



Small Business Administration

**SBA Information Technology Infrastructure
Segment Architecture**

**Target State
(with Current State)**

Version 1.00

March 2009



Revision Sheet

Revision History/Change Log

IT Infrastructure Segment Architecture Target State

Version	Date	Description
1.00	03/31/2009	Published.

Table of Contents

1	Executive Summary	1
2	Scope of the Document	4
3	Target State Drivers	5
4	IT Infrastructure Target State Architecture	7
4.1	<i>Target State Performance Architecture</i>	7
4.2	<i>Target State Business Architecture</i>	24
4.3	<i>Target State Service Component Architecture</i>	28
4.4	<i>Target State Data Architecture</i>	36
4.5	<i>Target State Technology Architecture</i>	36
4.6	<i>Security</i>	49
4.7	<i>IPv6 Transition</i>	49
5	Appendix A: Acronyms	50
6	Appendix B: Segment Architecture Overview	52
6.1	<i>Use of Segment Architecture</i>	52
6.2	<i>Ownership</i>	52
6.3	<i>Stages of Segment Architecture Process</i>	52
7	Appendix C: Organization and Stakeholders	54
8	Appendix D: SBA Goals and Objectives	57
9	Appendix E: Key Business Drivers	58
10	Appendix F: External Directives	59
11	Appendix G: Prioritized Opportunities	60
12	Appendix H: Current State Business Architecture	69
12.1	<i>Performance Analysis Summary</i>	69
12.2	<i>Operational Business Architecture</i>	70
12.3	<i>IT Infrastructure Current Investments</i>	82
12.4	<i>Business Architecture Key Observations</i>	83
13	Appendix I: Current State System Architecture	85
13.1	<i>Current State Service Component Architecture</i>	85
13.2	<i>Current State Data Architecture</i>	88
13.3	<i>Current State Technical Architecture</i>	89
14	Appendix J: Documents Reviewed	102

Table of Exhibits

FIGURE 1: CREATION OF TARGET SEGMENT ARCHITECTURE	5
FIGURE 2: FEDERAL ENTERPRISE ARCHITECTURE (FEA) FRAMEWORK	6
FIGURE 3: CORE BRM ALIGNMENT	24
FIGURE 4: TARGET STATE OPERATIONAL BUSINESS ARCHITECTURE	26
FIGURE 5: TARGET STATE SERVICE COMPONENT ARCHITECTURE	29
FIGURE 6: SBA TARGET STATE NETWORK INFRASTRUCTURE	43
FIGURE 7: SBA TARGET STATE DATA CENTERS AND NETWORK INFRASTRUCTURE	45
FIGURE 8: PIV SERVICES LEVERAGING SBA NETWORK INFRASTRUCTURE	47
FIGURE 9: SOA CONCEPTUAL PLATFORM	48
FIGURE 10: SEGMENT ARCHITECTURE PROCESS	53
FIGURE 11: OCIO ORGANIZATION (IT INFRASTRUCTURE HIGHLIGHTED).....	54
FIGURE 12: IT INFRASTRUCTURE OPERATIONAL BUSINESS ARCHITECTURE.....	70
FIGURE 13: SBA CURRENT STATE NETWORK INFRASTRUCTURE.....	95
FIGURE 14: PIV SERVICES LEVERAGING SBA NETWORK INFRASTRUCTURE	98
FIGURE 15: SBA DATA CENTERS AND NETWORK INFRASTRUCTURE.....	100
TABLE 1: TARGET STATE IMPLICATIONS ON CURRENT STATE OBSERVATIONS.....	2
TABLE 2: TARGET STATE DRIVERS.....	5
TABLE 3: RELEVANT SBA GOALS AND OBJECTIVES	7
TABLE 4: OCIO GOALS.....	8
TABLE 5: STRATEGIC PERFORMANCE METRICS	10
TABLE 6: SEGMENT PERFORMANCE METRICS – EUSS.....	11
TABLE 7: SEGMENT PERFORMANCE METRICS - MSSS	11
TABLE 8: SEGMENT PERFORMANCE METRICS - TSS	12
TABLE 9: CROSS-SEGMENT PERFORMANCE METRICS.....	13
TABLE 10: INFRASTRUCTURE SEGMENT PERFORMANCE METRICS.....	14
TABLE 11: BUSINESS PERFORMANCE METRICS - EUSS	15
TABLE 12: BUSINESS PERFORMANCE METRICS - MSSS	17
TABLE 13: BUSINESS PERFORMANCE METRICS - TSS.....	22
TABLE 14: OPERATIONAL PROCESSES TO METRICS MAPPING	27
TABLE 15: NEW SERVICE COMPONENTS MAPPING TO BUSINESS FUNCTIONS	29
TABLE 16: TARGET STATE SERVICE COMPONENTS.....	32
TABLE 17: MAP OF SERVICE COMPONENTS (SRM) WITH THE TECHNOLOGY COMPONENTS.....	37
TABLE 18: MAP OF THE TECHNOLOGY COMPONENTS WITH THE TRM.....	39
TABLE 19: LIST OF ACRONYMS	50
TABLE 20: OCIO INTERVIEW LIST.....	55
TABLE 21: SBA STRATEGIC GOALS.....	57
TABLE 22: PRIORITIZED OPPORTUNITIES.....	61
TABLE 23: OPPORTUNITY DETAILS.....	63
TABLE 24: SERVICE LEVEL MANAGEMENT.....	71
TABLE 25: CAPACITY MANAGEMENT.....	71
TABLE 26: AVAILABILITY MANAGEMENT	71
TABLE 27: IT SERVICE CONTINUITY MANAGEMENT	72
TABLE 28: INFORMATION SECURITY MANAGEMENT	72
TABLE 29: IT ARCHITECTURE MANAGEMENT	73
TABLE 30: SUPPLIER MANAGEMENT	73
TABLE 31: SERVICE PORTFOLIO MANAGEMENT.....	73
TABLE 32: IT FINANCIAL AND PERFORMANCE MANAGEMENT	74
TABLE 33: CHANGE MANAGEMENT	74
TABLE 34: CONFIGURATION MANAGEMENT.....	75
TABLE 35: TRANSITION PLANNING AND SUPPORT	75
TABLE 36: SERVICE VALIDATION AND TESTING	76

TABLE 37: RELEASE MANAGEMENT	76
TABLE 38: SERVICE DESK	77
TABLE 39: EVENT MANAGEMENT	77
TABLE 40: INCIDENT MANAGEMENT	78
TABLE 41: REQUEST FULFILLMENT	78
TABLE 42: ACCESS MANAGEMENT	79
TABLE 43: PROBLEM MANAGEMENT	79
TABLE 44: IT OPERATIONS MANAGEMENT	80
TABLE 45: IT FACILITIES MANAGEMENT	80
TABLE 46: BUSINESS PROCESS TO BUSINESS SERVICE MAPPING	81
TABLE 47: OCIO INFRASTRUCTURE CURRENT INVESTMENTS	82
TABLE 48: MAPPING OF BUSINESS FUNCTIONS TO SERVICE COMPONENTS AND SRM ALIGNMENT	85
TABLE 49: MAP OF SERVICE COMPONENTS (SRM) WITH THE TECHNOLOGY COMPONENTS	90
TABLE 50: MAP OF THE TECHNOLOGY COMPONENTS WITH THE TRM	91
TABLE 51: TIC CONNECTIONS	96

1 Executive Summary

As part of its long term planning process, the Small Business Administration (SBA) is creating an IT Infrastructure Segment Architecture in accordance with the Federal Enterprise Architecture (FEA) guidance and in conjunction with Office of Management and Budget's (OMB) IT Infrastructure Optimization Line of Business (ITILOB). The ITILOB's guidance emphasizes operational improvements gained from service component reuse, cost avoidance, elimination of redundancy, and collaboration. These goals are supported by recommendations in this Target State segment architecture document. Additionally, key changes between existing operational business processes and potential improvements are analyzed.

