterprise Large Site environment of the Paperless Processing Center system are planned for FY 2003. Hardware refreshment and storage architecture upgrades to Paperless infrastructure were completed in FY 2002 and are not scheduled again until FY 2005. Refreshment of the Paperless scanners is targeted for FY 2004.

Internet

Service Area Definition

The Internet service area defines the hardware/software infrastructure and processes required to provide a means for businesses and the general public to electronically access SSA's public information and, increasingly, do business with SSA.

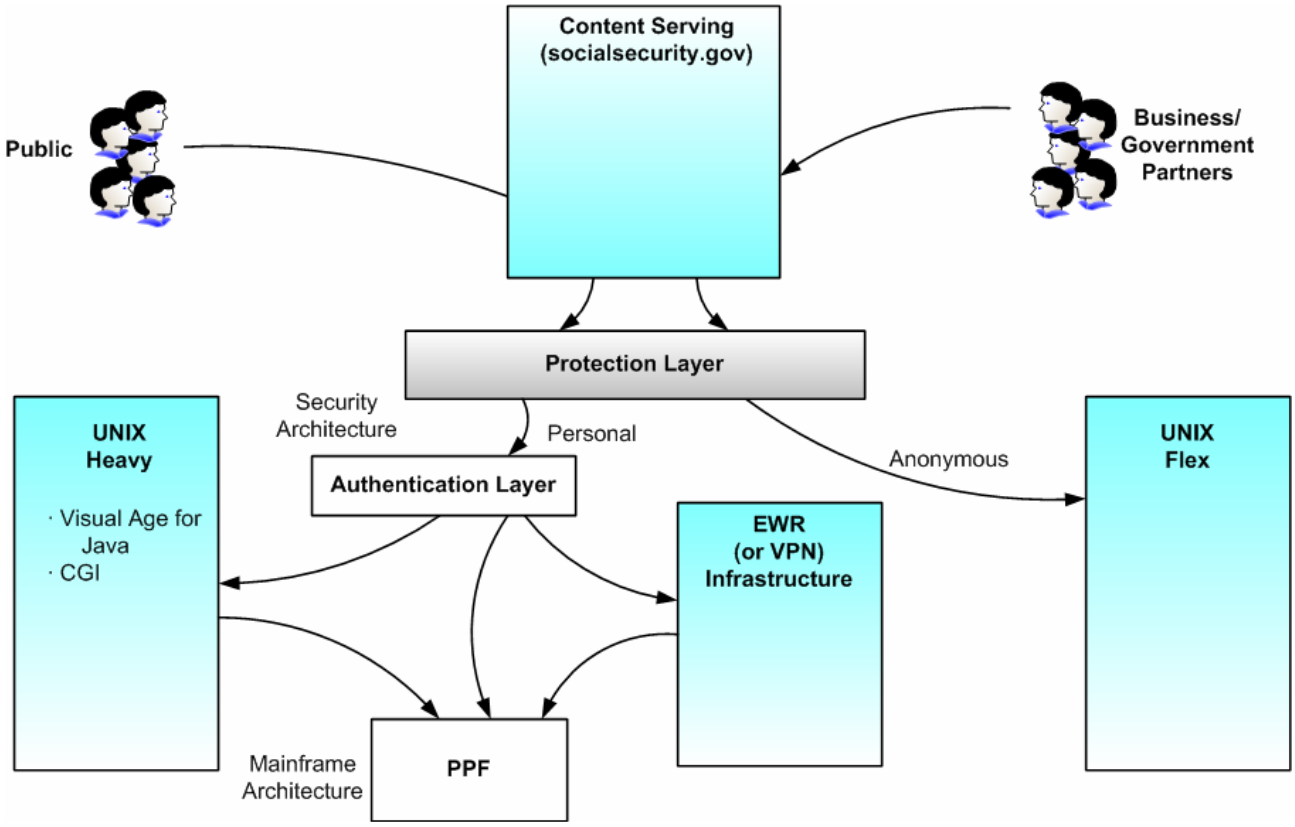


Figure 32: Internet Architecture

Current Architecture

This section describes the logical environments that are depicted in Figure 32.

The **Content Servers** house SSA's official Internet website (www.socialsecurity.gov). These servers provide information to the Internet community, both individuals and business partners, about social security benefits, procedures, history, etc. In addition, they provide links to online applications such as the *Social Security Statement*, Retirement calculator, Field Office Locator, I3368, etc.

The **Protection Layer** consists of a series of firewalls designed to protect the SSANet from Internet hacking activity and to provide a secure gateway to information to complete various applications such as the ones listed above.

The **Authentication Layer** is where user-identifying information, such as SSN, name, address, and date of birth, is verified, either through scripts or through coordination with the Mainframe.

UNIX Heavy refers to UNIX Web Servers that house WebSphere Application Server software. WebSphere is the Agency's standard development tool. The UNIX Heavy servers house various applications including the I3368 for AeDib and the Internet *Social Security Statement*. The applications connect on the back end to the MainFrame CICS, DB, and FOCUS data.

UNIX Flex is the environment housing all web applications and content developed under COTS packages and/or non-WebSphere tools. These include such applications as the Benefits Eligibility Screening Tool (BEST) and PolicyNet. Some of these applications have a back end to an Oracle database.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. The Internet architecture is one of those areas and will thus have a formally approved target. Key factors that will be considered in the development of the target architecture include the growth in "personal" applications available via the SSA Internet, and the evolution of web technology into the mainframe arena. But at the same time, the first consideration will always be the assurance of continued stability and capacity to support public access and use of SSA information and services.

In the short term, any architectural changes will be at the physical level, based on basic evolutionary improvements, such as keeping current with vendor software and hardware releases.

Transition

SSA has been providing statistical data to educational facilities and researchers via the Internet since 1989. In 1994, SSA established Social Security Online, an Internet site available at www.socialsecurity.gov, which allows the public electronic access to various SSA applications, publications, information, forms and employer information. Fifty-five million people will access Social Security services at our website, making us one of the largest providers of government services information via the Internet. With the planned addition of many new online applications, this number is expected to increase dramatically over the next few years. Users will expect a reliable, well-performing, and continuously available Internet experience.

SSA continues to develop customer-friendly, web-based applications from which the public can obtain information about SSA programs and policies. Online wage reporting, and other applications which encourage the public to contact the Agency electronically, are proliferating. SSA has begun development to put the entire suite of title II applications online, beginning with the RSI Claims process. This change stimulates expected growth throughout the planning horizon at socialsecurity.gov and supporting facilities.

SSA will begin an effort to migrate from UNIX based Firewall servers to Firewall network appliances. According to Gartner this is fast becoming the industry standard. The commercial support of the current platform shows signs of weakening. Thus, it is imperative that SSA positions itself for the future.

Intranet

Service Area Definition

SSA's Intranet service area defines the hardware/software infrastructure and processes required to provide a web-based information and processing platform for internal SSA users.

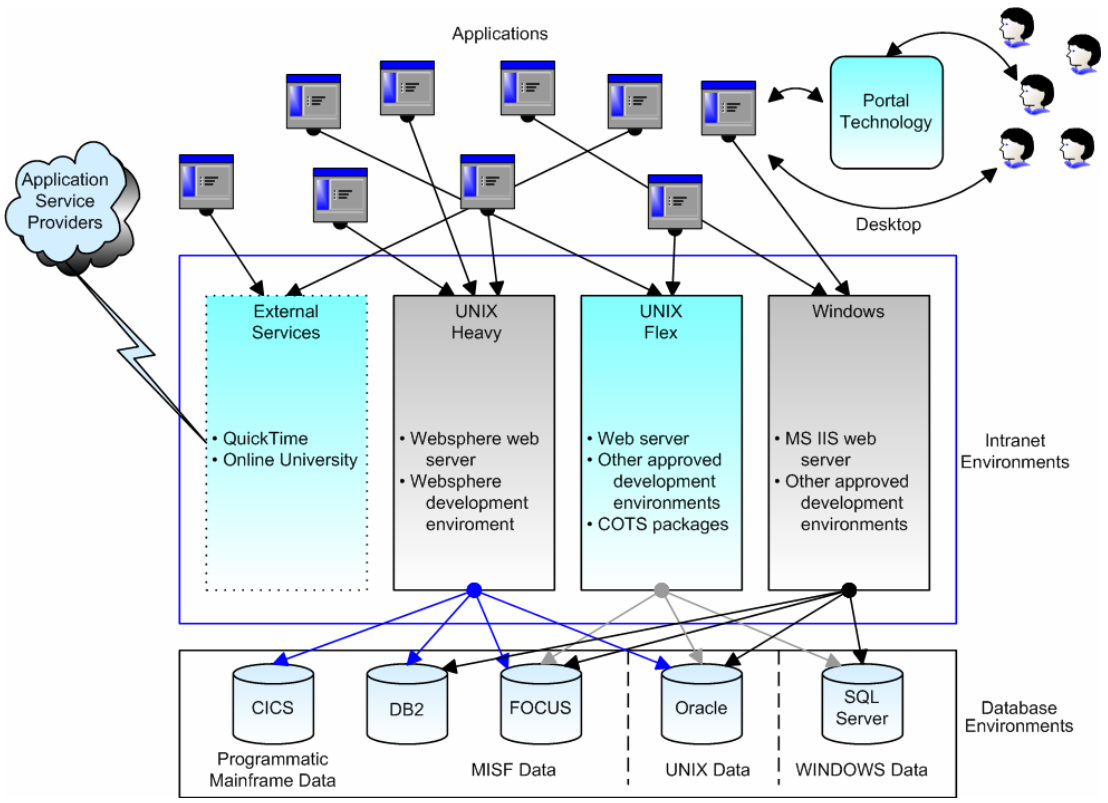


Figure 33: Intranet Architecture

Current Architecture

This section describes the logical environments that are depicted in Figure 33.

Access to External Services including the Internet, QuickTime, and the Online University from the SSANet is through the Access Firewalls. All LAN-attached workstations have access to the Intranet. Employees can locate web services using the eis.ba.ssa.gov home page or a plethora of host sites using dotted-decimal addressing, hyperlinks, or other registered names in SSA's domain name server.

The **UNIX Heavy** environment refers to UNIX Web Servers that house WebSphere Application Server software. WebSphere is the Agency's standard development tool. The UNIX Heavy servers house various applications including AeDib and Customer Help and Information Program (CHIP). The applications connect on the back end to

the Mainframe CICS, DB, and FOCUS data as well as the server-based Oracle Databases.

UNIX Flex is the environment housing all web applications and content not developed under the WebSphere Application Server environment. These are usually COTS packages and include such applications as the Employee Suggestion Program (ESP), Travel Manager, the Assignment and Correspondence Tracking System (ACT), and PolicyNet. Many applications have a back end to Mainframe FOCUS data, and Oracle and SQL databases.

The **Windows** environment houses various web and application servers including the Prisoner Tracking Management Information (PTMI) system, the SSA Digital Library, and Online Training courses. Many applications have a back end to the Mainframe FOCUS data, and Oracle and SQL databases.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. The Intranet architecture is one of those areas and will thus have a formally approved target. Key factors that will be considered in the development of the target architecture include the viability of the MS Windows web platform, the evolution of web technology into the mainframe arena, and the increased recognition of the role of collaborative software development at SSA. But at the same time, the first consideration will always be the assurance of continued stability and capacity to support the existing user and applications base.

In the short term, architectural changes will be at the physical level only, based on basic evolutionary improvements, such as keeping current with vendor software and hardware releases.

Transition

SSA provides Intranet functionality to its user community of approximately 80,000 employees located nationwide in the 50 states, as well as Washington, D.C., Puerto Rico, Virgin Islands, Guam and American Samoa. The Intranet provides access to up-to-date employee services and management information including job vacancy announcements, personnel information, SSA announcements, SSA Digital Library, as well as Intranet-based training. The Intranet supports a significant number of daily requests each year from the 64,000 SSA headquarters and field site employees and 16,000 DDS users. Requests will grow as more online services and/or existing applications are converted to web technology. The Intranet continues to be a dynamic and viable option in providing quality services to the SSA/DDS community.

SSA staffs nationwide have created a full range of Intranet application sites serving everything from static hypertext markup language (HTML) pages to complex active server pages and with linked database engines. The relative ease of deploying Intranet applications complicates global agency assessment of applications and network capacity planning. Budgeted applications such as the Employee Information Server, PolicyNet, Prisoner Tracking, SSA Digital Library, Process Engineering Tool, training, etc., are integral to the Agency Strategic Plan. Independent regional

office websites have been extensively developed to offer local applications and information to their geographically dispersed constituent offices. Given a server/workstation and readily available, end-user, budget priced tools, staffs have developed and deployed Intranet sites departmentally. For the most part, these applications deliver a local return-on-investment; however, they rely on or expect a perceived "free infrastructure" of unlimited communications services and ongoing operating budget support.

The Agency's plans for the Internet and Intranet are rapidly growing and changing; and thus OS expects initiatives other than the ones formally identified in this SSA planning process. New projects will be integrated into the existing infrastructure wherever possible; the project sponsors will fund various new Internet and Intranet projects that will require expansion and enhancement of the existing infrastructure.

In an effort to provide a robust platform within the Windows Intranet environment, we are testing the Microsoft Shared Hosting Solution. The Shared Hosting Solution will offer a platform in which all parties who administer and operate outside of the centralized server community can still have control over the daily task of a server administrator. This new and innovative technology will allow the Central Office to maintain, govern, and support all Intranet server activity from a centralized location. This solution is being piloted with the Dallas, Atlanta, and Central Office regions. If proven as a solution, the rest of SSA's end-user development community will fall under the blanket of this new shared hosting environment.

Local Area Network

Service Area Definition

The Local Area Network (LAN) service area defines the hardware/software infrastructure and processes required to provide connectivity within each SSA site and between certain specialized sites, via network design, network engineering, network connectivity, development and customization of network management processes/tools, network automation processes, and network performance testing.

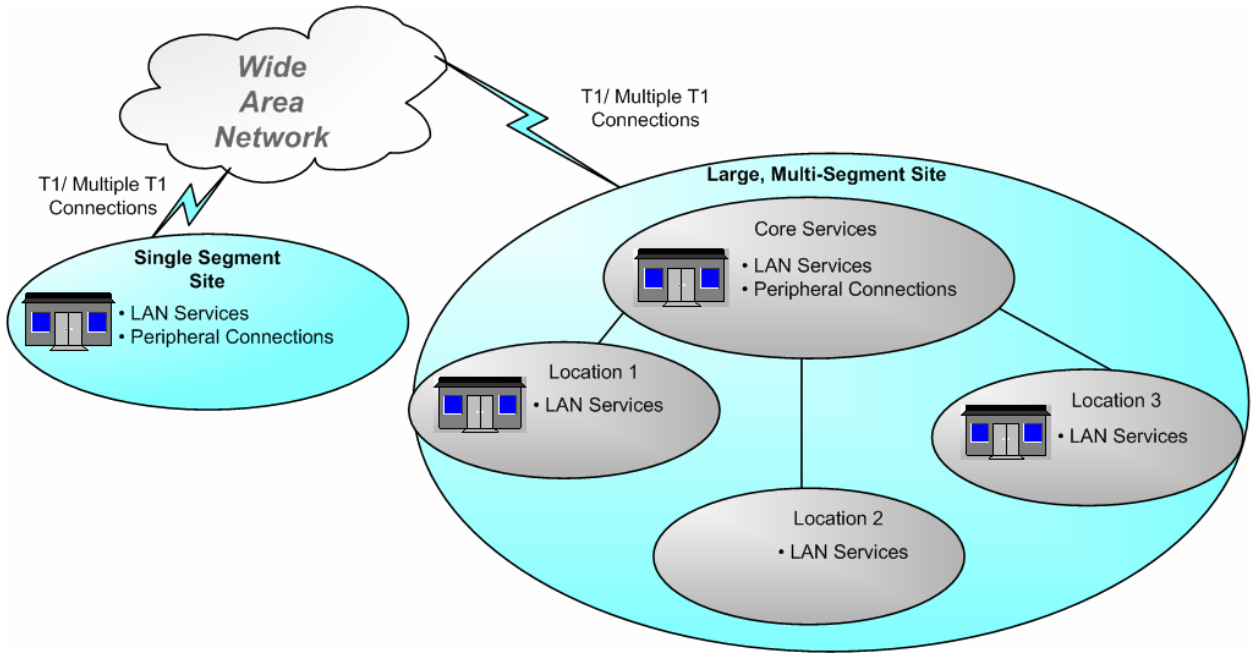


Figure 34: LAN Architecture

Current Architecture

This section describes the four logical environments that are depicted in Figure 34.

Single sites are the least complex sites in the network. The vast majority of these sites have a Cisco 2612 router, one LAN segment, and 2 Frame-Relay private virtual circuits (PVCs), one to the appropriate ROCC. In event of a PVC failure, all traffic will dynamically re-route over the remaining PVC.

Consolidated sites have multiple segments on location. They are classified this way because multiple departments are consolidated to form a common backbone. Also, these sites share the same WAN circuit(s) and router(s). There are usually no directly connected PVCs to the other field offices.

Parent/child sites are dependent. That is, they have directly connected PVCs to other field offices, as well as PVCs to their respective ROCCs. These directly connected PVCs are used primarily for IP traffic and for DDS's AS/400 access.

Virtual Private Network (VPN) connections are used for sites that do not have Frame Relay availability. Typically, they are contact/resident station sites that have not been converted to child sites.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. The Local Area Network architecture is relatively stable. At this point in the development process, it does not appear that the SSA LAN architecture will change much as Ethernet migration is only recently completed for all SSA and DDS locations. Potential growth of wireless and remote communications technologies, and evolutionary upgrades for the existing products including the integration of voice over IP telephony solutions and associated hardware are anticipated.

Transition

SSA has completed migration from its decade-old Token Ring Local Area Network (LAN) topology to the current industry-standard Switched Ethernet LAN topology. This phase of the SSANet modernization program followed on the heels of the FY 2000-2001 implementation of the ATM/Frame Relay Wide Area Network modernization, which provided routers for all SSA and DDS sites.

Ethernet deployment was accelerated in FY 02 and FY 03 based on early migration success and to avoid costly investment in the obsolete Token Ring elements.

Remote LAN Access is currently being provided via SSA's VPN. The VPN allows us to provide secure remote connectivity to SSANet and allows us to meet the goals of the Service Vision by using the latest technology available to maximize SSA's production via existing Internet resources. Through the VPN, this improved speed is coupled with uncompromising security to protect SSA data. We have designed, built and implemented a fully redundant architecture for our SSA managed VPN.

The SSA VPN represents the successful marriage of the Ethernet and Token-ring worlds with a private Internet Service Provider. The security is provided using third party hardware and software including smartcard front-end authentication and the ability to create a 3DES encrypted tunnel for data transmission from SSANet to the client and back. Additionally, the tools we are using are compatible with the biometrics technology of the future, implementation of which remains one of the recommendations of the SSA Chief Security Officer.