The SBA's Office of the Chief Information Officer (OCIO) manages the information technology services and support that enable the Agency's mission, including the information technology infrastructure.

SBA's IT infrastructure is made up of the following components, as defined by the ITILOB:

- End User Services and Support (EUSS);
- Mainframe and Server Services and Support (MSSS); and
- Telecommunications Services and Support (TSS).

In addition, this segment architecture will explore the component of Enterprise Application Support Services (EASS) as it relates to service oriented architecture (SOA) and the IT infrastructure.

The segment architecture process develops an institutional understanding of the current operational state of the IT Infrastructure segment, promotes performance by identifying improvement opportunities, and produces an actionable roadmap to realize these opportunities. Input from stakeholders, the OCIO staff, forms the foundation for all recommendations, filtered through ITILOB guidance. This document conveys the resulting vision of a target state segment architecture at all architectural layers (i.e., performance architecture, business architecture, service component architecture, and technical architecture).

The specific opportunities for improvement uncovered through the segment architecture process can be categorized into the following broad categories:

- **Performance Management** – continual collection and monitoring of performance metrics will enable continual improvement within SBA's IT infrastructure and better tracking of service levels provided to customers and by vendors.
- **Process Improvement** – the adoption of standard IT infrastructure library (ITIL) processes across the OCIO will improve effectiveness and efficiency throughout the IT infrastructure.
- **Data Center and Disaster Recovery** – the implementation of a next generation data center will position SBA's IT infrastructure to be secure, flexible, and modernized. It will provide necessary disaster recovery capabilities and position SBA to move towards Green IT initiatives.
- **Compliance with Federal Initiatives** – by working to achieve compliance with federal IT infrastructure initiatives, including Homeland Security Presidential Directive 12 (HSPD-12), Internet Protocol version 6 (IPv6), Trusted Internet Connection (TIC), Federal Desktop Core Configuration (FDCC), and the switch to the General Services Administration (GSA) Network contract, SBA will ensure that its infrastructure is optimized and interoperable with other federal agencies and ready to support government-wide solutions. It will also promote collaboration and resource sharing across the government.
- **SOA Preparation** – an SOA approach to delivering solutions will help achieve business flexibility and cost savings through the identification and reuse of common services.

Proper planning and continual governance for SOA will help sure ensure successful delivery.

- **Network Optimization** – efforts to proactively plan, analyze, and modernize the network infrastructure will help ensure a robust and scalable infrastructure to support the network bandwidth needs of the Agency.

Achieving the opportunities for improvement across these categories will address the issues raised by the IT Infrastructure current state segment architecture and position SBA to improve the ability of the IT Infrastructure to deliver the Agency’s strategic mission and goals. SBA will also be much better positioned to participate in and leverage the opportunities to come from the ITILOB efforts. Table 1 shows the recommendations and their implications.

TABLE 1: TARGET STATE IMPLICATIONS ON CURRENT STATE OBSERVATIONS

Current State	Target State Vision
<p>Metrics – comprehensive process-based performance metrics (especially LOB metrics) are not routinely tracked and reported across OCIO.</p>	<p>The IT infrastructure is managed by a process-oriented organization where a comprehensive list of performance metrics is defined, managed, tracked and used by OCIO.</p> <p>All ITILOB metrics are comparable to industry standards.</p>
<p>Processes - several infrastructure design, deployment, and management processes are immature, informal, or missing.</p>	<p>Standard ITIL process names are adopted throughout OCIO, and existing work is categorized according to these industry-standard terms.</p>
<p>Reuse – there is minimal redundancy/reuse, especially between OCIO and ODA (in part due to Congressional mandates on ODA appropriation). Minimal documentation of existing reuse instances exists. No clearinghouse of available services exists.</p>	<p>Duplicate operational business processes and service components are consolidated (where feasible and authorized). Common service components are shared.</p>
<p>Service Level Agreements (SLA)/ Operational Level Agreements (OLA) – few formal SLAs or OLAs exist</p>	<p>Robust OLAs and SLAs enable improved customer service, internal operations, and vendor management.</p>
<p>Data Center – there is a need for a robust, “next generation” data center.</p>	<p>SBA has a next generation data center, with all capacity, continuity, environmental, and security requirements met.</p>

Current State	Target State Vision
<p>Disaster Recovery –necessary redundancy is missing for some key applications, such as e-Tran and ODA e-mail.</p>	<p>The remote disaster recovery infrastructure is fully enabled, in coordination with Data Center.</p>
<p>Network – no significant problems, but network upgrades do not have a long-term planning horizon, and overall health is hard to know at any given time.</p>	<p>There is a complete, ongoing understanding of network health – and all areas are upgraded based on bandwidth need.</p>
<p>Networx - must shift to new contract.</p>	<p>Using Networx for unified communications.</p>
<p>TIC – too many Internet connections per TIC guidance.</p>	<p>Compliant with TIC.</p>
<p>IPv6 – the hardware is installed and a limited test was successful, but the applications have not been tested. IPv6 not in wide use by vendors.</p>	<p>Fully IPv6 enabled.</p>
<p>HSPD-12 – no PKI, no widespread use of PIV cards for logical access.</p>	<p>Agency-wide PIV card enabled logical access.</p>
<p>SOA - no formal SOA infrastructure or processes exist.</p>	<p>Fully SOA enabled. Regular reuse of service components.</p>

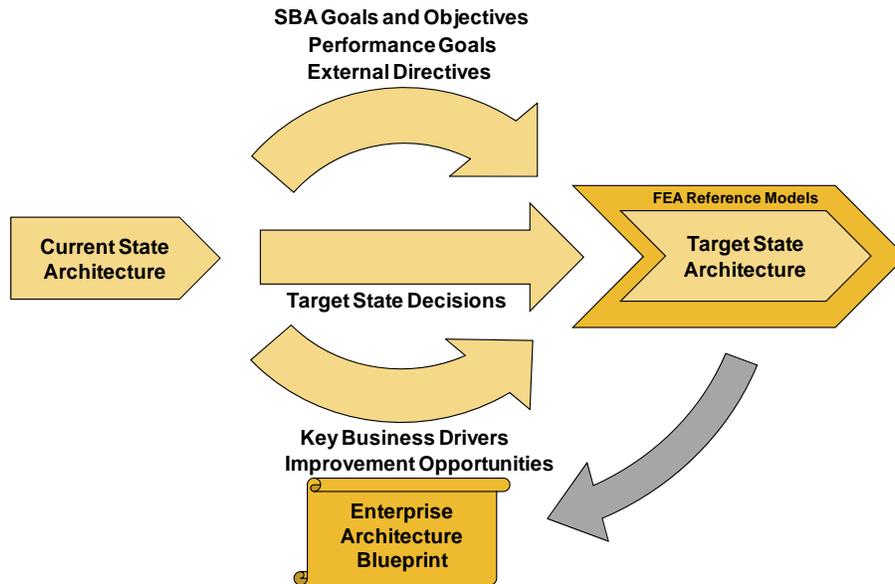
2 Scope of the Document

This document provides the target state architecture at all levels (i.e., performance, business, service component, and technical) for the SBA IT Infrastructure segment by identifying the program mission, goals, objectives, and performance metrics and targets. It also includes target state descriptions and high-level model architectures for the IT Infrastructure business operations, service components, and technology.

3 Target State Drivers

The target state architecture is a blueprint of the vision for future business operations and supporting technology. It describes the desired capability and structure of business processes, information needs, and IT services for the future.

FIGURE 1: CREATION OF TARGET SEGMENT ARCHITECTURE



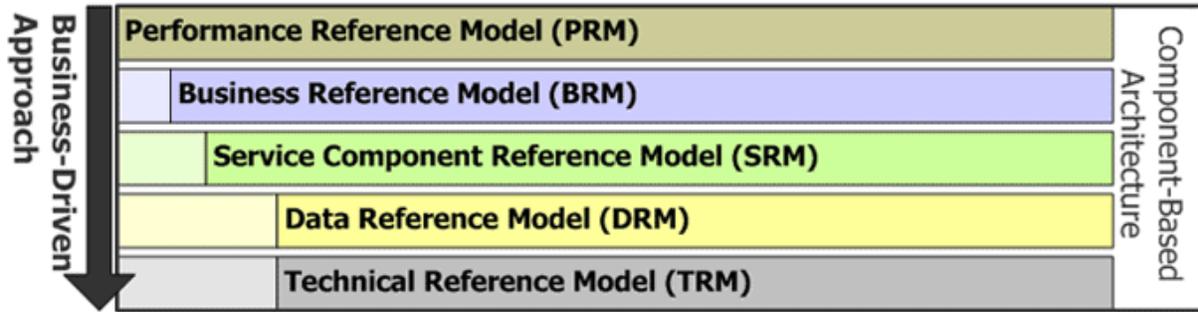
As illustrated in Figure 1, the agency goals and objectives, performance goals, external directives and mandates, key business drivers, improvement opportunities, and enterprise architecture standards are applied to the current state architecture models to set the constraints of the target state architecture. Decisions made within those constraints guide the final target state definition. The completed target state also informs the agency's enterprise architecture blueprint. Each of these drivers is discussed at greater length in the following sections:

TABLE 2: TARGET STATE DRIVERS

Target State Driver	Location
SBA Goals and Objectives	Appendix D: SBA Goals and Objectives
Performance Goals	Section 4.1 Target State Performance Architecture
Key Business Drivers	Appendix E: Key Business Drivers
External Directives	Appendix F: External Directives
Improvement Opportunities	Appendix G: Prioritized Opportunities
Enterprise Architecture Blueprint	<i>SBA EA Blueprint v2.03</i> (external document)

The target state is described using the FEA reference framework and the performance, business, data, service component, and technical architectures are defined using the elements of FEA.

FIGURE 2: FEDERAL ENTERPRISE ARCHITECTURE (FEA) FRAMEWORK



4 IT Infrastructure Target State Architecture

4.1 Target State Performance Architecture

The overarching theme behind the FEA is that performance measurement drives operation, which in turn drives IT investment. The starting point for designing a target state segment architecture is the performance model and the performance gaps that exist. Examining the mission and vision relevant to the segment drives understanding of the performance model. Realization of the vision and accomplishment of the mission is broken down into goals and objectives. Success of the organization in achieving these objectives is measured through performance indicators. The OCIO's performance model starts with SBA-wide goals and narrows to specific measurements found in ITILOB documents and OCIO budgets.

4.1.1 SBA Goals

The 2008 SBA Strategic Plan outlines the Agency's core values and four broad goals, each with long-term objectives. In general, the OCIO supports the entire Agency with technology that enables all work performed, but specific goals are particularly relevant to OCIO, as shown in Table 3.

TABLE 3: RELEVANT SBA GOALS AND OBJECTIVES

Goal #	Goal	LTO #	Long Term Objective
4	Ensure management and organizational excellence to increase responsiveness to customers, streamline processes, and improve compliance and controls	4.2	Provide a safe and secure information system environment to support business decisions and Agency operations
		4.3	Provide financial and performance management services to support efficient and effective program delivery

4.1.2 Mission

The OCIO's mission is to:

Foster an environment in which information and technology are used to support and enhance business decisions and Agency operations.

4.1.3 Strategic IT Goals and Long Term Objectives

The OCIO has its own goals that support the overall SBA goals, as indicated in the SBA IT Strategic Plan. Table 4 shows the OCIO's goals, with those most relevant to IT Infrastructure in bold print.

TABLE 4: OCIO GOALS

No.	Goal	Long Term Objective	SBA LTO#
1	Business and IT Strategic Alignment	1.1 Alignment via coordinated business and IT planning	4.2
2	The Right Technology Solutions, Infrastructure, and Architecture	2.1 Improve service delivery through enterprise-wide automation, web enablement, and system upgrades	4.2
		2.2 Enable employees through enterprise-wide automation, web enablement and system upgrades	4.2
		2.3 Improve IT Infrastructure	4.2
		2.4 Improve data integrity and provide an authoritative access point for data	4.2
		2.5 Promote internal and external collaboration	4.2
		2.6 Exploit the benefits of EA	4.2
		2.7 Realize the benefits of eGovernment	4.2
		2.8 Improve IT security and privacy	4.2
3	A Skilled and Knowledgeable IT Workforce	3.1 Provide excellent technical support	4.2
		3.2 Develop the IT workforce	4.2
		3.3 Improve the IT organization	4.2
4	Effective and Efficient Management of IT Resources and Operations	4.1 Enable proactive performance management (including advanced analytics)	4.2
		4.2 Continue to improve the Agency's capital planning and IT governance processes	4.2

4.1.4 Performance Indicators

Performance metrics are the practical realization of goals and objectives. The tables below show the current IT Infrastructure performance metrics as well as future performance metrics and those with the potential to be retired. OCIO reports current metrics on the PAR, Exhibit 300s, and internal scorecards. Future performance metrics may be assigned to any of these reports. Per OMB guidance, metrics are categorized as follows:

- **Strategic Performance** measures how the IT Infrastructure segment supports the strategic goals of SBA. These metrics come from the PAR.
- **Segment Performance** measures the success the IT infrastructure has within SBA. The source of these metrics is the benchmarks outlined by the IT Infrastructure Optimization Line of Business and included in the “SBA Consolidated 5 Year Plan Optimization Report.”
- **Business Performance** measures how the performance of technology and processes affect the infrastructure business outcomes, per OMB guidance for the segment architecture. The sources of these metrics are provided by the program offices.

The following tables illustrate existing/continuing metrics and new metrics, as well as those recommended for retirement. The metrics are distinguished by

- Existing/Continuing in plain text
- **New in bold text**
- *Retired in italic text.*

Note: Some of the existing/continuing business performance metrics in the tables below are designated with an “N/A” in the “Actual” column. This is due to 2007 being the baseline year for these metrics.