Lastly, we will be testing new technology in SSA's environment with our security requirements, including wireless e-mail as well as wireless remote LAN access for claims processing. This will also include cable modem hook-ups with appropriate personal firewall protection, and satellite connectivity.

Mainframe

Service Area Definition

The Mainframe service area defines the hardware/software infrastructure and processes required for online transaction processing and batch operations on this processing platform, which support SSA's program benefits and other key applications.

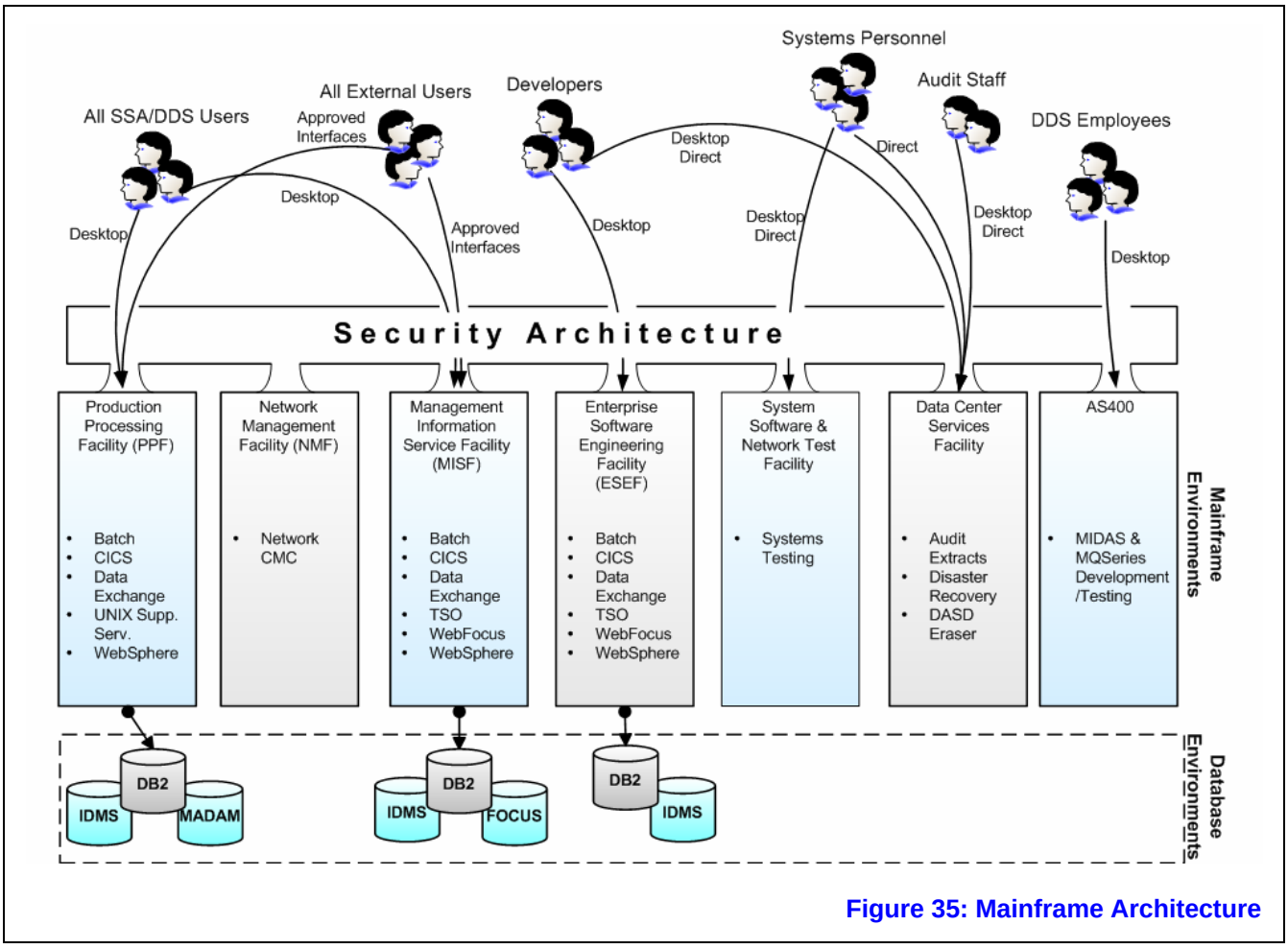


Figure 35: Mainframe Architecture

Current Architecture

This section describes the logical environments that are depicted in the Mainframe logical diagram. Specifically, the mainframe processor resources at SSA are divided into Logical Partitions (LPARs). Each LPAR acts as an independent MVS system capable of processing work. LPARs in turn are grouped together into system complexes (sysplexes) which share resources (e.g., Coupling Facility, DASD, tape etc.). A sysplex usually serves a specific function for a particular target audience, as described in Figure 35.

The **Production Processing Facility (PPF)** supports SSA's primary workloads, including its complex Customer Information Control System (CICS) online environment and batch operations. The PPF also houses the primary and backup Communications Management Configuration (CMC). The CMC manages and controls the network resources for both SNA and TCP/IP sessions.

There is no unscheduled, random access permitted in this environment. There is rigorous change control and a strict system development life cycle for applications which run on the PPF. A procurement vehicle is in place to ensure adequate processor capacity for the immediate future. Consequently, demanding Service Level Agreements are met, and user response times are maintained at high levels.

The **Document Management Facility (DMF)** supports the AeDib Document Management Architecture. Content Manager testing is currently underway on the DMF. The AeDib California Pilot began in October 2003.

The **Management Information Service Facility (MISF)** supports administrative, management information, research and actuarial functions; and Program Service Center (PSC) and Office of Child Support Enforcement (OCSE) workloads. It is host to a variety of development tools and high-level languages to support the user community. It is also host to a fully normalized database, which is structured to provide flexibility and support ad-hoc reporting.

The **Enterprise Software Engineering Facility (ESEF**) supports application development and testing. Mainframe code is developed, tested, validated and released into integration from the ESEF. Data housed in this environment is isolated from programmatic and MI data to ensure that security and privacy objectives are met. There are special development tools located on the ESEF to assist SSA's development community.

The **System Software Test Facility** supports systems software and product testing. It is the first point of installation and testing for new releases and maintenance of vendor and systems software, including the operating system.

The **Audit Test Facility** and the **Disaster Test Facility** support audit and disaster recovery functions within the Mainframe architecture. Storage for the LPARS is isolated as it contains subsets of production files.

Two **AS400s** located in the NCC support development and testing of MIDAS applications at SSA. The AS400s, technically not mainframes, are mid-range processors, which on the high end may be larger than a small mainframe. MIDAS applications are developed and tested on SSA's AS400s in support of those states whose DDS runs MIDAS, and are generally accessible only by DDS employees.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. The Mainframe architecture is one of those areas and will thus have a formally approved target. One key factor that will be considered in the development of the target architecture is the evolution of web technology into the

mainframe arena. But at the same time, the first consideration will always be the assurance of continued stability and capacity to support SSA's core programmatic workloads.

In the short term, architectural changes will be at the physical level, based on basic evolutionary improvements, such as keeping current with vendor software and hardware releases such as the move to IBM's z/OS operating system.

Transition

In the first quarter of FY 2004, the DMF LPARs will be migrated to new z990 mainframe processors. The AeDib production rollout is slated for January 2004.

The AS/400 9406 model 820 will be upgraded to a model 825 in early FY 2004. This upgrade provides the capacity to backup a state DDS in the event of a disaster. Beginning in FY 2004, after contracts are in place for vendor support, the states will be scheduled to perform disaster testing on the AS/400.

During FY 2004, WebSphere V4 will be upgraded to WebSphere V5 on the mainframe. WebSphere V5 is a major redesign which will align the z/OS WAS architecture more closely with that of the distributed (UNIX) WAS architecture. Several major WebSphere applications (ISSS, ONRS and I-Main) are targeted for production on the mainframe in FY 2004.

The z/OS operating system and support software (JES3, DFMS, RMF, BatchPipes, Security Server, TPNS, etc.) will be upgraded to the z/OS 1.5 ServerPac supported levels. The z/OS 1.5 operating system will provide the Agency with the latest state-of-the-art technology.

Print Services

Service Area Definition

The Print Services service area defines the hardware/software infrastructure and processes required to support SSA's varied print and output workloads.

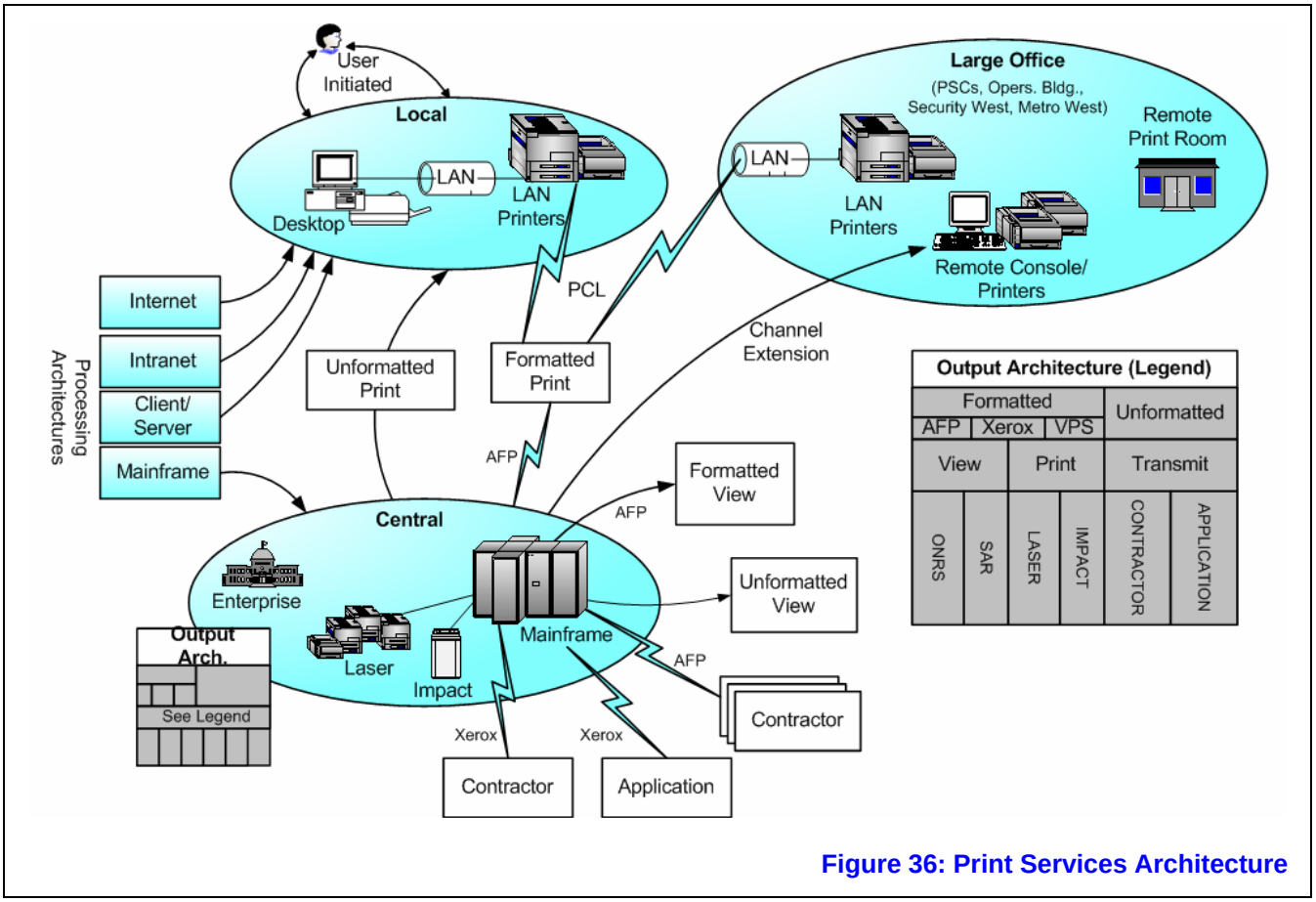


Figure 36: Print Services Architecture

Current Architecture

Printers are an integral part of SSA's mainframe systems and networks. Programmatic notices continue to be the primary means of providing clients with information regarding services and any changes that will affect them. The combination of notices and non-notice output amounts to a print workload of 19 million pages per month for headquarters and the processing centers. The Print Services architecture (Figure 36) supports these nation-wide printing requirements with a variety of hardware solutions.

Within the Print Services service area there are three environments:

The **Central** environment is where most of the Mainframe printing occurs. There are impact and laser printers attached to the Mainframe. The impact printer handles all Job Entry Subsystem (JES) printing, while the laser printed format is currently either

Advanced Function Presentation (AFP) or Xerox. A process is underway to eliminate the Xerox format and printers and use only AFP.

In this environment, the Mainframe is also capable of producing formatted and unformatted text files. These files are then available for transmission to outside vendors or other field or local offices. The Central environment also supports viewing print requests online either via the Sysout Archive and Retrieval System (SAR) or an IBM product called Online Notice Retrieval System (ONRS).

The **Large Office** environment consists of remote workstations and Mainframe printers. Print jobs from the Mainframe can be controlled from these remote workstations and printed on the local Mainframe printers. Currently, the remote Mainframe printers are Xerox brand, but they will be replaced with AFP printers within the next year.

The **Local Office** environment consists of several LAN-attached printers that receive print jobs from the OnePrint product located on the Mainframe in the Central environment. There are also local printers attached to the local desktops and/or shared on the LAN for individual print requirements.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. The Print Services architecture is relatively stable. At this point in the development process, it does not appear that the SSA Print architecture will change much at the logical level, but, perhaps at the physical implementation level. These changes will be driven largely by continuing paper reduction directives such as GPEA and new technologies designed to satisfy them, as well as evolutionary upgrades for the existing products and associated hardware.

Transition

As printers reach the end of their systems life, SSA replaces them with newer, more effective technology. A number of enterprise printers will be replaced and/or decommissioned each year.

The National Print+ Mail Initiative will remove ninety-five (95%) of the Program Service Center (PSC) workload through outsourcing and consolidate the remaining Agency notice processing at the Print/Mail Facility (P/MF). The P/MF will be used to profile the production of notices prior to outsourcing and to provide a more economic means to print and mail notices that will continue to be processed by SSA. The P/MF created at the NCC will continue to output 20 million notices and SSN cards, while serving as a backup operation for notice workloads contracted out to the private sector. The remaining notice groups associated with the National Print Mail Consolidation initiative are very complex and will require additional development and acquisition processing time. This initiative will also establish management information for notice production integrity whether a contractor or SSA produces the notices.

In order to reduce the need for high volume, centralized printers, the Agency has taken action to provide the capability to print AFP mainframe output on LAN attached printers. The Agency acquired a commercial print stream management software (CPMS) application that allows "hardware independence" so that any print file can be routed to any printer. The software enables mainframe and PC-based print files to be routed to the printer nearest the user, regardless of its platform. This capability delivers more timely reports to the user and reduces downtime as compared to centralized printing operations.

SSA uses impact-printing technology to produce Social Security cards on two IBM 6262 impact printers. The intaglio method (raised impression) of printing the emblem and border on the preprinted card stock provides a measure of security against counterfeiting. Impact printing technology is declining in the market in favor of more advanced laser printing techniques. Impact printing hardware will become increasingly more difficult to support as the market shifts to laser printing technology. New methods of laser printing technology and card stock are being evaluated to develop and test a replacement production process that will continue to meet the security requirements for producing tamper-proof Social Security cards.

The adoption of a new card stock by the Agency will require legislative approval. Alternative methods to SSN card production are currently being evaluated by Agency policy components. Recent discussions with SSA policy components indicate that a change in the current card stock will not occur immediately. However, efforts will continue for prototyping alternative SSN card production processes.

The ONRS is the repository for SSA notices that may be retrieved for viewing and reprinting. Online viewing capabilities exist today for SSA's mainframes systems output and reports. Options to expand these capabilities are currently under evaluation and review. During FY 2004, the Agency intends to investigate, evaluate and prototype online viewing utilities that are consistent with the Agency's strategic plan of a paperless workplace. These utilities will include various Web-to-host and LAN-to-host tools for user-friendly viewing of mainframe data.

Future enterprise output strategies that will be evaluated incorporate the use of a Data Stream Management Database to establish controls and provide management information for all output. This database will also function as a traffic controller to route the output to its optimum printer. Certain items may even be rejected for printing until the need to print them is validated. Patterned after the Automated Document Factory that is evolving in the private sector, the Print Services architecture will evolve into an Enterprise Output architecture that will provide electronic management of enterprise output with optimum print and non-print solutions.

Security Systems

Service Area Definition

The Security Systems service area defines the hardware/software infrastructure and processes required by all aspects of the Information Technology (IT) security program. IT security measures are essential for maintaining the privacy and integrity of SSA data, for identifying authorized users for SSA systems and for restricting access to sensitive resources.

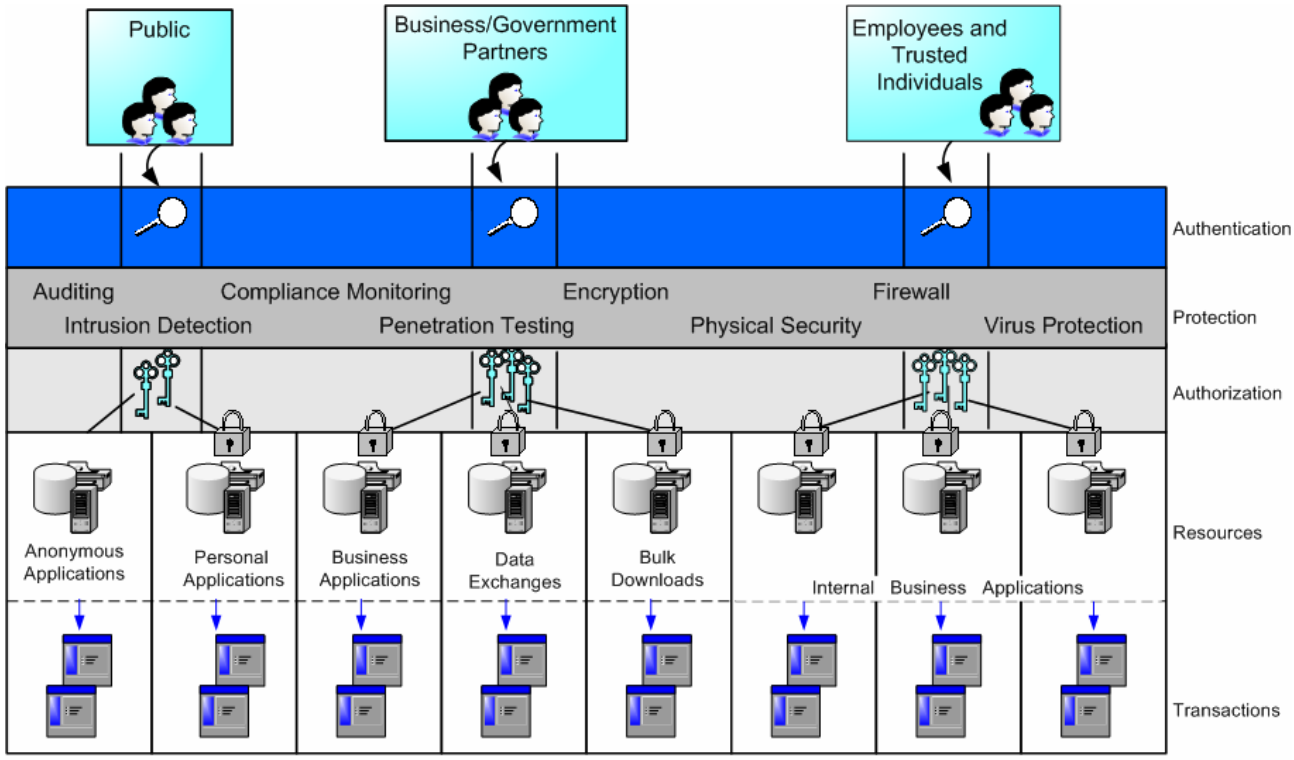


Figure 37: Security Architecture

Current Architecture

This section describes the logical components (agents, functions, resources, and transactions) that are depicted in Figure 37.

USER SECURITY GROUPS

Security Architecture is the design of hardware and software operating practices that implement security policies. These policies are designed to secure SSA's resources from a user community that includes the following user security groups:

- Employees and Trusted Individuals;
- Business and Government Partners; and

- The General Public

The security measures required for each of these user security groups differ. The authentication, protection, and authorization performed for each of the user security groups are explained in the following sections. Note that an individual may belong to one or more of the above user security groups. For example, an SSA employee may have desktop access to SSA resources, while at the same time owning a business that supplies wage reporting data to SSA; and of course he/she is a member of the general public as well.

The **Employees and Trusted Individuals** group consists of SSA employees, DDS employees, and trusted individuals who have internal access credentials (pin/password). Within the constraints of the security architecture, the user community may access intranet, mainframe, and client/server resources.

Business and Government Partners are organizational entities with which SSA does business. An organization may be given a unique identifier in order to access SSA resources. Individuals within the organization (designated by the organization and SSA) may have a separate unique identifier. For example, certain businesses may be authenticated for reporting wages to SSA, while SSA also exchanges data with states and other government entities such as the Department of the Treasury, the Bureau of Vital Statistics, and with prison systems (for benefit cutoff information).

Public groups are divided into two categories for systems security purposes, those without SSA access credentials (i.e., "anonymous" users), and those who have been granted SSA access credentials.

SECURITY PROTECTION LAYERS

The following section offers a brief description of the three security layers through which those wishing to access SSA resources must pass. The implementation of these layers varies, depending on the user security group to which the accessor belongs.

The **Authentication** layer is used to identify the requestor. The authentication should be performed independently of all business processes in the software application. If possible, the authentication should be in specialized security module(s) built or purchased for the sole purpose of providing security. The authentication mechanism differs for each user security group:

- **Employees and Trusted Individuals** use a PIN and Password for authentication in most circumstances. Every individual is assigned a unique PIN that is the initial identifier to the internal SSA environment. The Password, also an identifier to the internal SSA environment, is developed by the user, based on guidelines for Password usage. This PIN/Password is currently stored in a TOP SECRET database. If the employee or trusted individual is doing very sensitive work or is performing work remotely, PKI certificates, SmartCards or Security Tokens are required to access SSA resources.

- **Business and Government Partners** are pre-registered with SSA. In many cases, there is a point-to-point installation of specific hardware and software that enables the business and government partner to communicate with SSA. Business and Government partners may also conduct business online through the Internet with strong controls in place, including encryption and authentication where warranted.
- The **Public** uses the Internet to communicate with SSA. Many of the applications available via the Internet are anonymous applications, meaning that no authentication is required because no personal data is being requested, updated or displayed. Public applications accessing personal data provide authentication using a pre-assigned PIN and Password.

The **Protection** layer isolates SSA resources from a variety of threats, both intentional and unintentional. Protection methods include the following:

- **Auditing** validates and monitors access to SSA resources.
- **Compliance** monitoring ensures that the settings designed to protect the SSA resources are functioning properly. This function ensures that the hardware and software tools used to monitor all the security functions are not changed, and that virus protection software is checking all file types.
- **Encryption** provides the ability to alter data into a form that is not easily understandable by unauthorized people. Transport encryption is used by SSA to encrypt data as it travels between sites or within the SSA network. For sensitive data such as a set of passwords, SSA provides encryption to the resting data also. SSA also employs hardware encryption, such as that on the IBM mainframe communication channels.
- **Firewall** software is used to prevent unauthorized access to any resources inside the SSA environment.
- **Intrusion detection** is a full-time service that constantly scans the SSA network for patterns of activity that may be inappropriate.
- **Penetration** services include a suite of services (requested by SSA) that perform a controlled attack against the SSA security architecture. These attacks validate that procedures are effective in detecting unauthorized access to SSA resources.
- **Physical Security** is controlling the comings and goings of people and materials; protection against the elements and natural disasters. SSA provides physical security on a commensurate level with the degree of vulnerability of the various work spaces. This type of security, however, is not within the scope of the Enterprise IT Architecture.
- **Virus Protection** includes software tools that scan incoming data as it flows through the SSA architecture. This software is available at the server, local desktop and system-wide. Virus scanning of all transmissions via e-mail is addressed system-wide. At the servers and local desktop, a variety of executable files are scanned for viruses.

The **Authorization** layer identifies the SSA resources that the authenticated user is permitted to access. Within an authorization, the permitted resources may be further constrained by the role that the user is allowed to assume. The physical machine(s) at which the user's requests are serviced may vary based on authentication and role.

- **Employees and Trusted Individuals** will be authorized to use specific internal resources and transactions based on a profile that has been identified by SSA. These individuals do not have access to any SSA Internet applications based on their profiles. While most have access to an Internet browser that allows them to access Internet applications, they are not accessing the SSA Internet applications using the internal PIN and Password assigned by SSA.
- **Business and Government Partners** have signed a contract with SSA and have been given authorization to access specific SSA resources and transactions.
- **Public** individuals are only authorized to access SSA Internet applications. Many of these applications are content serving and do not provide specific personal data to the requestor. However, there are a growing number of applications that do provide specific personal data. Individuals who have access to these personal applications must either authenticate themselves by matching personal identification data SSA possesses or by using a Password. Individuals establish passwords by matching personal identification data and then creating a Password online using an access code mailed externally to them.

RESOURCES AND TRANSACTIONS

Upon successfully passing through the three security layers discussed above, the requestor will gain access to SSA resources and transactions. The resources available will depend upon the user security group to which the requestor belongs. This section describes the types of resources and transaction that are available to each of the user security groups.

Employees and Trusted Individuals have access to many internal business applications. Access to these applications is based on the authentication profile of the requestor. The internal business applications span the Mainframe, Client/Server, and Intranet processing platforms as described in other sections of this chapter. However, employees do not have access to any applications on the Internet processing platform as part of their membership in this user security group. When an employee or trusted individual uses an Internet browser in order to access an SSA Internet application, he or she is authenticated as a member of the Public user security group and loses the employee/trusted individual identity for that session.

Business and Government Partners do business with SSA in a variety of ways, depending on the requirements of the information that they require or provide. These methods are as follows:

- **Business Applications** provide businesses with a variety of information captured by SSA and other government agencies. Examples include Electronic

Wage Reporting System (EWRS), and Enumeration Verification System (EVS).

- **Data Exchange** is a transfer of data from a Business or Government Trading Partner to SSA or vice versa. Contracts or Memos-of-Understanding are often required for these exchanges. Several methods are used for these transfers including Virtual Private Networks, SSL (encrypted) Tunnels, Value Added Networks and dedicated point-to-point leased lines. Examples of products used for these exchanges include AAMVANet, NetScreen, VPN and Connect:Direct.
- **Bulk Downloads** provide the capability to perform data transfer with no contractual agreement having been established. This type of transaction is for ad hoc data transfers via File Transfer Protocol (FTP). An example of bulk download may be a system dump sent to IBM for technical support when SSA experiences problems with a job.

The **Public** also encounters differing levels of security depending on the type of application they need to use, as follows:

- **Anonymous Applications** provide non-personal data to the requestor. Anyone can access these content serving applications. An example is the Field Office Locator.
- **Personal Applications** provide the requestor with data regarding himself or herself or regarding an individual whose data the requestor has been authorized to access, such as a child. Depending on the requestor's identification and role, he or she may have access to different data within the same application. Individuals that use these applications must authenticate themselves by matching personal data in SSA's data bases or by use of a Password (see "Public" above). Examples include the Internet Retirement Insurance Benefits (IRIB), the Internet Social Security Benefits Application (ISBA), and Account Status applications.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. Security Systems is one of those areas and will thus have a formally approved target. At this point in the development process, it does not appear that the SSA security architecture will change much at the logical level, but rather, at the physical implementation level. In the short term, these changes will be based on some basic evolutionary improvements, incorporating enhanced versions of existing security products, such as the CA eTrust integrated product suite and Tivoli monitoring agents, as they become available and SSA is able to procure them. In the longer term, research and development and active piloting of future technologies such as biometrics will ensure that the Systems Security architecture evolves with the state of the industry.

Transition

SSA must be aware of security breaches and data compromise and the impact of these events. Appropriate security monitoring and planning, including an analysis of risks and contingencies and the implementation of appropriate contingency plans, must be completed to prevent unauthorized access to SSA information.

As we define the target Systems Security architecture we will continue to upgrade and improve the existing security tools. The numerous upgrades include multiple planned improvements to the CA TOP SECRET administration process; new versions of existing Security COTS products; strengthened Remote Access VPN monitoring and auditing; and multiple improvements and upgrades to the security request processes.

Security training for administrators and users of new security products and procedures will be designed and conducted as appropriate to facilitate the changes and upgrades listed in this section.

In addition, in anticipation of the target architecture, work has begun on a number of near and longer term initiatives. These include (by security layer):

Authentication

- For Internet Authentication, Tivoli Access Manager, a COTS Security Package using secure directory (LDAP) will be installed.
- Use of Authentication facilities within the Netscreen VPN for data exchange with government and business trading partners will be implemented.
- eTrust COTS package will be installed on the SSANet with an Employee-Based secure directory (LDAP) tied to CA TOP SECRET.
- Biometrics authentication project will be piloted.
- Enhanced internal resource security & user account administration will be accomplished through the use of CA eTrust Admin & Access Control.

Protection

- Additional Internet Intrusion Detection and content filtering facilities will be installed.
- Hardening of the SSANet will be accomplished via the CA eTrust (Intranet) Firewall deployment.
- Protection of SSANet will be strengthened through CA eTrust Policy Compliance Manager

Authorization

- Internet Authorization using DB2 "roles" database and Tivoli Access Manager and other COTS package(s) will be implemented.
- Security protection will be extended to new resources such as MQSeries and DB2 database connections.

Storage

Service Area Definition

The Storage service area defines the hardware/software infrastructure and processes required to supply DASD and tape storage media for the mainframe, client/server and Internet/Intranet processing platforms. OS support includes backup and recovery services (onsite and offsite backups), support for archiving and storage of historical data. Local file server storage is generally utilized for non-mission critical data resources and is supported by local site-LAN coordinators.

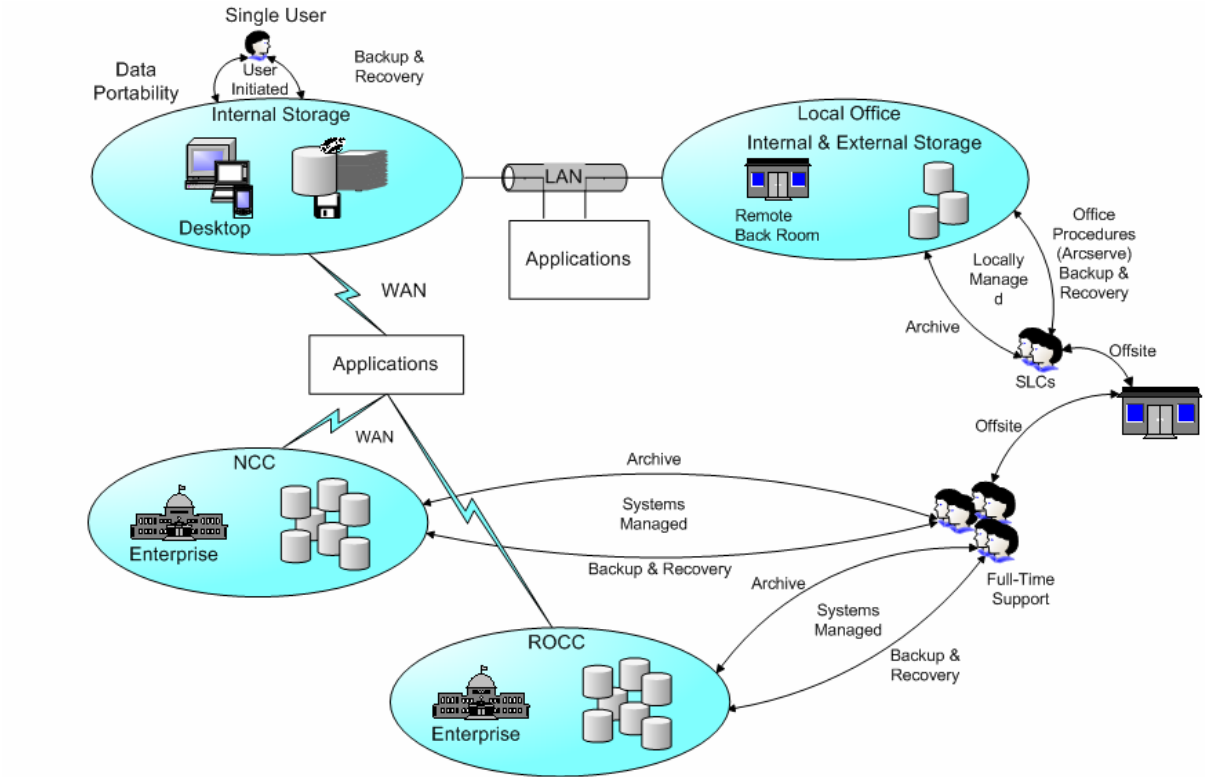


Figure 38: Storage Architecture

Current Architecture

The current installed storage in the NCC/ROCC environment (Figure 38) consists of approximately 28 terabytes (TB) of online DASD to support 6 mainframe MVS/JES complexes, and 19.3 TB to support the various platforms for the Client/Server, Intranet and Internet processing architectures. Shared DASD within the Open Systems environment is distributed in the NCC and the ROCCs.

SSA is currently implementing Storage Area Network (SAN) technology that will provide solutions to meet storage challenges and provide the infrastructure to eliminate Small Computer Systems Interface (SCSI) storage interfaces and to convert to robust backup strategies. SANs interconnect servers and storage at extremely high

speed, taking advantage of recent advancements in fiber (glass based) channel and switch technology to provide scalable, hierarchical storage solutions that increase accessibility and assure maximum availability at a greater performance and distance than ever before. This will increase connectivity options and allow better leveraging of each DASD subsystem.

Storage management services are provided to over 300 enterprise servers (UNIX, NT, AIX) in this distributed Local Office environment. The Agency's direction to distribute storage has provided the added challenge of managing these resources remotely. DASD in the client/server environment is not truly shared as it is in the mainframe. Each server "owns" its storage and maintains its own connection to the shared disk unit. Because of the SCSI connection limitations, additional DASD subsystems are often required before capacity limits of the unit are reached. Reconfigurations and distributed vendor support must be provided to assure timely fixes.

Desktop storage is limited to the hard disk in the desktop computer environment, as well as any portable media the individual user may have access to (e.g., diskette, writeable CD, "Zip/Jaz"). Creation and management of these storage platforms are entirely the local user's responsibility.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. The Storage architecture is relatively stable. At this point in the development process, it does not appear that the SSA Storage architecture will change much at the logical level, but perhaps at the physical implementation level. These changes will largely be driven by changes in the processing architectures and the applications that run within them, as well as evolutionary upgrades for the existing products and associated hardware.

Transition

Storage requirements must be consolidated and shared devices planned to provide the infrastructure facility to meet overall storage requirements.

With the immediate growth of Internet-based applications and the future promises of such technologies as video training, video mail and electronic medical evidence, the growth of data and data storage requirements have soared. Most IT organizations (i.e., Internal Revenue Service and Centers for Medicare and Medicaid Services) are predicting that storage needs will double in the next few years.

To plan for DASD capacity increases, users provide estimates annually to project their 3-to-5 year DASD requirements for each workload. The overall procurement strategy is to purchase "once-a year" resources through competition, with a 60-day lead-time on procurements.

The Agency has chosen to provide Storage Area Network (SAN) solutions to provide the infrastructure to eliminate SCSI storage interface limitations and to convert to robust backup strategies. SANs interconnect servers and storage at high speed, taking

advantage of recent advancements in fiber channel, and switch technology to provide scalable, hierarchical storage solutions that increase accessibility and assure maximum availability at a greater performance and distance than ever before.

SANs provide five basic benefits:

- Consolidation of storage devices—number of connections;
- Higher availability—separation of backup and messaging traffic;
- Better scalability—larger capacity storage subsystems, number of connections;
- More reliable backups—faster, separation of backup and messaging traffic; and
- More reliable recoveries—backups more reliable, separation of backup and messaging traffic.

Adding backup functionality under SANs in the FY 2003-2004 time frames will increase consolidation for tape backup equipment and further leverage storage, with elimination of costly maintenance on older equipment. Fiber-connected tape libraries are planned to allow consolidation of SCSI tape devices into more scalable units or to an existing mainframe silo configuration providing 9840 tape and/or Super DLT technology with performance enhancements. Newer technological improvements will also increase overall benefits. We estimate elimination of 4 backup configurations and savings from offsets in acquiring 4 additional backup configurations.

Telephone

Service Area Definition

The Telephone service area defines the hardware/software infrastructure and processes required for voice telecommunications services for all SSA facilities, including the National 800 Number Network (N8NN), Headquarters, regional offices, field offices, program service centers (PSCs), teleservice centers (TSCs), the Wilkes-Bare Data Operation Center and, contact and resident stations. SSA's telephone network has two major components: the equipment located at each SSA office and the network services that provide local and long distance voice communications.