TABLE 5: STRATEGIC PERFORMANCE METRICS ¹

Metric ID	PAR Metric	Fiscal Year	Office	Agency Code	Strategic Goal	Target	Actual	Achieved
PAR-1	IT Systems Availability	2008	OCIO	028-00	Ensure management and organizational excellence to increase responsiveness to customers, streamline processes, and improve compliance and controls	99.6%	99.8%	Yes
PAR-2	Unauthorized Network or Data Breaches	2008	OCIO /OIS	028-00	Ensure management and organizational excellence to increase responsiveness to customers, streamline processes, and improve compliance and controls	0	4	No

¹ Source: SBA Performance and Accountability Report (FY07)

TABLE 6: SEGMENT PERFORMANCE METRICS – EUSS²

Metric ID	Fiscal Year	Metric	ITI LOB Benchmark	Actual
SP-EUSS-1	2008	Cost per user	\$2,369- \$1,313	\$1,407
SP-EUSS-2	2008	Cost per primary device	\$2,369- \$1,853	\$1,149
SP-EUSS-4	2008	Restoration for mission critical, <=4 hrs	95%	0%
SP-EUSS-5	2008	Restoration for high priority, <=8 hrs	95%	0%
SP-EUSS-6	2008	Restoration for medium priority, <=next business day	90%	100%
SP-EUSS-7	2008	Restoration for low priority, <=second business day	90%	0%
SP-EUSS-8	2008	Cost per Help Desk handle contact	\$28.76- \$21.98	\$31.39
SP-EUSS-10	2008	Help Desk first contact resolution percentage	75%	70%
SP-EUSS-11	2008	Help Desk speed of answer percentage	90%	55%
SP-EUSS-12	2008	Total cost per user	\$3,029- \$2,405	\$ 1,949

TABLE 7: SEGMENT PERFORMANCE METRICS - MSSS³

Metric ID	Fiscal Year	Metric	ITI LOB Benchmark	Actual
-----------	-------------	--------	-------------------	--------

2 Source: Gartner ITILOB Report – SBA Data Analysis (EUSS section)

3 Source: Gartner ITILOB Report – SBA Data Analysis (MSSS section)

Metric ID	Fiscal Year	Metric	ITI LOB Benchmark	Actual
	2008	Mainframe cost per MIPS	\$9,989- \$6,704	\$5,161
	2008	Mainframe availability percentage	99.99%	99.99%
SP-MSSS-1	2008	Wintel cost per server	\$20,074- \$15,488	\$10,184
SP-MSSS-2	2008	Wintel server availability	99.78%	99.99%
SP-MSSS-3	2008	UNIX cost per server	\$70,249- \$39,524	\$575,037
SP-MSSS-4	2008	UNIX server availability percentage	99.9%	99.99%
SP-MSSS-5	2008	Linux cost per server	N/A	N/A
SP-MSSS-6	2008	Linux server availability percentage	N/A	N/A

TABLE 8: SEGMENT PERFORMANCE METRICS - TSS⁴

Metric ID	Fiscal Year	Metric	ITI LOB Benchmark	Actual
SP-TSS-1	2008	Wide area data network cost per device	\$448-\$391	\$925
SP-TSS-2	2008	Wide area data network availability	99.9%	99.9%
SP-TSS-3	2008	Metropolitan area network cost per gigabyte	N/A	N/A
SP-TSS-4	2008	Metropolitan area network availability	N/A	N/A

⁴ Source: Gartner ITILOB Report – SBA Data Analysis (TSS section)

Metric ID	Fiscal Year	Metric	ITI LOB Benchmark	Actual
SP-TSS-5	2008	Local area network cost per active port	\$234-\$203	\$676
SP-TSS-6	2008	Local area network availability percentage	99.9%	99.9%
SP-TSS-7	2008	Internet access cost per gigabyte	\$10.64-\$6.30	\$11.66
SP-TSS-8	2008	Internet access network availability percentage	99.9%	99.9%
SP-TSS-9	2008	Long distance telephony cost per minute	\$.067-\$.057	\$.45
SP-TSS-10	2008	Long distance telephony availability percentage	99.99%	99.99%
SP-TSS-11	2008	Cellular calling cost per minute	\$.095-\$.065	\$.22
SP-TSS-12	2008	Local telephony cost per extension	\$440-\$355	\$743
SP-TSS-13	2008	Local telephony availability percentage	99.99%	99.99%
SP-TSS-14	2008	Video conference cost per minute	\$8.11-\$4.87	\$.61

TABLE 9: CROSS-SEGMENT PERFORMANCE METRICS

Metric ID	Fiscal Year	Metric	Target	Actual
XSP-1	2011	Percentage of infrastructure performance-based contracts	100%	
XSP-2	2011	Number of completed segments	10	
XSP-3	2011	Percentage of SBA OCIO staff (employees and contractors) with PIV credentials	100%	

TABLE 10: INFRASTRUCTURE SEGMENT PERFORMANCE METRICS

Metric ID	Fiscal Year	Metric	Target	Actual
ISP-1	2011	Percentage of reused services	TBD, need baseline	
ISP-2	2011	Number of services documented in the service catalog/registry	TBD need baseline	
ISP-3	2011	Number of applications/systems gone through an SOA health check	TBD, need baseline	



TABLE 11: BUSINESS PERFORMANCE METRICS - EUSS⁵

Metric ID	Fiscal Year	Metric Type	Measurement Indicator	IT Investment Name	System/ App/ Program	Strategic Goal	Line of Business or Service Type	Sub-Function or Service Component	Agency Business Process	Target	Actual
MB-04-01-02-08.1	2008	Output Metric	Percent of tickets closed by in-house clerks	OCIO: IT Infrastructure End User Systems & Support	Help Desk & LAN Support	4	Administrative Management	Help Desk Services	Service Desk	90%	N/A
	<i>2008</i>	<i>Output Metric</i>	<i>Percent answered in less than 15 minutes</i>	<i>OCIO: IT Infrastructure End User Systems & Support</i>	<i>Help Desk & LAN Support</i>	<i>4</i>	<i>Administrative Management</i>	<i>Help Desk Services</i>	<i>Service Desk</i>	<i>80% of priority 1 calls answered in less than 15 minutes</i>	<i>N/A</i>

⁵ Source (2008 Fiscal year): SBA Exhibit 300s (FY10, EUSS Section)



Metric ID	Fiscal Year	Metric Type	Measurement Indicator	IT Investment Name	System/ App/ Program	Strategic Goal	Line of Business or Service Type	Sub-Function or Service Component	Agency Business Process	Target	Actual
	2008	Output Metric	Percent of calls resolved on first attempt	OCIO: IT Infrastructure End User Systems & Support	Help Desk & LAN Support	4	Administrative Management	Help Desk Services	Service Desk	80%	N/A
	2008	Output Metric	Average number of complaints per month per 100 users	OCIO: IT Infrastructure End User Systems & Support	Help Desk & LAN Support	4	Administrative Management	Help Desk Services	Service Desk	2	N/A



TABLE 12: BUSINESS PERFORMANCE METRICS - MSSS⁶

Metric ID	Fiscal Year	Metric Type	Measurement Indicator	IT Investment Name	System/ App/ Program	Strategic Goal	Line of Business or Service Type	Sub-Function or Service Component	Agency Business Process	Target	Actual
	2008	Output Metric	Minutes of downtime per month	OCIO: IT Infrastructure Mainframe & Server Systems & Support	Mainframe & Server Operations	4	Internal Risk Management and Mitigation	Continuity of Operations	Availability Management	120 Maximum	15
	2008	Input Metric	Mainframe and servers will be available for use 99% of the time, excluding periods of scheduled maintenance	OCIO: IT Infrastructure Mainframe & Server Systems & Support	Mainframe & Server Operations	4	Information and Technology Management	IT Infrastructure Maintenance	Availability Management	100% current	N/A