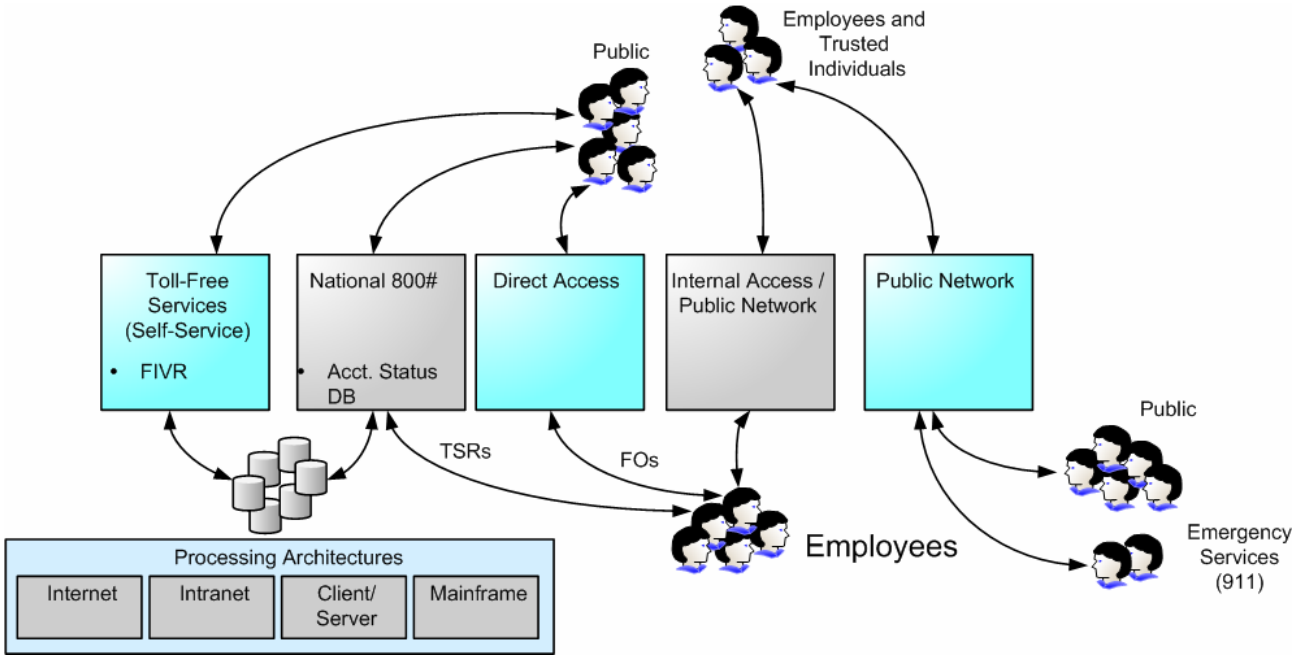


Figure 39: Telephone Architecture

Current Architecture

There are five logical environments depicted in the Telephone logical diagram (Figure 39):

The **Toll-Free Services (Self-Service)** environment will be the gateway for the public using toll-free telephone numbers to check some of the account information that they had to previously obtain from an SSA employee. This is similar to the automated telephone features available to the public from banks.

The **N8NN** environment is a very visible and important gateway for the public to do business with SSA. As a measure to improve its service to the public, SSA has a nationwide toll-free telephone service using a single 800 number (1-800-772-1213).

The N8NN uses 6,282 lines to route calls and provide toll-free agent service from 7 a.m. to 7 p.m. in every time zone with calls routed to 41 answering sites. Callers may use automated services 24 hours a day. SSA provides all agent and automated services in both English and Spanish. Load balancing routing changes and adjustments can be implemented on short notice. The National 800 Number Network also provides for pre-established emergency routing.

SSA has replaced the premise-based automatic call distributors with newer technology (i.e., WCOM's network-based services) and an intelligent network routing (INR) feature in 2001. The INR software feature consolidates all the National 800 Number network queues to SSA's various call centers into one logical queue. This network solution provides the Agency with a robust and flexible call answering capability. It enables SSA to increase the number of callers who reach the National 800 Number within 5 minutes, add additional answering capacity and allow the scope of telephone service to expand, as SSA deems appropriate.

The three environments **Direct Access**, **Internal Access/Public Network**, and **Public Network** are primarily concerned with telephone relationships between employees and the public and inter-employee communication. The equipment located at each SSA office consists of telephone sets and their related telephone system components, such as Private Branch Exchanges (PBXs), Automatic Call Distributors (ACDs), automated attendant and voice mail equipment, and network services termination equipment. A given SSA location may have its own SSA procured telephone system and/or switching services acquired through the General Services Administration (GSA). These three environments cover the field offices, the Program Service Centers, the Wilkes-Barre Data Operations Center, the Headquarters complex, and telephone network services.

- **Field Offices**—The Agency has over 1600 telephone systems with automated attendant and voice mail. SSA is currently implementing several initiatives to improve customer access to the field offices. One of these initiatives is to give the caller the option of being forwarded to the SSA National 800 Number if the caller encounters a busy signal when dialing the local SSA Field Office.
- **Program Service Centers**—All of the PSCs have been transitioned to FTS2001 for long distance calling. A new Fujitsu 9600 PBX was installed in the Mid Atlantic Program Service Center (MATPSC) in November, 2000. It replaced the GSA Centrex Service and the 9 Executone Telephone systems and provides the additional functionality that was required by the MATPSC. A new telephone system is planned to be installed during the South Eastern Program Service Center (SEPSC) move in FY 2007.
- **Wilkes-Barre Data Operations Center**—The Agency previously procured a PBX system for the WBDOC. This system has over 500 instruments with a total port capacity for stations and trunks of 1,300.
- **Headquarters**—The Woodlawn and Metro West campuses are supported by the SSA owned SL-100 telephone system. Wired to accommodate 30,000 lines, the system can provide support for voice, data, and video. It is also used to provide central office trunks to small systems within the campus. The SL-

100 uses a redundant distributed processing design to provide high reliability and maximum call processing capability. A server maintains information for an operating directory, service order process, billing and cable plant record keeping. The directory data within the server is used to maintain the SSA Intranet directory service and the Headquarters' Locator Service.

The Headquarters PBX is being enhanced continuously to provide high quality services to SSA's internal and external customers. Through the retrofit of existing hardware, which has been in service since 1987, SSA can upgrade the current switch configuration to one that will take SSA well into the next decade.

- **Telephone Network Services**—The telephone network services consist of over 50,000 circuits. These circuits are typically provided by the local telephone company exchange or the FTS contract carrier. The circuits permit local calling as well as connectivity to long distance communication services provided by the FTS contract carrier (FTS2001 long distance carrier for SSA is WorldCom). Recently competition for local service has entered the marketplace. GSA is offering local service through competitive contracts for specific metropolitan areas throughout the country through other local exchange carriers. This offering is called the Metropolitan Area Acquisition (MAA). SSA evaluated each of 23 regional MAA offerings to determine its value to SSA. While not reducing the number of circuits, the recurring cost decreased using the MAA contracts. SSA has converted over 200 offices to the MAA.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. In the future, moving the Telephone Architecture to a converged network using Voice over IP will enable changes to the target architecture that could make the voice in the telephone architecture just another application on the Wide Area Network Architecture, the Local Area Network Architecture and the Electronic Messaging Architecture. These changes will largely be driven by increasing need to provide alternate, web-enabled or web-supported methods of serving the public, the need to support increasingly sophisticated users both internal and external to SSA, and evolutionary upgrades for the existing products and associated hardware.

Transition

Replacement of telephone equipment is focused on retooling the whole enterprise with a new telephone solution. The vast majority of telephone systems are at end of life or no longer supported like the existing, aging Executone hybrid systems (500+ field offices) or the Fujitsu systems (800 field offices, 4 PSCs and WBDOC) that stopped being supported by Fujitsu Corporation at the end of 2001. Serviceability for older Executone equipment will continue to be difficult because replacement parts, product support, and service training are no longer readily available.

New advances in technology give us the opportunity to upgrade our systems into more adaptable and serviceable platforms. Newer stand alone PBXs provide more management information and easier programming than in previous years. Furthermore, telephony today is consistently developing toward server and software driven systems and Voice Over IP (VoIP). These software driven systems allow many options including more management information, easier remote programming, and more compatible computer/telephony integration (CTI). CTI helps improve workloads, and easier programming helps reduce downtime and provides improved reliability. These software-based systems can be bought as an interim new private branch exchange (PBX), up-gradable solution, or as a full scale VoIP system.

We will be evaluating VoIP systems, which are expected to out perform traditional PBX type systems providing new features and capabilities to enhance productivity and efficiency of service. IP telephony benefits the Agency in many ways. The SSA Service Vision calls for SSA to provide "one stop shopping" for SSA claimants. IP telephony over the data network allows the potential to route and transfer calls intelligently through the SSA network. Long-distance savings are achieved because long-distance calls can be routed through the SSA network to a point where the call is local, and can then be switched through the local carrier at no charge. Decreased moves, adds and changes (MACs) costs are achieved because the intelligence is carried within the IP telephone. Therefore, the need for manual reprogramming of the telephone switches is greatly reduced.

In FY 2003, development work and market research was done with stand-alone VoIP systems and Enterprise VoIP systems in preparation for the Telephone Systems Replacement Project (TSRP) scheduled for late FY 2004-FY 2007. FY 2004 will see Enterprise VoIP pilots that will use diverse carriers and be integrated with SSA's data network. The integration will lay the infrastructure for the converged network, with the ability to survive outages from any one carrier. The Enterprise VoIP approach is expected to out perform traditional PBX type systems, providing new features and capabilities to enhance productivity and efficiency of service.

Video Architecture

Service Area Definition

The Video service area defines the hardware/software infrastructure and processes required to provide video services to SSA users both within and outside SSANet.

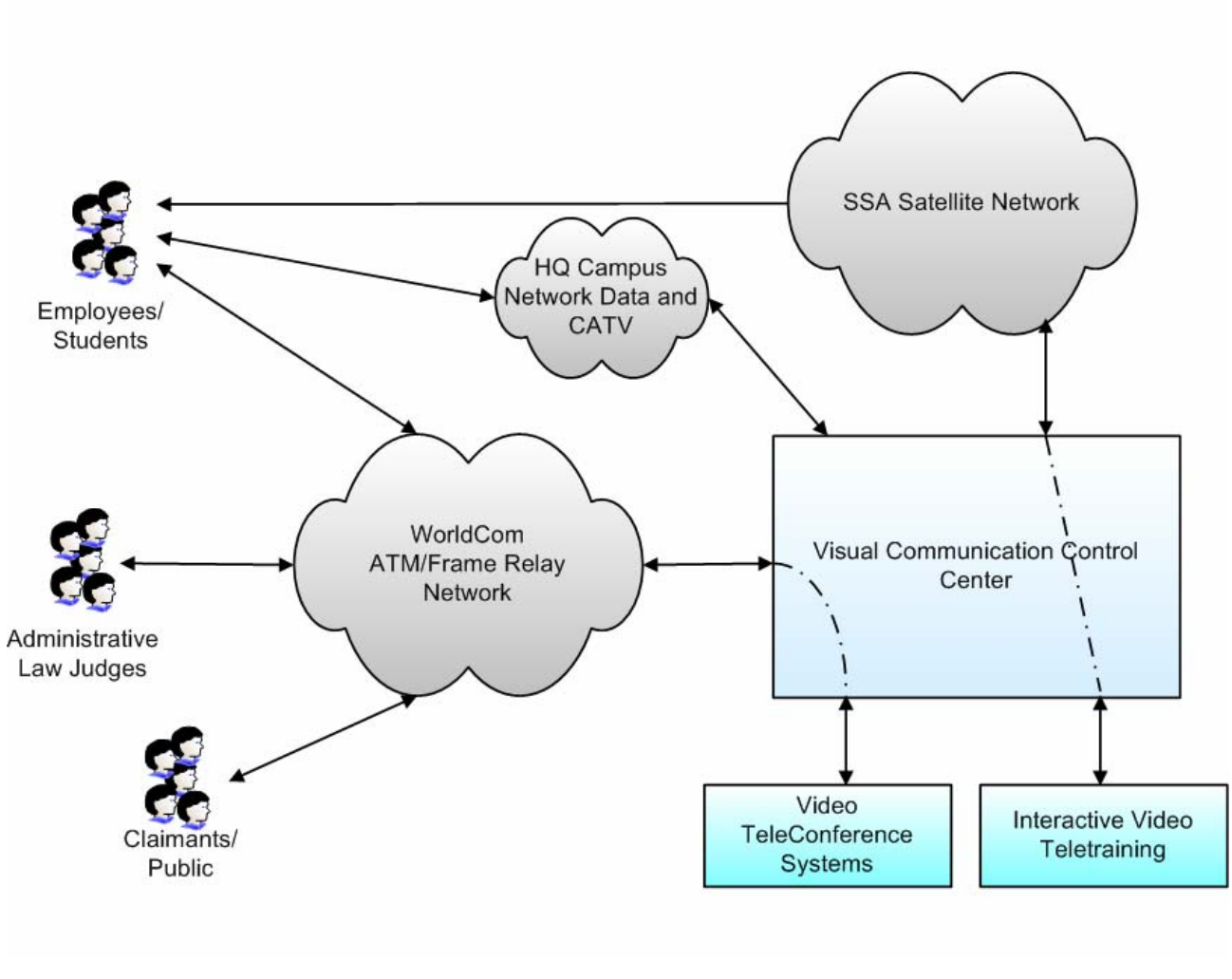


Figure 40: Video Architecture

Current Architecture

There are two categories within the Video Architecture: Video Teleconferencing and Interactive Video Teletraining.

Video Teleconferencing (VTC) provides the capability for participants to see and hear each other from several locations during the same video teleconference allowing complete two-way participation. VTC currently consists of video equipment at Headquarters, regional offices, IG Offices and district/hearing offices. The State Disability Determination Services use VTC to conduct disability hearings. OHA

conducts hearings using VTC, including hearings on the issue of disability. Additionally, equipment is installed to support initial disability claims-taking and disability hearings pilots on the Iowa Communications Network (ICN) pursuant to a Memorandum of Agreement (MOA) between the Central Iowa Federal Executive Council (CIFEC), ICN and the Federal government. A similar arrangement is in place in Montana. The primary network interface for SSA's video teleconferencing equipment is ATM/Frame Relay Internet Protocol services.

Interactive Video Teletraining (IVT) is one-way video, two-way audio technology that provides training to students not in the same room as the instructor, but still allows for full interaction between the two. The SSA IVT network is implemented by using SSA's satellite earth station, located at the National Computer Center (NCC), and by using receiver equipment, located at field offices, DDS and OHA offices nationwide. The IVT network uses MPEG 2 technology for video and audio and uses Frame Relay technology for data transmissions. The two studios at Baltimore headquarters are connected to the satellite earth station via fiber optics cable. The four regional broadcast studios are connected to the satellite earth station by using switched or dedicated T-1 service from their respective locations (Atlanta, Dallas, Kansas City and Seattle). IVT has been installed in more than 1,200 field offices.

SSA employees in FO classrooms are able to interactively communicate with an instructor located in a studio at a distant location. This interactivity between student and instructor is provided using IVT equipment installed in the FO classrooms. The satellite network provides the video infrastructure, while the IVT equipment provides the interactive communication between the classroom and instructor. All broadcasts from the studios are sent to the VCCC uplink system, which transmits the signal to the FO classrooms via satellite. Both of these elements are required for the current operation of the IVT network.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. The Video architecture is relatively stable. At this point in the development process, it does not appear that the SSA Video architecture will change much at the logical level, but rather, at the physical implementation level. These changes will largely be driven by the results of pilots already underway, as well as evolutionary upgrades for the existing products and associated hardware.

Transition

In FY 2003, SSA purchased and installed video teleconferencing equipment in support of the SSA-Wide Video Teleconferencing Strategy. Additionally, we are planning for a distributed architecture design using an H.323 video teleconferencing multipoint conferencing solution. When the multipoint conferencing solution is implemented, three or more video systems will be able to participate in the same conference and have external access to the outside world. The purchase and installation of additional multimedia presentation centers are also planned for the future.

Approval has been given to the Office of Hearings and Appeals to expand their use of VTC to include 316 offices. In FY 2004 through FY 2006 these installations will take place. The decision to move forward was based on positive ROI and intangible benefits presented by OHA.

At this point VTC has achieved its currently planned architecture on the ATM/Frame Relay Network. The future will bring more users and systems to the technology. Creating the capability to respond to increasing workloads, improving business processes and meeting citizen service demands are additional benefits that will be considered. The Agency recently transitioned its Wide Area Network (WAN) to a new IP router-based infrastructure, which should result in lower purchase costs for the new VTC equipment.

The SSA IVT network also achieved its currently planned architecture in early 2002 with the successful conversion of all downlink locations from the AT&T Oasis Virtual Private network to Frame Relay services provided by WorldCom. There is a new requirement to purchase equipment to expand IVT to an additional 126 field offices, which will bring training access to all of SSA's locations, for a total number of 1,640 IVT locations.

Wide Area Network

Service Area Definition

The Wide Area Network (WAN) service area defines the hardware/software infrastructure and processes required to provide wide-area connectivity , including the network design, network engineering, network connectivity, development and customization of network management processes and tools, network automation processes, and network performance tracking.

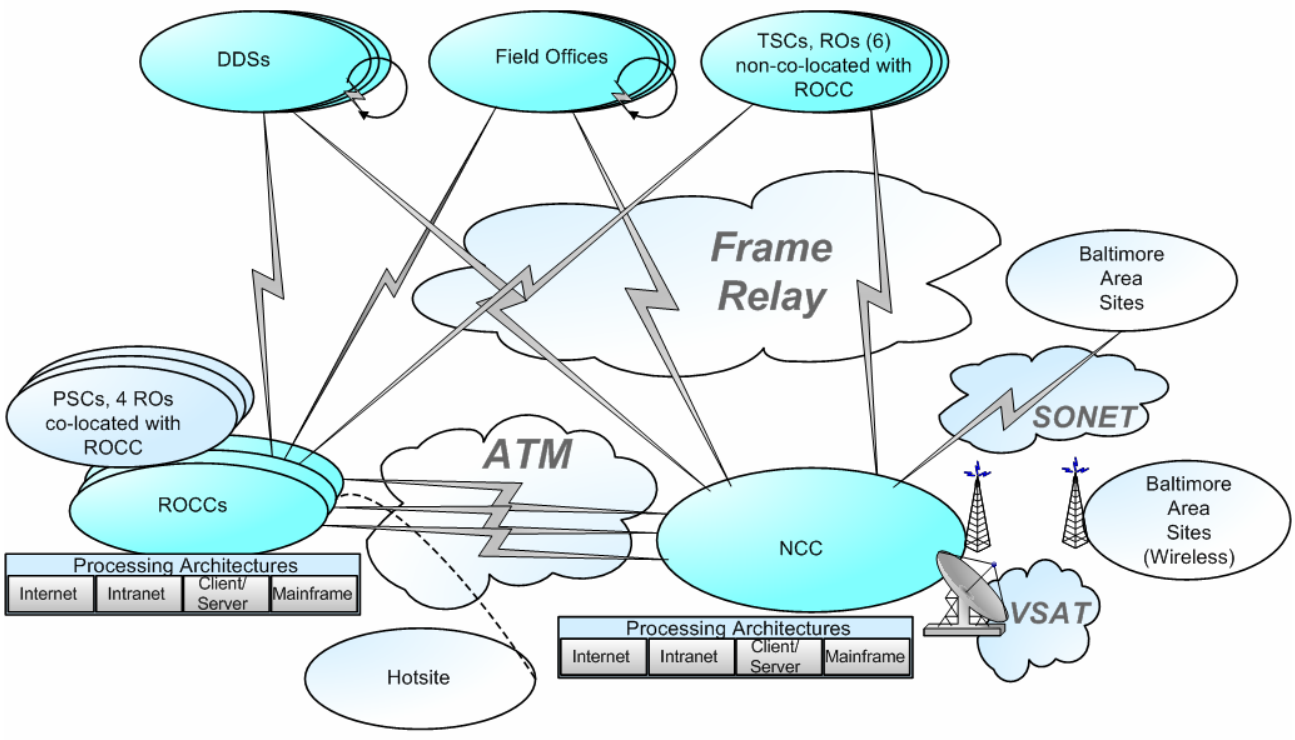


Figure 41: WAN Architecture

Current Architecture

This section describes the logical environments that are depicted in the Wide Area Network logical diagram.

Within the past two years, the Agency has migrated from a hierarchical bridged network to MCI's Asynchronous Transfer Mode (ATM)/Frame Relay network, which provides connections from each remote user site to its servicing ROCC and to SSA's NCC. Peer- to- peer connectivity is achieved through the NCC or the ROCC. The ATM infrastructure provides a flexible platform that can quickly be expanded as requirements for WAN network capacity increase. In addition, ATM technology enables the integration of voice, data and video in one state-of-the-art, fault tolerant technology. Each ROCC is provisioned with two DS-3s while the NCC has six DS-3s.

The **NCC** network infrastructure interconnects SSA mainframe processors and associated storage to SSANet and its thousands of users through Cisco routers. Other services provided at this network level include Internet access for authorized SSANet users. All SSANet users equipped with a browser have access to Intranet Web services connected through the NCC SSANet infrastructure. In addition, the NCC houses supporting enterprise network services for Windows, Exchange/Mail, and client/server IP applications. Also, the NCC provides backup for the ROCC SNA and Internet Protocol traffic.

Below the apex, ROCC services provided at the **Remote** network level include SNA routing for mainframe users and data base access for distributed applications. In addition, the ROCCs also house enterprise network services for Windows NT, Exchange/Mail and client/server IP applications.

SSANet **user sites** can be divided into two categories:

- Operating components, the largest of which is the nearly 1500 field offices, Teleservice Centers, Program Service Centers, 142 OHA sites, the State DDS locations; and
- Supporting administrative components located primarily at Headquarters in Baltimore but also at 10 regional offices.

Most of the user sites are connected through the ATM/Frame Relay network. Telecommunications access from 256 kbps to multiple T-1s (1.5 mbps each) is supported from end-user connections to servicing ROCCs and the NCC. The SSA **Headquarters Campus**, however, employs a gigabit Ethernet core to connect most of the outlying buildings. Some of the campus sites are connected via wireless technology. **Synchronous Optical Network (SONET)**, with an OC-3 backbone, is used to connect the outlying Headquarters Metro West building to the core.

There is also a connection to a **disaster recovery hotsite**. There is a DS-3 connection from the MCI network to the hotsite. The hotsite will function as the NCC in case of an emergency. This configuration enables SSA to quickly restore the National Computer Center (NCC) computing environment at the alternate site in the event of a natural or man-made disaster.

SSA sites that are outside of the continental United States include Hawaii, Alaska, Guam, the Virgin Islands, and Puerto Rico. These sites connect to SSA with a front-end Private Lease Line from the field office, a Frame Relay Only connection, or a Frame Relay Only connection with VSAT. In all other respects, the International Sites are identical to a single-ringing site. Puerto Rico concurrently utilizes a Frame relay circuit and a VSAT connection to the NCC.

Target Architecture

As stated in the introduction to this section, SSA has instituted a formal process for the development of target infrastructure architectures within the EA, beginning with five key service areas. The Wide Area Network architecture is relatively stable. At this point in the development process, it does not appear that the SSA WAN architecture will change much at the logical level, but rather, at the physical

implementation level. These changes will largely be driven by changes in the other SSA infrastructure architectures and emerging network technologies such as Multi-Protocol Layer Switching, as well as evolutionary upgrades for the existing products and associated hardware.

SSA recognizes that different telecommunications solutions will be needed depending on the nature, size and platform of the application. Emerging technologies will be studied to determine the most feasible approaches for intra-agency connectivity as well as inter-agency support. The use of technology designed to share bandwidth and to increase the economies of the network architecture will be a factored in the solution, regardless of application type.

Transition

Additional incremental bandwidth adjustments will be made for DMA sites (DDSs, OHA, and OQA) on an ongoing basis to meet DMA document retrieval requirements. Bandwidth adjustments will also be made in conjunction with Agency approval of increased video conferencing. In addition, we will implement monitors on new operating systems; implement new network management tools; test management of Voice over IP (VoIP); and institute new monitoring of AeDib/DMA.

Transition Strategy

Summary of strategy

This portion of the IRM Strategic Plan describes SSA's transition strategy for migrating from our existing IT architecture to a future (target) architecture. The strategy addresses the four major components of the SSA enterprise architecture—data, business processes, applications, and IT infrastructure. It defines the principles and methods that will be used to define schedules and manage the transition processes. These principles and methods are described in the following subsections.

Nature and Scope of the Transition Effort

SSA's transition planning makes use of the work done by the CIO Council's Architecture and Infrastructure Committee (AIC) and the five reference models; Business, Service Components, Technical, Performance and Data, which are in varying degrees of completion. The principles that drove this analytical process are illustrated in Figure 42.

The reader will note from Figure 42 that SSA does not expect its target enterprise architecture (over the next 3-5 years) to be drastically different than the existing architectural structure. The Agency envisions evolutionary, not revolutionary, architectural changes. SSA will embrace and move with new technology when it supports the Agency's mission and goals. However, the overall IT computing and data storage architecture should remain highly centralized, even as additional computing resources are added for local and regional offices. While SSA continues to upgrade and refine our existing systems (e.g., by adding web-based access capabilities), there are no plans for wholesale replacement of the existing programmatic application systems that have served it and its clientele so well for many years. In some cases new application systems will be developed and selected existing applications will be re-engineered, but these instances will be far outnumbered by initiatives that build upon the existing application base.

Transition planning is based on a conservative approach to systems management. SSA considers large system redevelopment and replacement efforts to be high-risk undertakings. Industry statistics support this view. The Agency prefers to build new system capabilities and enhance existing systems through a series of relatively small projects that can limit risks through effective project planning and rigorous project management.

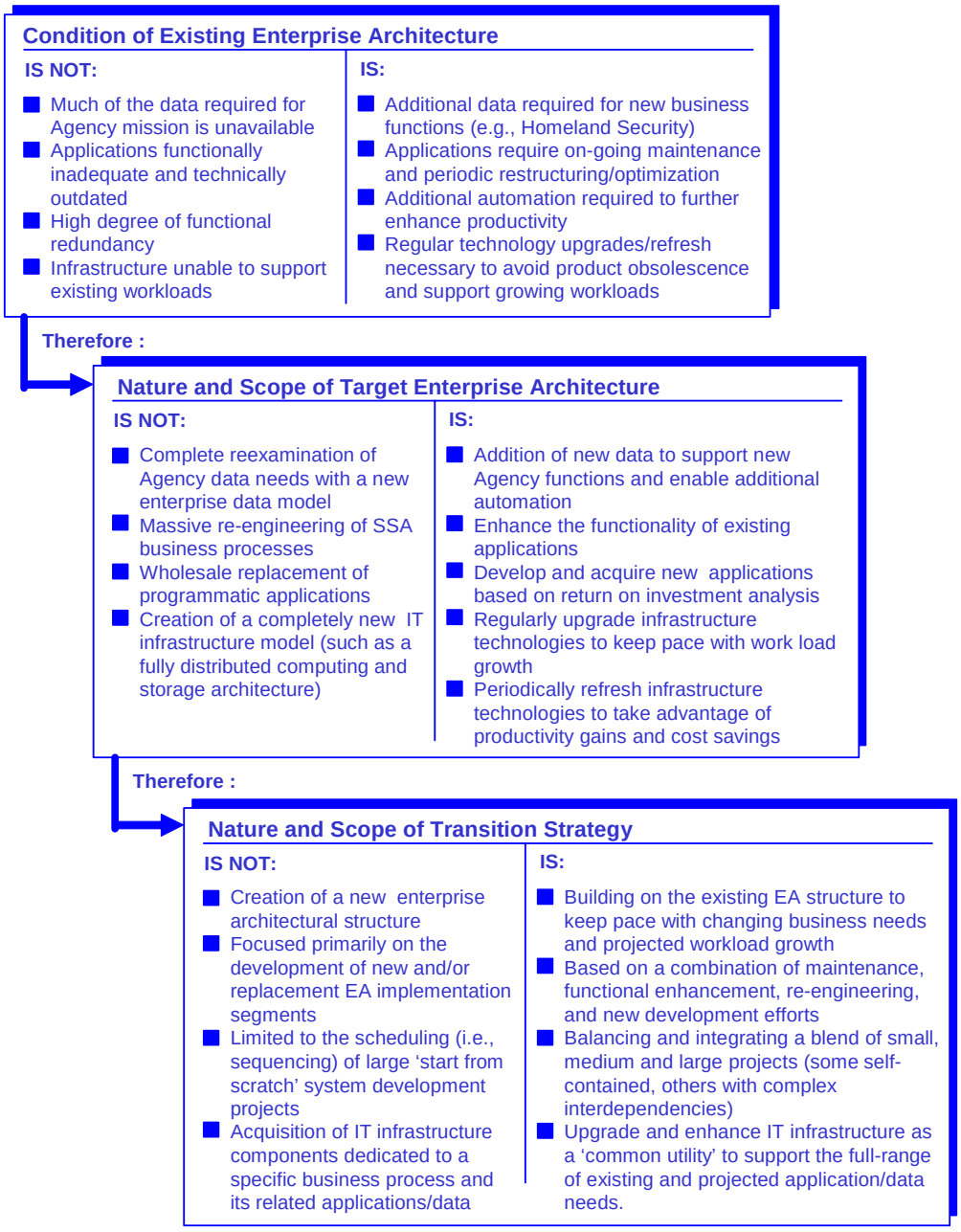


Figure 42: Basis of Transition Strategy

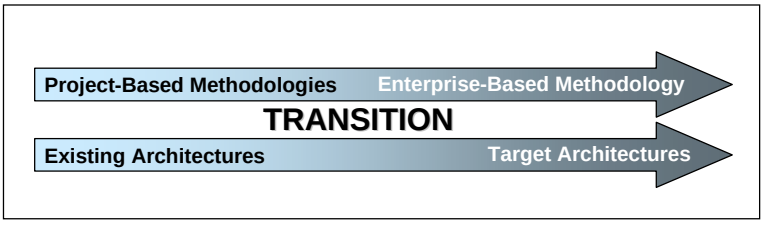
SSA's transition strategy (shown in Figure 42 above) is based on an objective analysis of the specific characteristics of our current and target enterprise architectures (as opposed to a generic methodology that presumes a step-wise replacement of existing IT architecture).

SSA's initiatives to upgrade our IT infrastructure will not typically be tied to a specific project or enterprise architecture (EA) implementation segment. Rather, infrastructure will be upgraded, refreshed and extended to serve as a common technology platform or utility that supports the full range of existing and projected

application systems. SSA will rarely establish an infrastructure environment that is for the sole use of a particular business process and its related application(s). We will continue to make use of shared IT infrastructure resources looking to optimize performance and limit costs based on economies of scale.

Adoption of Enterprise-Based Methodologies

SSA's transition planning actually has two distinct avenues of implementation. One involves the transition from the existing enterprise architecture to a future, target EA structure. This type of transition is discussed in some depth in the Federal Enterprise Architecture literature. The other transition path is well recognized but infrequently discussed. That is, how does an agency, such as SSA, transition from a well-established systems management environment based on *projects* to one based on the *enterprise?* And, since such a transition can not happen over night, how should IT initiatives be conducted during this transition period?



SSA has adopted the following strategy for continuing to push ahead with our critical IT initiatives as we incorporate enterprise architecture methods into our systems management processes:

- We have developed and continue to refine enterprise-based documentation of existing and target data, business process, applications, and infrastructure as quickly as we can without drastically curtailing critical systems maintenance, functional enhancement, and new development/acquisition efforts.
- SSA is developing and adopting architectural models in conformance with the architectural artifacts released by the Federal Enterprise Architecture Program Management Office (FEAPMO) within the Office of Management and Budget (OMB). The FEA Reference Models are: The Business Reference Model, the Performance Reference Model, the Service Components Reference Model, and the Technical Reference Model. This past spring we built a Business Reference Model (BRM) that aligns directly with the FEA BRM Version 2.0 published by the FEAPMO on June 12, 2003.
- We have established an Architecture Review Board (ARB) with experienced, knowledgeable technical and line-of-business representatives from all the SSA organizations involved in the IT acquisition, development and operations processes. The ARB serves the governance function for the enterprise architecture by enforcing adherence to the principles and standards of SSA's target architecture, including the following:

  - Ensure that system acquisition and development projects support the Agency's mission and its stated strategic business goals and objectives;
  - Ensure appropriate system security/privacy protections, and data accuracy/integrity protections are incorporated in all system implementation efforts;
  - Maximize return on investment of hardware and software purchases; for example, by use of standard tools, Enterprise licensing, large shared servers and movement away from server-attached direct access storage;
  - Ensure that developers use approved tools as shown in the new tools section of the EA; and,
  - Adhere to all applicable Federal and Agency IT standards.
- Major IT projects with potential to change any of the existing SSA business process, data, applications, or infrastructure architectures are evaluated for possible conflict with the evolving enterprise architecture. OESAE conducts this evaluation with oversight and approval provided by the ARB.
- When the OESAE/ARB evaluation determines that a pre-existing project is consistent with the evolving target architecture, the architectural components addressed by the project are identified as target architecture *implementation segments* for inclusion in the appropriate enterprise models.
- In any case where an existing project appears to be inconsistent with the target EA characteristics, the project is referred to the SSA Executive Staff for possible redirection or other corrective action. The SSA Chief Information Officer (CIO) leads the discussion of such referrals with the SSA Executive Staff.

Implementation Segment Selection

Upon completion of the five reference models and FEAMS, SSA will establish a new transition management process. The foundation of this process will be a more disciplined approach to the establishment of EA implementation segments.

The term implementation segment is defined as any IT project or program that is intended to supply an identifiable portion, or segment, of the SSA target architecture.

Selection of implementation segments is one of the most critical elements of SSA's enterprise-based approach to information resource management. Not only must a project map to a segment of the target architecture, it must also be:

- Properly sized so that that it is achievable within a limited time period;
- Focused on a portion of the target architecture that can be effectively isolated (i.e., it must represent a piece that that can be 'plugged' into the evolving IT architecture with a minimum amount of temporary bridging construction between old and new system components); and,

- Fit within a larger scheme of 'building block precedence' (i.e., a sequence of projects in which early-on projects establish a portion of the environment needed by follow-on projects).

The target approach to the selection of implementation segments will have two primary paths—top-down and bottom-up. The top-down method is the classical approach most discussed in current EA literature. This process, which is directly linked to the Agency-wide strategic planning process, will be conducted once each year. The existing IT architectures (data, business processes, applications and infrastructure) will be compared to the corresponding target architectures and a 'gap analysis' will be performed. The gap analysis will identify the remaining pieces of the target architecture that have not yet been developed or scheduled. These remaining pieces will then be divided into workable-sized chunks (implementation segments) and scheduled for development and/or acquisition. The top-down approach to implementation selection is illustrated in Figure 43. As the illustration description related to Figure 43 suggests, identification of implementation segments is the beginning, not the end, of the transition planning process.

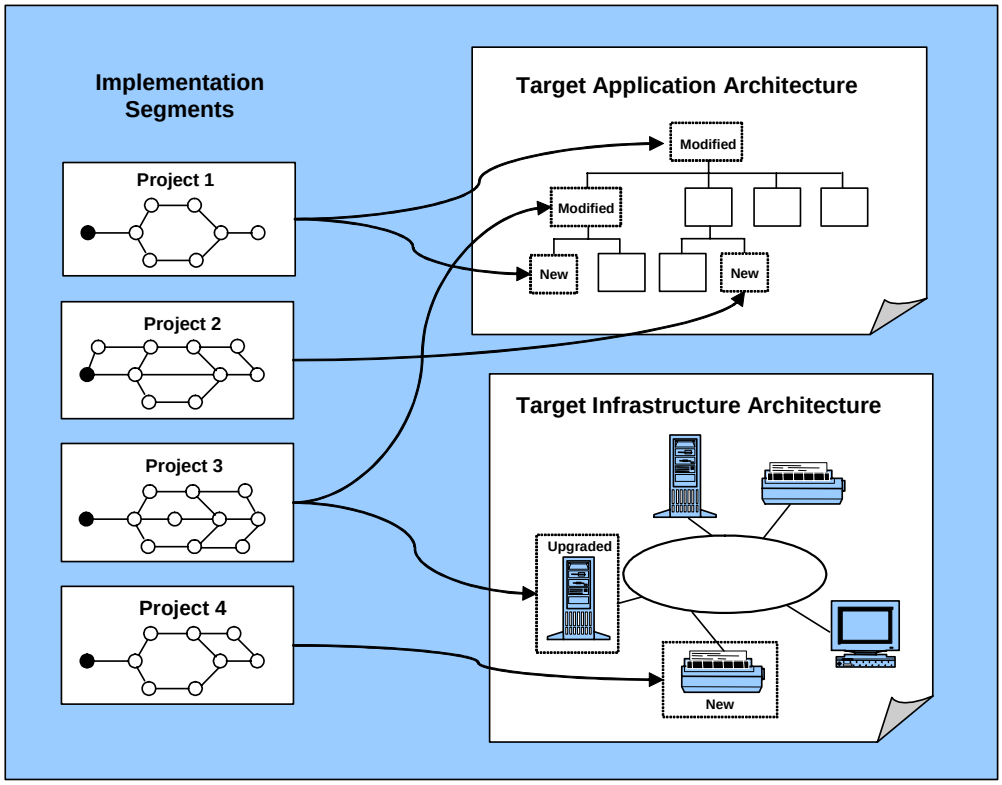


Figure 43: Identification of Implementation Segments

A straightforward mapping of implementation segments to the target architecture is adequate for project establishment. Additional transition planning is required to establish target installation dates and facilitate technology integration.

The bottom-up approach to implementation segments might not appear so orderly, but is no less needed. Important, even necessary, projects are going to bubble up from within the organization and from external sources (no matter how rigorous the strategic planning effort). Legislative changes, inter-agency initiatives, and unforeseen emergencies are only a few examples of the types of projects that are going to be created outside the orderly strategic planning processes. These projects also need to fit somewhere within the Agency target architecture definition. When projects of this type are identified, they will be compared to the evolving target architecture and evaluated for architectural compliance. Sometimes, because of the nature of these projects, it may be necessary to modify or extend the target architecture definition to accommodate an important initiative that was not considered when creating the currently defined EA target.