⁶ Source (2008 Fiscal Year): SBA Exhibit 300s (FY10, MSSS Section)



Metric ID	Fiscal Year	Metric Type	Measurement Indicator	IT Investment Name	System/ App/ Program	Strategic Goal	Line of Business or Service Type	Sub-Function or Service Component	Agency Business Process	Target	Actual
			e								
MB-04-04-05-08.1	2008	Output Metric	Timeliness of backups	OCIO: IT Infrastructure Mainframe & Server Systems & Support	Mainframe & Server Operations	4	Internal Risk Management and Mitigation	Continuity of Operations	Availability Management	95%	100%
MB-04-04-05-08.2	2008	Input Metric	IT Security recommended patches	OCIO: IT Infrastructure Mainframe & Server Systems & Support	Information Security	4	Information and Technology Management	Information Security	Information Security Management	Apply 90% of recommended patches by IT security within 72 hours	N/A



Metric ID	Fiscal Year	Metric Type	Measurement Indicator	IT Investment Name	System/App/Program	Strategic Goal	Line of Business or Service Type	Sub-Function or Service Component	Agency Business Process	Target	Actual
	2008	Output Metric	Complaint responses	OCIO: IT Infrastructure Mainframe & Server Systems & Support	Mainframe & Server Operations	4	Administrative Management	Help Desk Services	Service Desk	Respond to 95% of complaints within 24 hours 100% of the time	N/A
	2008	Output Metric	Server uptime	OCIO: IT Infrastructure Mainframe & Server Systems & Support	Mainframe & Server Operations	4	Internal Risk Management and Mitigation	Continuity of Operations	Availability Management	99% available	N/A
MB-04-04-05-08.3	2008	Output Metric	Timeliness of root cause analysis of outages	OCIO: IT Infrastructure Mainframe & Server Systems & Support	Mainframe & Server Operations	4	Internal Risk Management and Mitigation	Service Recovery	IT Service Continuity Management	48 hours after resolution	24 hours



Metric ID	Fiscal Year	Metric Type	Measurement Indicator	IT Investment Name	System/ App/ Program	Strategic Goal	Line of Business or Service Type	Sub-Function or Service Component	Agency Business Process	Target	Actual
MB-04-04-05-08.4	2008	Output Metric	Load test for concurrent system users	OCIO: IT Infrastructure Mainframe & Server Systems & Support	Mainframe & Server Operations	4	Information and Technology Management	IT Infrastructure Maintenance	Capacity Management	8,000	12,194
MB-04-04-05-11.5	2011	Output Metric	Power usage effectiveness (PUE)	OCIO: IT Infrastructure Mainframe & Server Systems & Support	Mainframe & Server Operations	4	Information and Technology Management	IT Infrastructure Maintenance	Availability Management	Need baseline < 2 by 2013	N/A
MB-04-04-05-11.6	2011	Output Metric	Carbon footprint	OCIO: IT Infrastructure Mainframe & Server Systems & Support	Mainframe & Server Operations	4	Administrative Management	Facilities, Fleet, and Equipment Management	Availability Management	Need baseline 25% reduction by 2013	N/A



Metric ID	Fiscal Year	Metric Type	Measurement Indicator	IT Investment Name	System/App/Program	Strategic Goal	Line of Business or Service Type	Sub-Function or Service Component	Agency Business Process	Target	Actual
MB-04-04-05-11.7	2011	Output Metric	Percentage of standard (pre-approved/defined) changes	OCIO: IT Infrastructure Mainframe & Server Systems & Support	Mainframe & Server Operations	4	Information and Technology Management	Lifecycle / Change Management	Change Management	100%	N/A
MB-04-04-05-11.8	2011	Output Metric	Percentage of SLAs met	OCIO: IT Infrastructure End User Systems & Support	Help Desk & LAN Support	4	Customer Relationship Management	Call Center Management	Service Desk	Need baseline Increasing	N/A
MB-04-04-05-11.9	2011	Output Metric	Number of internal applications with customer service level agreements	OCIO: IT Infrastructure End User Systems & Support	Help Desk & LAN Support	4	Customer Relationship Management	Call Center Management	Service Desk	Need baseline Increasing	N/A



TABLE 13: BUSINESS PERFORMANCE METRICS - TSS⁷

Metric ID	Fiscal Year	Metric Type	Measurement Indicator	IT Investment Name	System/ App/ Program	Strategic Goal	Line of Business or Service Type	Sub-Function or Service Component	Agency Business Process	Target	Actual
MB-04-04-04-08.1	2008	Input Metric	Percent of HQ SBA employees served by Telecom	OCIO: IT Infrastructure Telecommunications Systems & Support	Communications Technology Services	4	Information and Technology Management	IT Infrastructure Maintenance	IT Operations Management	99.99%	N/A
MB-04-04-04-08.2	2008	Input Metric	Percent of network infrastructure up to date	OCIO: IT Infrastructure Telecommunications Systems & Support	Communications Technology Services	4	Information and Technology Management	IT Infrastructure Maintenance	Service Asset and Configuration Management	100%	N/A

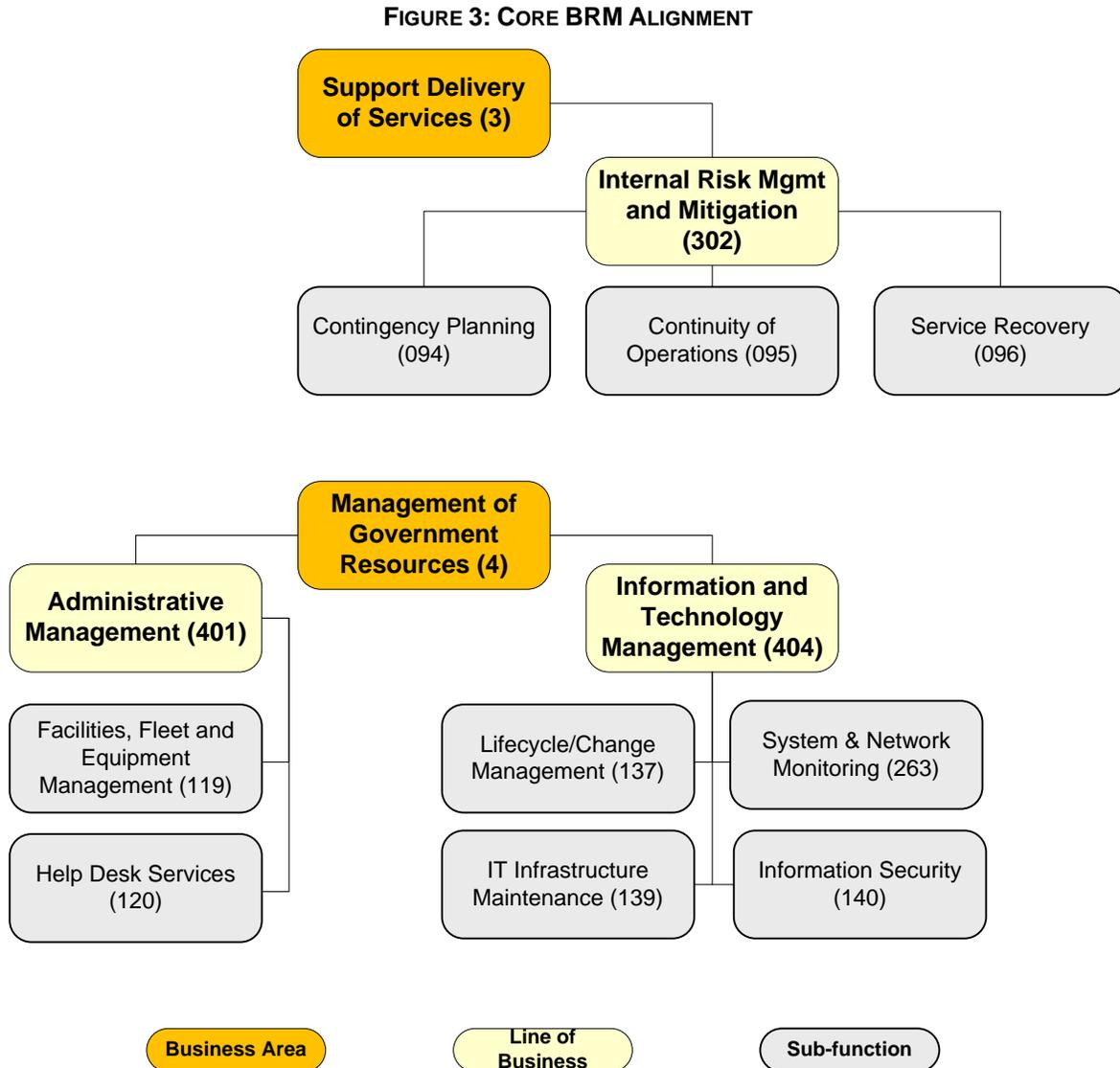
⁷ Source (2008 Fiscal Year): SBA Exhibit 300s (FY10, TSS Section)