Implementation segments identified by either the top-down or bottom-up methods will be reviewed by the ARB as a quality assurance check to maintain the integrity of the transition process and the target architecture definition. During this review process, the ARB will use the documented target architecture definition (rather than relying solely on the knowledge, skills, and experience of the Board members).

Work Planning and Scheduling

SSA has a well-established work planning and scheduling process that will continue to be used, in more or less its current form, following the documentation of SSA's target enterprise architecture. This process pulls together all of the proposed and approved IT projects and arranges them in (customer) priority order based upon objective and subjective measurement of return on investment. See Chapter 8 for an overview description of this management process.

Readers of this document should be aware that the vast majority of the 'projects' that are ranked by the IT Prioritization Process will have no substantive impact on the Agency's applications or infrastructure architectures. This is because we do not attempt to build a new IT system to satisfy every new set of system requirements. In fact, our first and natural tendency is to incorporate new requirements within an existing architectural structure. This enables us to continue to control costs by realizing additional return on prior IT investments. The IT Prioritization Process does, however, provide important contributions to overall EA transition management; e.g.,

- IT initiatives are approved by a rigorous process that ensures project compliance with Agency mission and stated strategic goals and objectives;
- Positive return on investment or some other quantifiable benefit is established for approved projects;
- Customer prioritization begins to establish a relative order (sequencing) of projects that is essential to effective transition planning; and,
- The work planning process establishes a single, comprehensive, documented list of IT projects that need to be considered for transition planning.

The IT Prioritization Process also sets proposed implementation dates for each approved project. These dates need to be refined by more detailed transition planning, but they serve as important transition targets (that are not to be changed without consideration and agreement by the Agency's IT customer community). The subsequent subsections describe the methods used to refine target implementation dates and arrange projects in an orderly, achievable, transition sequence.

Prototypes, Pilots and Phased Implementations

As noted earlier, SSA takes a relatively conservative approach to the development and management of IT infrastructure and the application systems that use infrastructure services. An example of this conservative approach is the importance we place on the use of proof-of-concept experiments, prototypes, pilots, and phased implementations.

It is our standard practice to not adopt any new foundation technology (particularly one that represents a major paradigm shift for the Agency) without first thoroughly testing the new technology and its use in the SSA environment. This applies to new hardware and software technologies such as: operating systems, major operational support tools, database management systems, software development suites or languages, and application and infrastructure platforms, networking/communication protocols, security technologies, etc. It also includes Commercial Off-the-Shelf (COTS) products. Use of prototypes, pilots and phased implementations is one of the ways that we limit the risk of new implementation efforts and down-size projects into manageable undertakings. This controlled approach to the identification and controlled testing and introduction has been termed technology infusion. SSA cannot use such pilots to justify future noncompetitive acquisitions for the products being piloted. If such products are eventually acquired on a noncompetitive basis, approval must be obtained from the appropriate source selection authority.

As a general rule, we avoid the establishment of any project that would require more than 12 months to complete the development, testing, and integration phases of the system development life cycle (SDLC). When we are dealing with a new technology that has not been previously used within the Agency, we may begin with a proof-of-concept experiment (that would typically be conducted in a laboratory setting, such as the Office of Systems' Electronic Technology Center). We may conduct the experiment ourselves or invite an industry consortium (such as CommerceNet) to demonstrate the technology for an evaluation team of potential system users and IT professionals. In some cases, we may actually ask industry to assemble a prototype installation that illustrates the use of the new technology to perform the types of functions that would be required for the use of the technology in the SSA setting. If the results of experimentation and/or prototyping indicate positive potential, SSA may plan for a limited (pilot) implementation in SSA's production environment with a defined decision point at which the pilot will be evaluated for termination or expansion. This decision point discipline is targeted at controlling support requirements for technologies or products which, while attractive in the small scale, e.g., to the pilot test group, are discovered not supportable for their original, larger

intended customer base. If uncontrolled, unending "pilot" support requirements represent a cost which cumulatively will represent a serious drain on SSA manpower and budget resources.

Various methods can be used to minimize the impact and risk of pilot implementations such as limiting the volume of transactions that are directed to the pilot system, installing the pilot in only a limited number of SSA offices, or by conducting the pilot in parallel with the live production operations and comparing results from both. It should also be noted that SSA also makes extensive use of pilot implementations for other types of projects that do not involve new technologies. In fact, pilots are the SSA-preferred method for limiting the risk of many types of system implementations. In addition to pilot projects, SSA also routinely makes use of phased implementations as a way to ease the transition from one set of operating methods to a new method that may require on-site component installation, extensive user training, or similar considerations during the roll-out of a new systems capability.

In all of these types of incremental implementations, the various steps are treated as if they were separate projects. That is, they are scheduled separately and integrated within an overall framework of all other projects that are being conducted/targeted for the same time period. The orchestration and integration of such a collection of projects is discussed in the next subsection.

Integration Planning

A key element of the SSA approach to effective integration planning is to limit integration issues by structuring projects so that implementation activities are isolated and self-contained within a given project as much as possible. Other important principles are:

- Identify integration requirements early and plan the integration process;
- Disseminate information about the need to integrate as early and widely as possible;
- Give all parties as much time as possible to react and plan; and,
- Place integration steps in the project plans for related or impacted projects.

Our established approach to integration planning is to conduct such planning in layers. That is, first we integrate (organize and schedule) the projects and tasks that have impact just within a given major system (such as title II claims). At the same time, we identify the projects/tasks for that system that have impact on other systems or projects. This integration process is conducted by the system development component(s) responsible for the system in question, working with their counterparts in the SSA user community. All of the projects that have impact outside of a given system area are then brought together for integration within a larger framework (as an example, all of the systems that support the title II programmatic processes). At this higher level, the integration planning process is repeated based upon planning discussions conducted between collections of system developers and system users.

The integration planning process is then repeated at the next highest level for those projects that have integration dependencies across major architectural lines (such as projects that involve both programmatic and ADMIN/MI applications, or projects that involve both applications development and the acquisition IT infrastructure components).

The basic concept is to deal with integration planning at the lowest level possible and escalate to a higher level only those projects with integration issues or requirements that involve other architectural components or organizational entities. In theory, the number of projects with inter-component integration issues should substantially decrease as we move upward in the organizational structure. If we find that this is not the case, we then have evidence that we are not doing a good enough job in selecting and structuring projects so that most are self-contained and properly sized so as to minimize inter-project integration requirements. If we find that we have many projects reflecting complex inter-dependencies with other projects and across architectural lines, we then need to be less aggressive in scheduling many of these projects for the same time period. The primary outputs of this integration planning process are:

- A set of clearly defined integration tasks;
- An integration schedule that is cycled back into the Systems Work Planning Process to update the master list of projects with more refined target implementation dates; and,
- A set of *transition architectures* (that are discussed in the nest subsection).

Transition Architectures

Transition architectures are tools that are designed to (1) assist the transition planning process and (2) provide documentation of the results of the planning process. Simply stated, a transition architecture is a snapshot of a fully integrated, planned architecture as it will appear at some point in the future. Figure 44 on page 195 illustrates the process that is followed to develop transition architectures.

A transition architecture may be developed for any type of enterprise architecture, but we expect such definitions to be developed most frequently for future business processes, applications, and the IT infrastructure. The Office of Systems is responsible for organizing and publishing integration architectures based on information that it solicits from the SSA line organizations. The Office of Systems does not operate as a 'central planning' organization that develops transition plans for the rest of the Agency to follow. Rather, it ensures that the organizations involved in the IT management processes develop transition plans with proper attention to the special needs of effective integration planning. It then assembles the plans (checking to see that the integration linkages have been properly defined) and disseminates the plans throughout the organization for use by both the system development and system user communities.

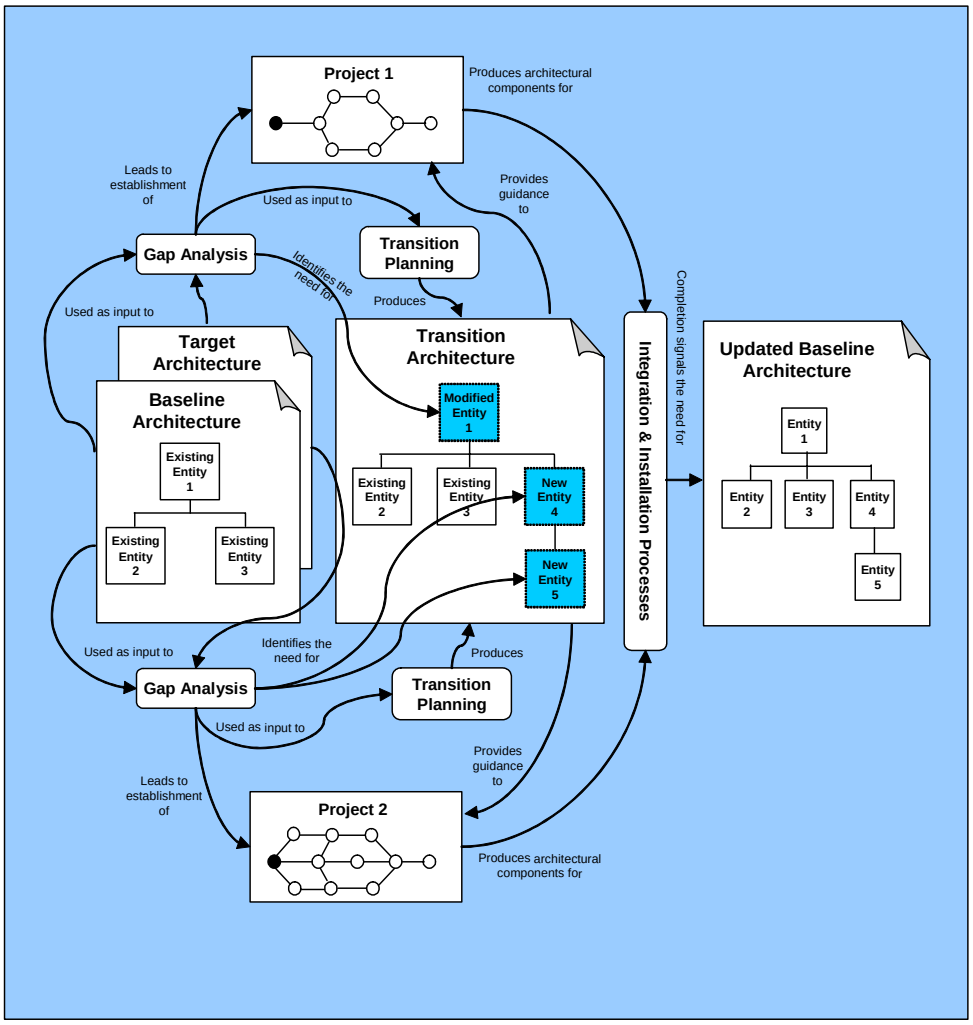


Figure 44: Transition Architectures

Transition architectures provide an integrated target for multiple projects scheduled for the same installation cycle. Following implementation, the existing architecture baseline is updated and a new transition architecture is established for the next implementation cycle.

Current plans call for transition plans to cover the upcoming one year period. The number of transition architectures that may be developed for each 1-year period will vary depending on the nature of the included projects and the frequency in which some aspect of the EA must change in order to accommodate these projects. During some 12- month periods there may be several checkpoints along the timeline where some aspect of the architecture will need to change. In these cases there will be several transition architectures for the 1-year period (maybe as many as one for each month).

In other cases, there may be only one or two major architectural modifications targeted for the upcoming year. In this case there would be only one or two transition architectures defined. The complicating factor will be the fact that transition architectures can and will be defined for each of the four types of IT architectures: data, business process, applications, and infrastructure. It will not be uncommon to have many transition architectures for say the IT infrastructure and applications with only a few, if any, transition architectures for data and business processes.

Integration Testing

Integration planning is an important part of the transition management process, but integration testing is the essential ingredient in the process. Planning deals with the expected; testing identifies the unexpected. While development organizations conduct various types of integration tests, a discrete office has primary responsibility for performing the enterprise-level integration tests for SSA application and infrastructure releases. There are three major challenges in conducting effective integration tests in the highly volatile SSA environment:

1. Provide future infrastructure configurations, as they will appear at time of target release points in the future. Target hardware/software infrastructure environments need to be acquired and put into place well in advance of the target production release date (so that application developers can conduct testing in the proper target environment).
2. Track the various target application and infrastructure configurations, as they will exist at each checkpoint across the transition period from today to an eventual target date in the future. This requires highly effective acquisition and engineering processes, plus strong configuration management.
3. Build and maintain the libraries of comprehensive test data that will be needed to conduct the various types of integration and related tests needed for effective transition management.

Application development organizations focus on the functional aspects of integration testing (e.g., do software components link and communicate properly passing data and control as envisioned in the application design). SSA conducts regression tests for changes to existing applications systems to ensure that planned modifications do not result in unintended changes that degrade the existing functionality of production systems. The Agency also conducts regression tests with more focus on maintaining the operational integrity and performance profile of the overall application and infrastructure environment.

Communication and Feedback

There are those who say that the real benefit of integration and transition planning is in the doing. That is, it's the process of making the pieces fit together that actually provides the knowledge needed for effective IT management. This is only partially true.

The people that do the planning obviously benefit from the process and gain insights that they would not otherwise acquire. But, integration and transition plans are developed to be shared and used as tools for effective implementation management. It is, therefore, essential that these plans are widely communicated throughout the Agency and that feedback is used to keep the plans current and relevant. SSA will use what amounts to a 'full court press' to disseminate information about transition plans and schedules:

- Plans will be posted to SSA's internal Intranet, including the Enterprise Architecture (EA) website;
- A combination of memorandums, procedural revisions, and e-mail broadcast messages will be used (as they are today) to pass along information about planned system implementations;
- Various types of conferences are held throughout the year to keep line managers up-to-date on future system plans;
- The Systems Work Planning process conducts major work prioritization and scheduling discussion each quarter; and,
- Application system developers and their counterparts in the SSA field and Central Office organizations met regularly to discuss upcoming system implementation plans and to resolve integration issues such as those that result from project inter-dependencies.

SSA uses the feedback that results from these communication forums to update the Systems Work Plan and the associated transition architectures.

Conclusion

With the completion of its enterprise architecture within the last six months, SSA's transition planning process has matured significantly. We are incorporating the five reference models into our systems life cycle and have expanded on efforts to collaborate with other federal agencies. Our ever-increasing focus on e-government is evidence of our commitment to the Federal Enterprise Architecture.

SSA plans to continue its efforts to improve its EA. This year we conducted a market survey of EA tools and acquired and implemented METIS, a robust EA modeling tool. We are wrapping up a major analysis of our ARB process and hope to implement improvements soon, requiring greater involvement of business process experts. One such improvement is already well underway: the development of business architecture principles. These principles will serve as important guidelines for the ARB and for development of data, applications and infrastructure principles.

Finally, beginning this year, SSA has implemented an Independent Verification and Validation (IV&V) process hereby a third party subject-matter expert reviews our entire EA for completeness, conformance with OMB requirements, and level of maturity. Through these reviews, we will continuously improve our enterprise architecture.

SSA IT Systems Security Plan

Introduction

The Social Security Administration (SSA) is responsible for administering the most successful domestic programs in the nations' history; the Old Age Survivors Insurance, Disability Insurance and the Supplemental Security Income programs. To accomplish its mission, SSA collects and maintains some of the largest electronic files of personal data held by any Federal agency. SSA efficiently integrates activities across all these programs through a single national service delivery structure supported and enabled through its information technology (IT) systems. Key business processes and associated financial management operations are performed electronically, e.g., enumeration, individual wage and earnings tracking, claims tracking, claims processing and death registration. This level of IT integration, combined with processing sensitive, unclassified data on over 260 million citizens, requires SSA to put considerable emphasis on information security.

Numerous governing directives and sound management principles have resulted in SSA implementing a security program that is comprehensive and far-reaching, and which is continually evaluated and enhanced to effectively protect its diverse ITS resources, including data. SSA has installed many safeguards and implemented management controls Agency-wide to protect the confidentiality, integrity and availability of SSA's systems, data, and all ITS assets critical to SSA's mission.

Incorporating and Funding Security in Information Systems Investments

The Office of Management and Budget (OMB) requires that agencies be able to demonstrate that security has been integrated into all information systems. OMB's preference is that security infrastructure costs be related to each IT system/application for which a Capital Asset Plan is submitted. As a result, SSA has adopted a "proportional utilization" model allocating security for IT initiatives based on workstations affected by the initiative. Below are the IT security expenditures in the FY 2005 Capital Asset Plan. Specific project details are available in SSA's Resources Exhibit 53.

IT Security Costs (in millions)		
Projects	**FY 2004**	**FY 2004**
Financial Management Systems	$ .2	$ .2
Service Initiatives	11.0	9.4
Stewardship Initiatives	7.7	7.4
Staff Initiatives	4.0	3.2
Infrastructure	14.1	13.4
Telecommunications	6.8	7.9
Office Automation	3.6	3.7
Software Imaging Management	3.6	3.7
Enterprise Architecture & Planning	3.6	3.7
Totals	**$ 54.5**	**$ 52.5**

SSA's Security Architecture

SSA has formally adopted a Security Architecture modeled after the OMB Architecture and integrated with the Enterprise Architecture model of the agency and OMB's Federal Enterprise Architecture model.

SSA's Security Architecture model is comprised of seven layers which roll-up into the suggested four layer OMB model (figure 1.) The seven layers include:

- Resources;
- Applications;
- Physical;
- Technology;
- Authentication;
- Administration; and
- Policy.

Across these enterprise layers, access and interaction takes place through four clearly defined user paths:

- Employees;
- External Government Agencies;
- Business Partners; and
- Public.

Specifically, the Policy and Authentication layers of the architecture have unique requirements and controls to address each of the access groups.

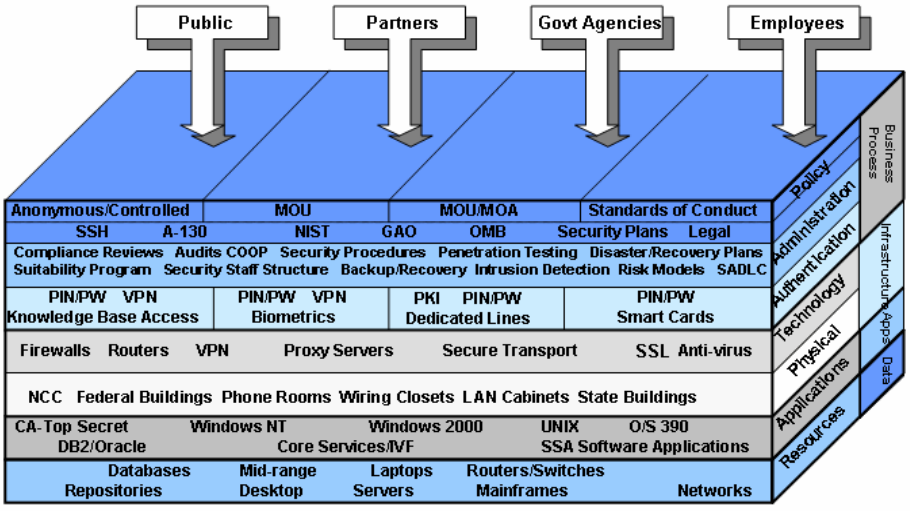


Figure 45: SSA's Security Architecture

The three basic security services of Confidentiality, Integrity and Availability (CIA) are ensured through the implementation of a three-tiered approach to access control:

- Identification;
- Authentication; and
- Authorization

The discrete techniques and technology used to provide these controls vary based upon the entity seeking access and the resource or resources being requested.