Metric ID	Fiscal Year	Metric Type	Measurement Indicator	IT Investment Name	System/ App/ Program	Strategic Goal	Line of Business or Service Type	Sub-Function or Service Component	Agency Business Process	Target	Actual
MB-04-04-04-08.3	2008	Input Metric	Percent of hardware updated annually	OCIO: IT Infrastructure Telecommunications Systems & Support	Communications Technology Services	4	Information and Technology Management	IT Infrastructure Maintenance	Service Asset and Configuration Management	25% refresh per year	N/A
	2008	Input Metric	Infrastructure downtime	OCIO: IT Infrastructure Telecommunications Systems & Support	Communications Technology Services	4	Internal Risk Management and Mitigation	Continuity of Operations	Availability Management	99% availability	N/A

4.2 Target State Business Architecture

The Target State Infrastructure Business Reference Model (BRM) categorizes a segment's functions in terms of day-to-day operations. The target state functions are shown in Figure 3. The business architecture is unchanged from the current state.



Per the *FEA Consolidated Reference Model Document Version 2.3*, October 2007, the business services shown above (highlighted in gray) are defined as follows:

- **(3) Support Delivery of Services** provides the critical policy, programmatic and managerial foundation to support federal government operations.
 - **(302) Internal Risk Management and Mitigation** involves all activities relating to the processes of analyzing exposure to risk and determining appropriate countermeasures.
 1. **(094) Contingency Planning** involves the actions required to plan for, respond to, and mitigate damaging events.

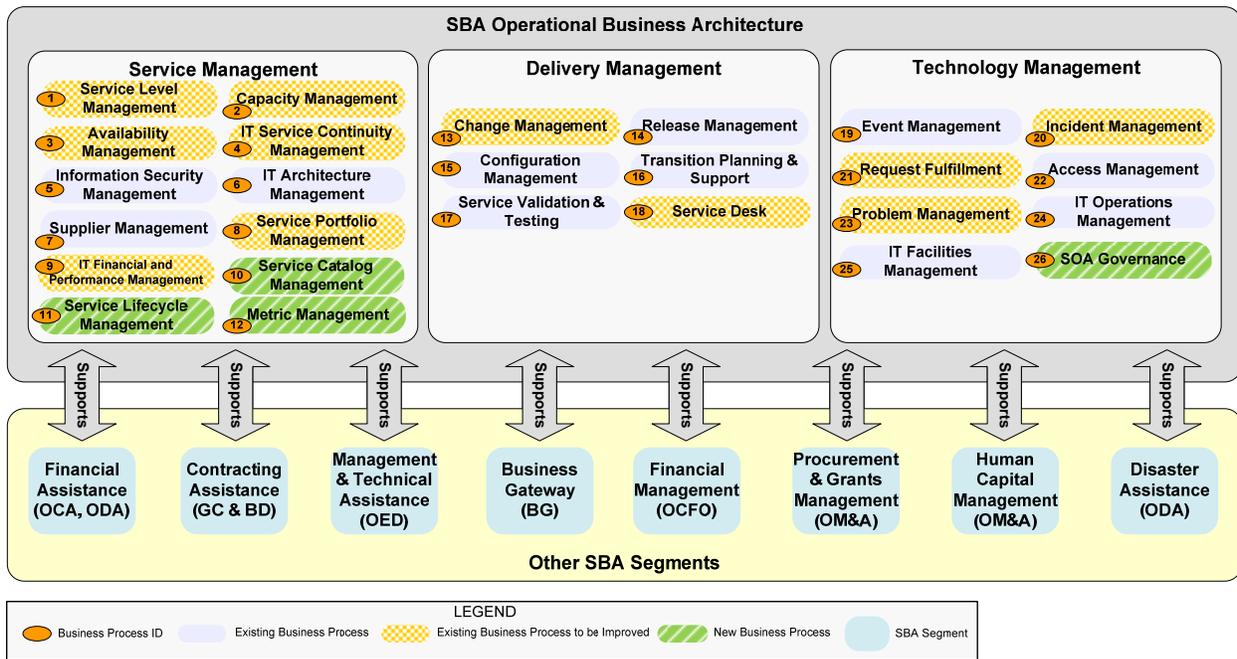
2. **(095) Continuity of Operations** involves the activities associated with the identification of critical systems and processes, and the planning and preparation required to ensure that these systems and processes will be available in the event of a catastrophic event.
 3. **(096) Service Recovery** involves the internal actions necessary to develop a plan for resuming operations after a catastrophic event occurs.
- **(4) Management of Government Resources** refers to the support activities that enable the government to operate efficiently
 - **(401) Administrative Management** involves the day-to-day management and maintenance of the internal infrastructure.
 1. **(119) Facilities, Fleet, and Equipment Management** involves the maintenance, administration, certification, and operation of office buildings, fleets, machinery, and other capital assets that are possessions of the federal government.
 2. **(120) Help Desk Services** involve the management of a service center to respond to government and contract employees' technical and administrative questions.
 - **(404) Information and Technology Management** involves the coordination of information and technology resources and systems required to support or provide a service.
 1. **(137) Lifecycle/Change Management** involves the processes that facilitate a smooth evolution, composition, and workforce transition of the design and implementation of changes to agency resources such as assets, methodologies, systems, or procedures.
 2. **(139) IT Infrastructure Maintenance** involves the planning, design, and maintenance of an IT Infrastructure to effectively support automated needs (i.e. platforms, networks, servers, printers, etc.).
 3. **(140) Information Security** involves all functions pertaining to the protection of federal information and information systems from unauthorized access, use, disclosure, disruptions, modification, or destruction, as well as the creation and implementation of security policies, procedures and controls.
 4. **(263) System and Network Monitoring** supports all activities related to the real-time monitoring of systems and networks for optimal performance.