Identification

SSA's IT Security Policies (Layer 7 of the architecture) have been designed to respond to a user community that includes the following four user security groups:

- *Employees and trusted individuals*—SSA employees, Disability Determination Service employees, and trusted individuals who have access credentials. Currently, these credentials most often take the form of Personal Identification Numbers (PIN) with some use of Public Key Infrastructure (PKI) digital certificates for remote employee access. Within the constraints of the security architecture, this user community may access intranet, mainframe, and client/server resources.
- *Government Agencies*—External government agencies / entities with which SSA does business and exchanges information are issued

credentials either to individuals or applications within the partner agency. These agencies / entities include States and other government organizations such as the Department of the Treasury, Department of Education and the Bureau of Vial Statistics.

- *Business Partners*—These are non-governmental entities with which SSA does business. An organization may be given a unique identifier in order to access SSA resources. Individuals within the organization (designated by the organization and SSA) may have a separate unique identifier.
- *General Public*—The public is divided into two major categories; those without SSA access credentials, i.e. anonymous users, and those with SSA access credentials. These credentials most often take the form of PINs. National 800 Number users are included in this user security group.

Authentication

The Authentication Layer (Layer 5 of the architecture) is used to validate the authenticity of the requestor's credential(s). The technology in this service layer will identify the requestor's user security group and validate his or her identification. Each user security group is authenticated against a distinct database with distinct credentials. The authentication mechanisms differ for each user security group. For example, each employee is assigned a unique PIN and password that identifies them to the SSA environment. This PIN/Password is stored in a security database. PKI credentials are authenticated against both internal and external certificate services as well as some pilot validation and authentication activities performed in collaboration with the GSA sponsored E-Authentication Gateway and the Federal Bridge CA. Additional authentication services available within this layer include Knowledge Based authentication and some Biometric capabilities.

Authorization

This very important activity is performed by services located primarily in Layers 7, 4 and 2. Policy describes what resources an authenticated entity should have access to and what that access should allow. Technology allows authenticated entities to pass while blocking unauthorized attempts (a sort of first-line gatekeeper), and security software applications, such as CA-TOP SECRET, provide discrete and granular access to final resources based on policy matrices.

Within a valid authorization, the permitted resources may be further constrained by the role that the user is allowed to assume. The physical machine(s) at which the user's requests are serviced may vary based on authentication and role. For example, employees will be authorized to use specific resources and transactions based on a profile that has been identified by SSA. Business partners have signed a contract with SSA and have been given authorization to access specific SSA resources and transactions. They do not have access to any of the internal business applications

Other Security Considerations

In addition to the security services previously discussed, the security architecture provides a host of necessary services to ensure the overall safeguarding of SSA's IT resources.

Layer 1—Resources—Provides some native security functionality inherent in the environment within which the resources reside. These include such protections as Data Base access protocols, Router and Switch configurations, server security configurations and more. Some encryption services reside within this layer, particularly those that protect data on mainframe communication channels.

Layer 2—Applications—Provides additional security functionality not only through the previously described security applications, but also through native MS-Windows NT and 2000 logon services, process application specific security and native ZoS security features.

Layer 3—Physical—This layer is core to the secure operating environment for all of SSA's IT service providing technology. Most can be found in the SSA National Computing Center (NCC) where extensive physical controls are in place and tested. However, many physical controls extend to the Regional and field office locations where hardware and software reside along with protected telephonic resources.

Layer 4—Technology—Protection provided by Firewalls, Proxy Servers, and configured Routers make up the preponderance of hardware-based security but there are also services provided in depth by Secure Socket Layer, encryption, anti-virus, VPN and Secure Transport software-based solutions.

Layer 5—Authentication—This layer supports all of the functions previously identified in the Authentication discussion through the use of PIN / Password schemas, Knowledge Based database approaches, PKI (digital certificates), Smart Cards, Biometric devices and schemas, as well as dedicated protected communication lines between some resources.

Layer 6—Administration—Here is where much of the assurance for continued resource protection is maintained. A vast array of security controls such as Disaster Recovery and Continuity of Operations Plans ensure non-interrupted services. Extensive audit procedures ensure compliance and effectiveness of all security controls in place. Risk Models ensure that machine configurations are current and in compliance with best practices. Penetration Testing programs and Intrusion Detection services ensure the secure operation of the network facilities. Suitability programs ensure that due diligence has been taken prior to allowing personnel to occupy positions of trust within the security program and finally, a large SSA Security Staff organization ensures that all of the security policies, procedures, controls and approaches are functioning, effective and state-of-the-art at all times.

Layer 7—Policy—This all-important first step in the Security Architecture provides overall guidance and direction to the entire security operation. Policy is developed to provide compliance with all mandated external security guidance such as that produced by OMB, NIST, GSA and other governing agencies as well as policy to

enable SSA's unique security functionality and architecture such as Security Plans for each major application and system.

Agency Current and Future IT Security Initiatives

New security standards and technology are always being integrated into SSA's business processes to protect software and hardware from both physical and cyber security threats. Efforts underway include the following:

Intrusion Detection

This initiative includes increased penetration testing conducted from within as well as by outside experts.

- SSA has established an Intrusion Protection Team comprised of Systems technical experts supported by contractors. They anticipate and test potential vulnerabilities, validate proposed system patches as well as monitor systems activities for potential attacks and analyze trends.
- SSA contracted with IBM Managed Security Services (MSS) to provide real-time Intrusion Detection Services (IDS). IDS uses IBM's in-house NSA scanning/reporting product and other off-the-shelf products. These technologies identify attempts to gain unauthorized access to network resources and consist of four elements:
    1. Sensors;
    2. 24/7 Monitoring;
    3. Incident Control and Recovery; and
    4. Investigative Services.

MSS performs a weekly compliance test on SSA's external network including the firewalls and web servers. A monthly hard copy audit report is produced, documenting the results of the weekly compliance testing, monthly vulnerability evaluations and intrusion detection services. This contract also provides a proactive search service that provides information about computer and network security vulnerabilities, as well as technical support from IBM resources to answer specific security questions pertaining to our environment.

Smart Card Technology

The Smart Card can be used as an identity card, allowing a number of security features, including biometrics, to authenticate identification. Card personalization may include a picture and personal data including name, agency and other basic information.

SSA has replaced the first generation remote access technology, Remote LAN Node (RLN), with the new Virtual Private Network (VPN) technology. The VPN allows remote users to securely connect to a private network via the Internet or an IP (Internet Protocol) backbone, while providing optimum security to the SSA Network.

SSA incorporated additional security to the VPN solution with the introduction of the Safenet SmartCard. The SmartCard is the key to additional encryption and authentication technologies. The combined technology of a digital certificate on the card and a Personal Identification Number (PIN)/Password allows authentication of the individual requesting access. The SmartCard meets the present security requirements of "What you have (SmartCard)" and "What You Know (PIN/Password)". SSA now requires all remote access clients to use SmartCards. The required SmartCard technology (designed by Safenet/IRE) provides front-end authentication as well as additional encryption capability.

Biometrics

SSA is currently reviewing and evaluating the use of biometrics in combination with SmartCard technology. SSA is reviewing the Fingerprint Scan biometric option, and will evaluate and test other biometric solutions before determining if biometrics is a viable option to employ at SSA.

Biometrics involves the use of a unique biological feature used to verify the identity of an individual through automated means. The biological feature may be based on a physiological or behavioral characteristic. The physiological characteristics measure a physical feature such as a fingerprint or face. The behavioral characteristics measure a reaction or response such as a signature or voice pattern. The biometrics available under the Smart Identification Card include:

1. Fingerprint Scan;
2. Hand Geometry;
3. Facial Recognition;
4. Iris Scan; and
5. Voice recognition.

Access Control (Computer Associates - Top Secret)

Standardized Security Profile Project (SSPP)

SSPP is being implemented. The SSPP will require that all access be provided via approved 'standardized profiles' which will alleviate all individual access. This effort will require that all non-standard profile names be changed, dataset naming conforms to standards of the data dictionary and all administration must be performed through the Top Secret Admin Screens.

PSC Segregation of Duties

Profiles are being built to segregate programmer access from operator access. The final analysis and directives are being prepared in concert with each region.

eTrust Single Sign-On (SSO)

SSO is one of several supplemental authentication devices SSA is exploring for possible wide-scale use within SSANet. Supplemental authentication devices being

considered are biometrics and smartcards (mentioned above), PKI, key fobs or a combination.

Agency objectives include interoperability with computing platforms, possible elimination of user maintained passwords, improvements in user account management, improved authentication controls and strengthened security for mobile users.

As SSANet has evolved from a limited platform, centralized network into multi-platform, decentralized local area networks with remote connections to hundreds of trusted business partners, the need for improved security access has escalated. The growth of SSANet into dissimilar computing platforms has increased complexity in managing user accounts and enforcing uniform information systems security policies such as password management.

While growth of SSANet has benefited the Agency's overall mission, new risks to the enterprise exist as the system is opened up to more outside attacks. The more sensitive web-based enterprise applications are particularly vulnerable if not protected sufficiently. The first line of defense in mitigating these vulnerabilities is access management technology. Firewalls, encryption, VPN and PKI complement access management to harden the environment.

Recent government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) (which sets stringent standards for healthcare organizations to protect the confidentiality of stored and transmitted patient data), and digital signature legislation such as the E-Sign Act (which confers legal validity to digital signatures, allowing transactions to be completed online) are only two items driving the need for strong authentication and non-repudiation.

Roles and Responsibilities

SSA's information security program is broad in scope and covers all components of the Agency. It relies upon an effective Agency network of security coordinators and executives to be successful. The following SSA executives, and designated individuals within their respective components, have specific responsibilities for maintaining SSA information systems security.

Chief Information Officer (CIO)

The CIO is an executive position within each Federal agency established by the Information Technology Management Reform Act of 1996. The CIO is directly responsible to the Commissioner of Social Security (COSS) for developing the Information Resource Management Plan and defines the Information Technology (IT) vision and strategy for the SSA. The CIO advises the COSS in all areas of information resource management, oversees the design, development and implementation of information systems, and monitors and evaluates systems performance.

SSA Chief Security Officer (SSACSO)

The CSO is directly responsible to the CIO and heads the Office of Information Technology Security Policy in the OCIO. The CSO is responsible for directing and managing SSA's overall information systems security program, including the development of SSA's IT security policy requirements, and the effective implementation of other governing directives. The CSO also guides SSA-wide security awareness programs for management and employees on IT security policy, setting policy for SSA's state information exchange program and leading and coordinating IT physical security policy.

Office of Systems Security Operations Management (OSSOM)

The OSSOM is responsible for the operational program management responsibilities for IT systems security under the Deputy Commissioner for Finance, Assessment and Management's Office of Financial Policy and Operations. OSSOM directs, coordinates and manages SSA's information systems security programs and includes the development of SSA's security program requirements and procedures and overseeing the implementation of governing directives in the areas of systems security. OSSOM works through a network of designated information systems security coordinators in other SSA components (and outside organizations linked electronically with SSA) who assist in coordinating the Agency's national program. The network includes:

- **Center Directors for Security and Integrity (CDSI)**—formerly Regional Security Officers (RSO)—an individual in every SSA regional office who is responsible for region-wide security coordination;
- **Component Security Officers (CSO)**—an individual in every SSA headquarters component who is responsible for their component's security coordination;
- **Local Security Officers (LSO)**—an individual in every SSA field facility who is responsible for local security coordination; and
- **External Security Officials**—SSA has many information exchange partners in both the Federal government and the states. These entities also have designated security officials who act as an extension of SSA's internal network to ensure information systems security aspects of their agreements with SA are properly implemented.

Office of Facilities Management (OFM)

OFM, in conjunction with the SSACSO, is responsible for developing physical security policies and controls and assuring that those controls are properly implemented throughout SSA's facilities nationwide. OFM also uses a network of individuals in other SSA components to carry out their responsibilities. This network includes:

- **Regional Security Coordinators**—individuals in each SSA regions who are responsible for region-wide physical security coordination; and
- **Headquarters Physical Security Specialists**—OFM employees who work with designated security coordinators in each SSA headquarters facility.

Deputy Commissioner for Systems (DCS)

The DCS assures that SSA systems are developed with the necessary security controls in place.

Deputy Commissioner for Operations (DCO)

The DCO also is responsible for managing the network of CDSIs and LSOs who work with the SSASCO to carry out SSA's security program.

Office of Inspector General (OIG)

The SSA OIG is responsible for monitoring SSA programs, and reporting possible vulnerabilities to the Commissioner.

All Deputy Commissioners

SSA's Deputy Commissioners are responsible for assuring that security requirements are met within their scope of operations.

Glossary

#

24/7	24 hours per day, 7 days per week

A

ABA	Administrative Business Architecture
ABC	Administrative Budget Control System
ACD	Automatic Call Distributor
ACs	Associated Commissioner
ACT	Assignment and Correspondence Tracking System
AeDIB	Accelerated Electronic Disability
AFP	Advanced Function Presentation
AIF	Application Interface Facility
API Net	Administrative Payment Information Network
APP	Agency Performance Plan
ARB	Architecture Review Board
ASDLC	Application System Development Life Cycle
ASG	Allen Systems Group
ASP	Agency Strategic Plan
ATM	Asynchronous Transfer Mode
AWS	Alternative Work Schedule

B

BCAS	Benefit Certification and Accounting System
BDC	Backup Domain Controller
BEST	Benefits Estimate Calculator
BEVE	Benefits Verification
BLOB	Binary Large Object

C

CAS	Cost Analysis System
CCB	Configuration Control Board
CHIP	Customer Help and Information Program
CICS	Customer Information Control System
CIFEC	Central Iowa Federal Executive Council
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPP	CIP Plan
CM	Configuration Management
CMM	Capability Maturity Model
COTS	Commercial Off-The-Shelf
CPIC	Capital Planning and Investment Control
CPMS	Commercial Printstream Management Software
CPU	Central Processing Unit
CS	Computer Science
CTI	Computer/Telephony Integration

D

DARPA	Defense Advanced Research Projects Agency
DASD	Direct Access Storage Device
DBMS	Data Base Management System
DCS	Deputy Commissioner for Systems
DDS	Disability Determination Services
DEADA	Division of Enterprise Architecture and Data Administration
DHCP	Dynamic Host Configuration Protocol
DI	Disability Insurance
DIET	Division of Integration and Environmental Testing
DLT	Digital Linear Tape
DOC	Data Operations Center
DOCS	Distributed Online Correspondence System
DRMS	Data Resource Management System

E

e-mail	Electronic Mail
EA	Enterprise Architecture
EDCS	Electronic Disability Control System
eDib	Electronic Disability System
EDR	Electronic Death Registration
EITA	Enterprise Information Technology Architecture
EMIS	Executive and Management Information System
E-R	Entity-Relationship
ESD	Electronic Service Delivery
eTC	Electronic Technology Center
EVS	Enumeration Verification System
EVVE	Electronic Verification of Vital Events
EWR	Electronic Wage Reporting
EWRS	Electronic Wage Reporting System
EWD	Employees with Disabilities

F

FACTS	Financial ACcounTing System
FASB	Federal Accounting Standards Board
FAWG	Federal Architecture Working Group
fax	facsimile
FDDS	Federal Disability Determination Services
FedCIRC	Federal Computer Incident Response Center
FI	Financial Institutions
FIVR	Financial Interactive Voice Response System
FO	Field Office
FPPS	Federal Personnel/Payroll System
FSP	Foreign Service Post
FTE	Full-Time Equivalent
FTETS	Full-Time Equivalency Tracking System

FTP	Full-Time Permanent File Transfer Protocol
FTS	Federal Telecommunications System
FY	Fiscal Year

G

GLTP	Graduate-Level Training Program
GOTS	Government-Developed Off-The-Shelf
GPEA	Government Paperwork Elimination Act
GPRA	Government Performance and Results Act
GUI	Graphical User Interface

H

HP	Hewlett-Packard
HR	Human Resources
HRMIS	Human Resources Management Information System
HTML	Hypertext Markup Language

I

IAA	Inter-Agency Agreement
IBM	International Business Machines
ICN	Iowa Communications Network
ICR	Intelligent Character Recognition
IDM	Imaging and Document Management
IDMS	Integrated Data Base Management System
IMRC	Internet Medicare Replacement Card
INR	Intelligent Network Routing
IP	Internet Protocol Immediate Payments
I-PLC	Internet Project Life Cycle
IPT	Intrusion Protection Team
IRM	Information Resources Management
IRIB	Internet Retirement Insurance Benefits

IRS	Internal Revenue Service
IS	Information Systems
ISA	Information Systems Architecture
ISBA	Internet Social Security Benefits Application
ISP	Information Systems Plan
IT	Information Technology
ITA	Information Technology Architecture
ITAB	IT Advisory Board
ITAP	Information Technology Architecture Plan
ITMRA	Information Technology Management Reform Act
ITS	Information Technology Systems
IVEN	Interactive Validation Environment
IVT	Interactive Video Teletraining
IWS	Intelligent Workstation

J

JAD	Joint Application Design
JES	Job Entry Subsystem
JEVP	Joint Employment Verification Pilot
JFMIP	Joint Financial Management Improvement Program

K

kbps	kilobits per second

L

LAN	Local Area Network
LPARS	Logical Partitions

M

MAA	Metropolitan Area Acquisition
MACs	Moves, Adds and Changes
MADAM	Master File Access Method

MATPSC	Mid-Atlantic Program Service Center
MATSSC	Mid-Atlantic Social Security Center
mbps	megabits per second
MCAS	Managerial Cost Accounting System
MFD	Multifunction Device
MI	Management Information
MISF	Management Information Services Facility
MMS	Managed Member Server
MOA	Memorandum of Agreement
MSP	Microsoft Project
MTAS	Mainframe Time and Attendance System

N

NAPHSIS	National Association of Public Health Statistics and Information Systems
NCC	National Computer Center
NCSC	Network Customer Service Center
NIST	National Institute of Standards and Technology
NMF	Network Management Facility
NOC	Network Operations Center

O

OC	Office of the Commissioner
OCIO	Office of the Chief Information Officer
ODBC	Open Data Base Connectivity
ODS	Operational Data Store
OESAE	Office of Enterprise Support Architecture and Engineering
OHA	Office of Hearings and Appeals
OITSP	Office of Information Technology Security Policy
OITSR	Office of Information Technology Systems Review
OLAP	Online Analytical Process
OMB	Office of Management and Budget
ONRS	Online Notice Retrieval System