4.2.1 Operational Business Model

The target state IT Infrastructure operational business architecture, as shown in Figure 4 below, outlines the functions of the IT Infrastructure that support the other SBA business segments (e.g., Financial Assistance, Procurement & Grants Management, etc.). It provides a framework to manage and support the IT infrastructure and related services while also mitigating risk in order to meet the service targets of the business. The IT Infrastructure operational business architecture leverages processes from ITIL version 3 in the areas of:

- **Service Management** covers the definition of services, creating suitable measures, and a go-to-market strategy.

- **Delivery Management** ensures a proper interface back to customers of IT Infrastructure, including work intake mechanisms and reporting and client management functions.
- **Technology Management** places emphasis on simplifying technical operations and ensuring a highly available environment.

FIGURE 4: TARGET STATE OPERATIONAL BUSINESS ARCHITECTURE


Target state operational processes that have been identified as “existing business process to be improved” are existing processes that have been improved or updated and processes designated with “new business process” are new operational processes for the target state. Below is the list of operational processes that fall into one of the aforementioned categories:

Existing Business Process to be Improved

- (1) Service Level Management
- (2) Capacity Management
- (3) Availability Management
- (4) IT Service Continuity Management
- (8) Service Portfolio Management
- (9) IT Financial and Performance Management

New Business Process

- (10) Service Catalog Management
- (11) Service Lifecycle Management
- (12) Metric Management
- (26) SOA Governance

Existing Business Process to be Improved New Business Process

- (13) Change Management
- (18) Service Desk
- (20) Incident Management
- (21) Request Fulfillment
- (23) Problem Management

Table 14 provides a list of all the operational processes (current and target state) with their appropriate mapping to performance metrics

TABLE 14: OPERATIONAL PROCESSES TO METRICS MAPPING

Operational Process	Metric
Service Management	
(1) Service Level Management	XSP-1, MB-04-01-02-11.1, MB-04-01-02-11.2
(2) Capacity Management	PAR-1, SP-MSSS-2, SP-MSSS-4, SP-MSSS-6, SP-TSS-2, SP-TSS-4, SP-TSS-6, SP-TSS-8, SP-TSS-10, SP-TSS-13
(3) Availability Management	PAR-1, MB-04-04-05-8.4
(4) IT Service Continuity Management	SP-EUSS 4, SP-EUSS 5, SP-EUSS 6, SP-EUSS 7, MB-04-04-05-8.1
(5) Information Security Management	PAR-2, MB-04-04-05-08.2
(6) IT Architecture Management	XSP-3
(7) Supplier Management	MB-04-04-04-11.3
(8) Service Portfolio Management	All
(9) IT Financial and Performance Management	SP-EUSS-1, SP-EUSS-2, SP-MSSS-1, SP-MSSS-3, SP-MSSS-5,
(10) Service Catalog Management	XSP-2, ISP-2
(11) Service Lifecycle Management	MB-04-04-04-08.1, MB-04-04-04-08.2

Operational Process	Metric
(12) Metric Management	All
Delivery Management	
(13) Change Management	MB-04-04-04-11.4
(14) Release Management	MB-04-04-04-11.4
(15) Configuration Management	MB-04-04-04-08.1, MB-04-04-04-08.2
(16) Transition Planning & Support	N/A
(17) Service Validation & Testing	MB-04-04-04-11.4
(18) Service Desk	SP-EUSS-8, SP-EUSS-10, SP-EUSS-11, MB-04-01-02-08.1
Technology Management	
(19) Event Management	PAR-1, MB-04-01-02-11.3
(20) Incident Management	PAR-1, MB-04-01-02-11.3
(21) Request Fulfillment	SP-EUSS-10, SP-EUSS-11,
(22) Access Management	PAR-2, XSP-3
(23) Problem Management	PAR-1, MB-04-01-02-11.3
(24) IT Operations Management	All
(25) IT Facilities Management	XSP-3, MB-040404-11.1, MB-040404-11.2,
(26) SOA Governance	ISP-1, ISP-2

Please refer to Appendix H: Current State Business Architecture for further details on the current state business architecture.

4.3 Target State Service Component Architecture

4.3.1 Service Component Model

The goal of the target state service component architecture is to define how IT infrastructure and services will align with the desired future state capabilities to meet its strategic objectives.

The FEA service component reference model provides guidance for federal agencies to identify, categorize, build and catalog discrete services. The service components are identified based on the business services they need to support.

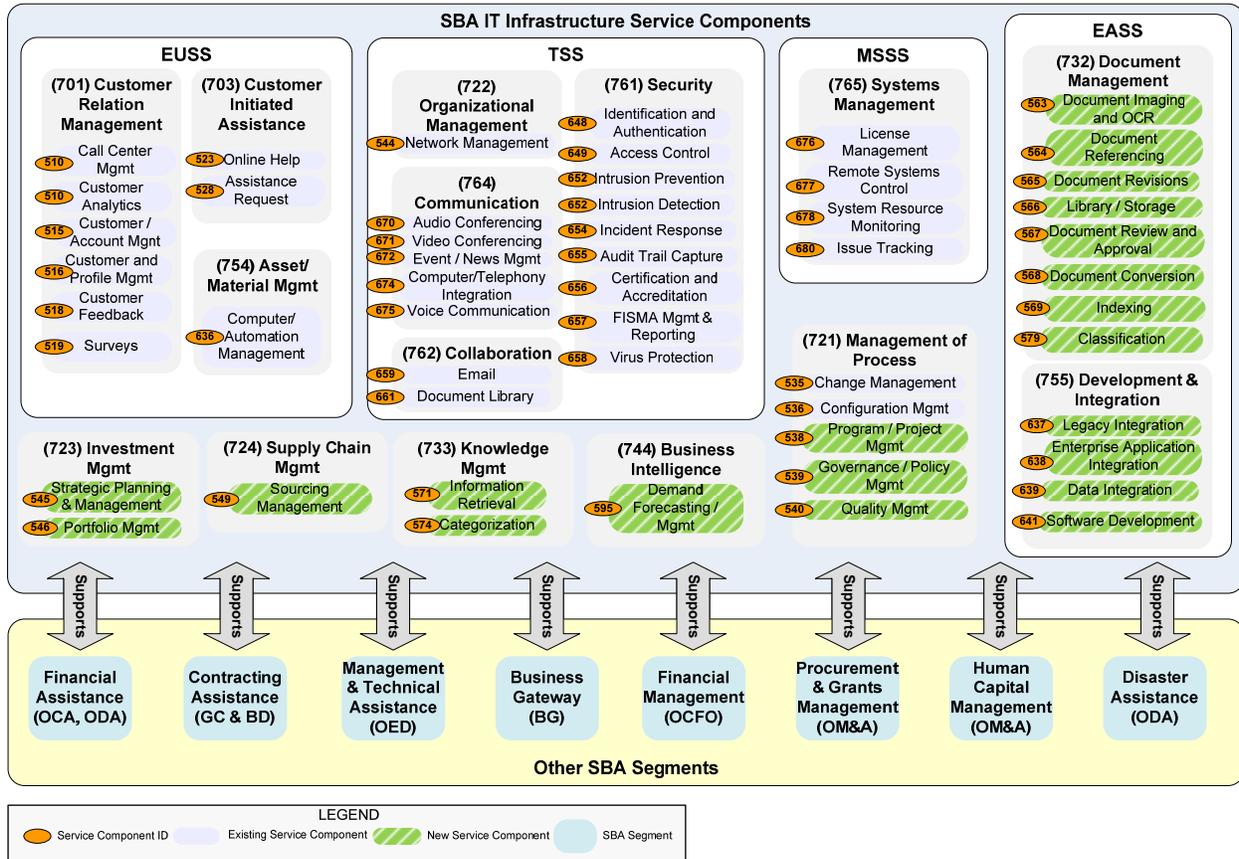
FIGURE 5: TARGET STATE SERVICE COMPONENT ARCHITECTURE


Table 15 provides a mapping of each of the 13 new service components to the business functions they support. These new service components are essential for the SBA transition to an SOA delivery capability.