OS	Office of Systems
OSSOM	Office of Systems Security Operations Management
OTSO	Office of Telecommunications and Systems Operations
OUTSS	Official Union Time Tracking System

P

PARR	Payroll Analysis Recap Reports
PBX	Private Branch Exchange
PC	Personal Computer
PCRS	Purchase Card Requisition System
PDC	Primary Domain Controller
PDD	Presidential Decision Directives
PE	Postentitlement
PEBES	Personalized Earnings and Benefit Estimate Statement
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PM	Project Manager
PMA	President's Management Agenda
P/MF	Print/Mail Facility
PMIS	Payroll Management Information System
PPF	Programmatic Processing Facility
PRIDE	Project Resource GuIDE
PSC	Program Service Center
PTMI	Prisoner Tracking Management Information
PVC	Private Virtual Circuit

Q

QA	Quality Assurance
QC	Quality Control

R

RAD	Rapid Application Development

RAS	Resource Accounting System
RDBMS	Relational Data Base Management System
RFACTS	Financial Accounting System Replacement
RLS	Record Level Sharing
RO	Regional Office
ROCC	Regional Operational Communications Center
ROI	Return on Investment
RPC	Remote Procedure Calls
RSDI	Retirement, Survivors and Disability Insurance

S

SAN	Storage Area Network
SAR	Sysout Archive and Retrieval System
SBU	Sensitive But Unclassified
SCSI	Small Computer System Interface
SDLC	System Development Life Cycle
SEF	Software Engineering Facility
SEI	Software Engineering Institute
SEPSC	Southeastern Program Service Center
SLC	Site LAN Coordinator
SMS	System-Managed Storage Systems Management Server
SNA	Systems Network Architecture
SOLQ	State Online Query
SONET	Synchronous Optical Network
SPI	Software Process Improvement
S-PLC	Standard Project Life Cycle
SQL	Structured Query Language
SRP	Systems Rotational Program
SSA	Social Security Administration
SSACSO	Social Security Administration's Chief Security Officer
SSANet	SSA Communications Network
SSASRT	SSA Agency-wide Security Response Team

SSASy	SSA's Streamlined Acquisition System
SSI	Supplemental Security Income
SSL	Secured Sockets Layer
SSN	Social Security Number
SSR	Supplemental Security Record
SSS	Social Security Statement
STTP	Systems Technical Training Program
SYSPLEXES	System Complexes

T

TDD	Telecommunications Device for the Deaf
TM	Travel Manager
TONS	Training Online Nomination System
TPPS	Third Party Payment System
TSC	TeleService Center
TSR	Teleservice Representative
TTS	Text-to-Speech
TWG	Technical Work Group

U

UDB	Universal DDS Backbones
UPS	Uninterruptible Power Supply

V

VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VSAM	Virtual Storage Access Method
VTC	Video Teleconferencing

W

WAN	Wide Area Network
WBS	Work Breakdown Structure

WICS	Workstation Initiated CICS Server
WMS	Workload Management System

X

XML	Extensive Markup Language

Z

z/OS	Operating System Software

Index

Accelerated Electronic Disability System (AeDib), 45, 46, 117, 150, 151, 153, 155, 161, 162, 184
Administrative Budget Control System (ABC), 208
Administrative Business Architecture (ABA), 119, 121, 122, 123, 208
Administrative Payment Information Network (API Net), 120, 208
Administrative Systems, 119
Advanced Function Presentation (AFP), 164, 165, 208
Agency Performance Plan (APP), 1, 8, 9, 10, 208
Agency Strategic Plan (ASP), 1, 6, 7, 8, 9, 10, 23, 36, 76, 94, 156, 208
Application Interface Facility (AIF), 134, 135, 208
Application Software, 6, 25, 35, 47, 55, 64, 75, 108, 109, 112, 114, 116, 117, 118, 134
Architecture Review Board (ARB), 68, 69, 113, 188, 189, 191, 197, 208
Asynchronous Transfer Mode (ATM), 44, 159, 180, 181, 182, 183, 208
Audit Test Facility, 161
Automated Call Distributor (ACD), 208
Backup Domain Controller (BDC), 139, 208
Benefit Certification and Accounting System (BCAS), 119, 124, 208
Biometrics, 29, 30, 78, 159, 170, 171, 201, 202, 203, 204, 205
Budget, 1, 3, 4, 5, 6, 7, 8, 9, 10, 17, 28, 36, 40, 47, 52, 61, 62, 68, 86, 90, 92, 95, 96, 107, 119, 120, 126, 157, 188, 193, 198, 208, 213
Capability Maturity Model (CMM), 64, 66, 67, 70, 85, 209
Capacity, 5, 6, 14, 32, 35, 43, 67, 71, 72, 117, 153, 156, 161, 162, 173, 174, 176, 182
Chief Information Officer (CIO), 10, 14, 17, 19, 20, 22, 27, 68, 85, 186, 189, 205, 206, 209, 213
Circular A-130, 7, 48, 61, 68
Claims, 31, 35, 43, 45, 47, 49, 50, 51, 75, 98, 100, 103, 104, 105, 106, 112, 115, 116, 117, 125, 126, 153, 159, 180, 193, 198
Clinger-Cohen Act, 6, 28, 61, 68
Commercial off-the-shelf (COTS), 22, 25, 48, 70, 114, 117, 118, 119, 120, 121, 122, 123, 124, 127, 128, 129, 130, 132, 133, 135, 142, 149, 150, 153, 156, 171, 192, 209
Communications Network, 6, 180, 211, 215
Configuration Control Board (CCB), 69, 209
Cooperative Processing, 64, 84, 85, 87, 88
Core Business Processes, 98, 99
Customer Help and Information Program (CHIP), 155, 209
Customer Information Control System (CICS), 66, 71, 84, 119, 134, 141, 153, 156, 161, 209, 217
Data Center Management, 70
Data Operations Center (DOC), 102, 176, 209
Database Architecture, 133, 141
DataBase Management Systems (DBMS), 23, 118, 129, 131, 132, 135, 141, 142, 209
Direct Access Storage Devices (DASD), 160, 172, 173, 209
Disability Determinations Services (DDS), 43, 46, 47, 48, 104, 110, 143, 144, 145, 146, 147, 156, 159, 161, 162, 167, 180, 183, 209, 216
Disability Insurance (DI), 2, 5, 47, 103, 198, 209, 215
Disaster Test Facility, 161
Distributed Online Correspondence System (DOCS), 113, 209

Distributed Shared Server, 138, 139
Earnings, 1, 8, 35, 42, 46, 47, 98, 100, 101, 102, 103, 104, 115, 116, 126, 133, 198, 214
Electronic Disability Control System (EDCS), 45, 210
Electronic Disability System (eDib), 43, 44, 45, 210
Electronic Folders, 150
Electronic Service Delivery (ESD), 3, 4, 7, 39, 40, 49, 109, 210
Electronic Technology Center (ETC), 79, 192, 210
Electronic Wage Reporting (EWR), 40, 43, 46, 47, 116, 170, 210
E-mail, 29, 45, 83, 145, 146, 147, 159, 168, 197, 210
Enterprise Architecture (EA), 2, 3, 4, 10, 14, 17, 18, 19, 20, 22, 23, 24, 25, 27, 61, 68, 69, 77, 128, 129, 130, 139, 142, 144, 146, 150, 153, 156, 159, 161, 164, 170, 173, 177, 180, 183, 187, 188, 189, 190, 191, 195, 197, 199, 209, 210
Enterprise Information Technology Architecture (EITA), 10, 14, 17, 18, 19, 20, 22, 23, 24, 25, 68, 129, 130, 139, 142, 144, 146, 150, 153, 156, 159, 161, 164, 170, 173, 177, 180, 183, 189, 197, 210
Enterprise Server, 138, 139
Enterprise Software Engineering Facility (ESEF), 66, 161
Enumeration, 98, 100, 101, 133, 170, 210
Ethernet, 44, 83, 159, 183
Executive and Management Information System (EMIS), 127, 210
Extranet, 108
Federal Personnel/Payroll System (FPPS), 120, 210
Financial Accounting System (FACTS), 8, 43, 48, 121, 123, 210, 215
Financial Interactive Voice Response System (FIVR), 120, 210
Firewalls, 30, 79, 152, 154, 155, 159, 168, 171, 202, 203, 205
Frame Relay, 44, 159, 178, 180, 181, 182, 183
Fraud, 31, 114
General Services Administration (GSA), 30, 33, 54, 75, 114, 176, 177, 201, 202
Government Performance and Results Act (GPRA), 9, 211
Government-Developed off-the-shelf (GOTS), 119, 120, 122, 124, 211
Graduate-Level Training Program (GLTP), 90, 211
Graphical User Interface (GUI), 77, 84, 112, 211
Human Resources Management Information System (HRMIS), 120, 124, 211
Imaging and Document Management, 149, 150
Imaging and Document Management (IDM), 149, 150, 151, 211
Information Resource Management (IRM), 1, 2, 3, 4, 5, 6, 7, 8, 10, 13, 14, 17, 22, 24, 95, 110, 136, 186, 205, 211
Information Resources Management (IRM), 1, 2, 3, 4, 5, 6, 7, 8, 10, 13, 17, 22, 24, 95, 110, 136, 186, 211
Information Systems Plan (ISP), 6, 212
Information Technology Architecture (ITA), 3, 5, 6, 10, 14, 15, 17, 68, 76, 88, 129, 197, 210, 212
Information Technology Architecture Plan (ITAP), 6, 76, 212
Information Technology Infrastructure, 107, 108
Information Technology Management Reform Act (ITMRA), 68, 205, 212
Infrastructure, 2, 13, 17, 20, 21, 22, 23, 24, 25, 27, 28, 31, 32, 37, 43, 44, 45, 47, 51, 53, 54, 55, 71, 72, 73, 76, 77, 85, 87, 89, 107, 108, 113, 114, 117, 118, 127, 128, 130, 136, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 149, 150, 151, 152, 153, 155, 156, 157, 158, 159, 160, 161, 163, 164, 166, 170, 172, 173, 175, 177, 178, 179, 180, 181, 182, 183, 186, 187, 188, 189, 190, 191, 192, 194, 196, 197, 198, 199, 200, 209, 214
Integrated Database Management System (IDMS), 132, 133, 134, 135, 141, 211

Integrated Systems Architecture (ISA), 212
Intelligent Character Recognition (ICR), 211
Intelligent Workstations (IWS), 54, 84, 89, 127, 134, 139, 143, 212
Interactive Video Teletraining (IVT), 2, 43, 54, 179, 180, 181, 212
Inter-Agency Agreement (IAA), 75, 211
Internal Revenue Service (IRS), 46, 53, 100, 103, 112, 173, 212
Internet, 2, 4, 30, 33, 36, 39, 44, 46, 50, 55, 67, 72, 78, 79, 81, 84, 88, 90, 93, 103, 108, 109, 110, 112, 114, 115, 116, 135, 145, 146, 147, 152, 153, 155, 157, 159, 168, 169, 170, 171, 172, 173, 180, 183, 203, 211, 212, 216
Internet Project Life Cycle (I-PLC), 67, 211
Internet Protocol (IP), 30, 77, 79, 84, 123, 158, 159, 161, 177, 178, 180, 181, 183, 184, 203, 211, 216
Intranet, 22, 25, 33, 84, 108, 135, 136, 139, 146, 155, 156, 157, 169, 171, 172, 177, 183, 197
Joint Application Design (JAD), 69, 88, 212
Local Area Network (LAN), 30, 33, 54, 70, 71, 79, 82, 83, 84, 89, 117, 127, 134, 139, 143, 149, 150, 155, 158, 159, 164, 165, 172, 177, 203, 212, 215
Local Member Server, 138, 139
Local Shared Server, 138, 139
Mainframe, 31, 43, 66, 68, 71, 72, 77, 81, 83, 84, 87, 89, 90, 113, 117, 119, 120, 127, 133, 134, 135, 138, 139, 141, 153, 156, 160, 161, 162, 163, 164, 165, 167, 168, 169, 172, 173, 174, 183, 200, 202, 213
Mainframe Time and Attendance System (MTAS), 120, 213
Management Information (MI), 14, 22, 23, 48, 51, 52, 65, 66, 77, 94, 107, 108, 119, 120, 121, 122, 124, 125, 126, 127, 128, 131, 132, 133, 134, 156, 161, 164, 165, 178, 194, 210, 211, 213, 214
Management Information Architecture, 119, 121, 122, 124, 126, 127
Management Information Service Facility (MISF), 161, 213
Master Data Access Method (MADAM), 129, 131, 132, 133, 134, 135, 212
Multimedia, 84, 90, 180
National Computer Center (NCC), 32, 70, 71, 75, 76, 112, 136, 137, 139, 150, 151, 158, 161, 164, 172, 180, 182, 183, 202, 213
National Institute of Standards and Technology (NIST), 17, 30, 61, 202, 213
Network Management, 84, 213
Network Management Facility (NMF), 213
Office of Hearings and Appeals (OHA), 46, 48, 49, 104, 113, 117, 143, 144, 179, 180, 181, 183, 184, 213
Office of Management and Budget (OMB), 3, 7, 9, 17, 28, 30, 36, 48, 61, 68, 94, 121, 188, 197, 198, 199, 202, 213
Office of Systems (OS), 3, 4, 10, 15, 27, 65, 67, 68, 77, 79, 81, 82, 89, 90, 91, 92, 93, 95, 96, 115, 119, 120, 123, 132, 138, 139, 141, 142, 150, 157, 162, 172, 192, 194, 206, 214, 217
Official Union Time Tracking System (OUTTS), 120, 214
Online Analytical Process, 127, 213
Online Notice Retrieval System (ONRS), 162, 164, 165, 213
Online University, 155
Open Data Base Connectivity (ODBC), 134, 213
Operational Data Store (ODS), 124, 127, 213
Paperless Processing, 43, 51, 116, 150, 151
Payroll Management Information System (PMIS), 214
Performance Measures, 52
Postentitlement (PE), 35, 50, 51, 98, 104, 106, 112, 116, 118, 214
President's Management Agenda (PMA), 1, 3, 7, 8, 10, 13, 36, 45, 47, 52, 94, 119, 214
Print/Mail Facility, 164, 214
Private Branch Exchange (PBX), 176, 177, 178, 214
Production Processing Facility (PPF), 161, 214

Program Service Center (PSC), 51, 116, 117, 126, 143, 150, 161, 164, 176, 183, 204, 213, 214, 215
Programmatic Processing Facility (PPF), 161, 214
Programmatic Software Architecture, 109
Project Resource Guide (PRIDE), 64, 67, 69, 214
Public Key Infrastructure (PKI), 29, 30, 78, 114, 147, 167, 200, 201, 202, 205, 214
Purchase Card Requisition System (PCRS), 214
Quality Assurance (QA), 65, 84, 113, 214
Quality Control (QC), 65, 214
Rapid Application Development (RAD), 69, 214
Regional Operational Communications Center (ROCC), 140, 158, 172, 182, 183, 215
Relational Database Management System (RDBMS), 23, 132, 133, 134, 215
Remote Procedure Calls (RPC), 134, 215
Retirement, Survivors and Disability Insurance (RSDI), 35, 103, 104, 215
Security, 14, 27, 28, 29, 30, 31, 32, 44, 61, 68, 78, 84, 90, 113, 114, 159, 162, 166, 167, 168, 170, 171, 198, 199, 200, 202, 203, 204, 206, 207, 213, 214, 215, 216
Servers, 33, 55, 71, 72, 78, 79, 109, 127, 134, 135, 136, 138, 139, 140, 142, 146, 149, 152, 153, 154, 155, 156, 162, 168, 169, 172, 173, 189, 202, 203, 213, 215, 217
Service Delivery, 2, 3, 4, 5, 7, 9, 10, 39, 40, 49, 53, 68, 78, 109, 198, 210
Small Computer System Interface (SCSI), 172, 173, 174, 215
Social Security Number (SSN), 8, 42, 47, 53, 100, 101, 104, 153, 164, 165, 216
Social Security Online Accounting (SSOARS), 48, 119, 121, 123
Social Security Statement, 35, 103, 152, 153, 216
Software Engineering Facility (SEF), 66, 161, 215
Software Process Improvement (SPI), 35, 64, 66, 67, 69, 85, 215
SSA Chief Security Officer (SSACSO), 27, 68, 159, 206, 215
SSANETWORK (SSANet), 29, 143, 144, 146, 150, 152, 155, 159, 171, 179, 183, 204, 205, 215
Standards, 17, 30, 48, 127, 210, 213
State Online Query (SOLQ), 116, 215
Storage, 5, 23, 25, 43, 49, 51, 71, 75, 78, 111, 113, 117, 128, 131, 146, 150, 151, 161, 172, 173, 174, 183, 186, 189, 209, 215, 216
Storage Architecture, 44, 150, 151, 172, 186
Storage Area Network (SAN), 172, 173, 215
Storage Management, 51
Storage Media, 172
Strategic Plan, 1, 2, 3, 4, 6, 7, 8, 9, 10, 13, 15, 21, 22, 23, 24, 29, 36, 68, 76, 81, 91, 156, 165, 186, 190, 191, 208
Structured Query Language (SQL), 134, 135, 142, 156, 215
Supplemental Security Income (SSI), 2, 5, 35, 47, 49, 50, 100, 103, 104, 113, 115, 198, 216
Synchronous Optical Network (SONET), 183, 215
System Development Life Cycle (SDLC), 17, 20, 29, 135, 192, 208, 215
System Managed Storage (SMS), 140, 215
System Software Test Facility, 161
Systems Network Architecture (SNA), 161, 183, 215
Systems Rotational Program (SRP), 86, 215
Systems Technical Training Program (STTP), 87, 88, 89, 90, 216
Technology Infusion Board (TIB), 77
Technology Infusion Process (TIP), 77
Telecommunications, 2, 6, 23, 43, 44, 54, 72, 76, 90, 108, 130, 175, 183, 184, 199, 211, 214, 216
Teleservice Centers (TSC), 143, 183, 216
Third Party Payment System (TPPS), 48, 119, 123, 216
Title II, 43, 50, 51, 112, 115, 116, 118, 119, 124, 126, 127, 133, 153, 193

Title XVI, 50, 113, 116, 118, 119, 124, 126, 127, 133
Token Ring, 159
TOP SECRET, 31, 113, 167, 171, 201
Training Online Nomination System (TONS), 120, 216
Travel Manager (TM), 48, 123, 156, 182, 216
Uninterruptable Power Supply (UPS), 108, 216
Unix, 55
Video Teleconferencing, 44, 113, 117, 179, 180, 184, 216
Wide Area Network (WAN), 44, 70, 71, 84, 117, 158, 159, 177, 181, 182, 183, 216
Wilkes-Barre, 102, 176
Workload Management Systems (WMS), 125, 217
Workstation, 54, 55, 72, 79, 83, 89, 90, 117, 134, 140, 143, 144, 155, 157, 164, 198, 212, 217
www.socialsecurity.gov, 39, 72, 147, 152, 153