TABLE 15: NEW SERVICE COMPONENTS MAPPING TO BUSINESS FUNCTIONS

Service Domain	Service Type	Service Component	Business Functions Supported
Business Management Services	(721) Management of Process	(538) Program / Project Management	(119) Facilities, Fleet and Equipment Management (137) Lifecycle / Change Management
Business Management Services	(721) Management of Process	(539) Governance / Policy Management	(119) Facilities, Fleet and Equipment Management (137) Lifecycle / Change Management

Service Domain	Service Type	Service Component	Business Functions Supported
Business Management Services	(721) Management of Process	(540) Quality Management	(139) IT Infrastructure Maintenance (263) System & Network Monitoring
Business Management Services	(723) Investment Management	(545) Strategic Planning and Management	(094) Contingency Planning (095) Continuity of Operations (137) Lifecycle / Change Management
Business Management Services	(723) Investment Management	(546) Portfolio Management	(119) Facilities, Fleet and Equipment Management (137) Lifecycle / Change Management
Business Management Services	(724) Supply Chain Management	(549) Sourcing Management	(119) Facilities, Fleet and Equipment Management
Digital Asset Services	(732) Document Management	(563) Document Imaging and OCR	(139) IT Infrastructure Maintenance
Digital Asset Services	(732) Document Management	(564) Document Referencing	(139) IT Infrastructure Maintenance
Digital Asset Services	(732) Document Management	(565) Document Revisions	(139) IT Infrastructure Maintenance
Digital Asset Services	(732) Document Management	(566) Library / Storage	(139) IT Infrastructure Maintenance
Digital Asset Services	(732) Document Management	(567) Document Review and Approval	(139) IT Infrastructure Maintenance
Digital Asset Services	(732) Document Management	(568) Document Conversion	(139) IT Infrastructure Maintenance
Digital Asset Services	(732) Document Management	(569) Indexing	(139) IT Infrastructure Maintenance

Service Domain	Service Type	Service Component	Business Functions Supported
Digital Asset Services	(732) Document Management	(570) Classification	(139) IT Infrastructure Maintenance
Digital Asset Services	(733) Knowledge Management	(571) Information Retrieval	(139) IT Infrastructure Maintenance
Digital Asset Services	(733) Knowledge Management	(574) Categorization	(139) IT Infrastructure Maintenance
Business Analytical Services	(744) Business Intelligence	(595) Demand Forecasting / Management	(094) Contingency Planning (095) Continuity of Operations (137) Lifecycle / Change Management
Back Office Services	(755) Development and Integration	(637) Legacy Integration	(137) Lifecycle / Change Management (140) Information Security
Back Office Services	(755) Development and Integration	(638) Enterprise Application Integration	(137) Lifecycle / Change Management (140) Information Security
Back Office Services	(755) Development and Integration	(639) Data Integration	(137) Lifecycle / Change Management (140) Information Security
Back Office Services	(755) Development and Integration	(641) Software Development	(137) Lifecycle / Change Management (140) Information Security

The target state service component architecture will address the following issues observed from the current state:

1. Reuse and Sharing of IT Infrastructure Services - ODA uses both OCIO and its own IT services to support its infrastructure in current state. Since ODA has different operating standards and service level requirements than OCIO, it will still provide some of its own IT services such as systems management functions to support operations. However, other duplicate service components, such as email, virus protection, change

management, and configuration management will be gradually consolidated with the same functions in OCIO. ODA will have stronger collaboration with OCIO to promote the opportunities for sharing common service components.

2. Formalize Service Level Agreements – New service components, such as program / project management, quality management, and governance / policy management, will be included in the target state to support the management and reporting of SLAs.
3. Strategy for the Next Generation Data Center Services – New service components, such as strategic planning / management and demand forecasting / management, could project the future requirements for data center planning. Sourcing management service component could support the vendor selection and relation management for outsourcing data center services.
4. Process Compliance – New service components, such as governance / policy management and portfolio management, could help to ensure that the policies or mandates that impact processes in other segments are fully addressed. Existing processes will be assessed and revised to ensure the policy compliance across segments within SBA.
5. Alignment and Integration – New service components, such as strategic planning and management and portfolio management, can help to ensure that the impact caused by a new IT investment is communicated to all stakeholders so that the potential conflicts in design, architecture, and project sequencing could be resolved in a well-planned manner.
6. Transition to SOA Environment – Governance / policy management will address the governance of SOA policies and performance metrics for the program offices. Information retrieval and categorization, under the knowledge management service type, will support the service registration and discovery for SOA. The legacy integration and enterprise application integration services will help to transition the existing applications to SOA.

Table 16 provides a full list of the target state service components and the opportunities each supports.

TABLE 16: TARGET STATE SERVICE COMPONENTS

Service Domain	Service Type	Service Component	Business Area	Opportunity Supported
Customer Services	(701) Customer Relation Management	(510) Call Center Management	EUSS	13, 28, 39
Customer Services	(701) Customer Relation Management	(511) Customer Analytics	EUSS	39
Customer Services	(701) Customer Relation Management	(515) Customer/Account Management	EUSS	39
Customer Services	(701) Customer Relation Management	(516) Contact and Profile Management	EUSS	39

Service Domain	Service Type	Service Component	Business Area	Opportunity Supported
Customer Services	(701) Customer Relation Management	(518) Customer Feedback	EUSS	39
Customer Services	(701) Customer Relation Management	(519) Surveys	EUSS	39
Customer Services	(703) Customer Initiated Assistance	(523) Online Help	EUSS	39
Customer Services	(703) Customer Initiated Assistance	(528) Assistance Request	EUSS	39
Business Management Services	(721) Management of Process	(535) Change Management	All	38
Business Management Services	(721) Management of Process	(536) Configuration Management	All	31, 38
Business Management Services	(721) Management of Process	(538) Program / Project Management	MSSS, EASS	20, 27, 28, 29, 36, 37, 38, 39, 40, 41, 42, 43, 52
Business Management Services	(721) Management of Process	(539) Governance / Policy Management	EASS	26, 36, 37, 38, 39, 40, 41, 42, 43, 44, 46, 51, 52, 53, 54
Business Management Services	(721) Management of Process	(540) Quality Management	All	38, 39, 40, 41, 42, 53
Business Management Services	(722) Organizational Management	(544) Network Management	TSS	1, 2, 4, 8, 18, 19, 24, 25, 40, 43, 46, 47, 51
Business Management Services	(723) Investment Management	(545) Strategic Planning and Management	All	1, 2, 3, 5, 8, 14, 15, 16, 20, 24, 29, 30

Service Domain	Service Type	Service Component	Business Area	Opportunity Supported
Business Management Services	(723) Investment Management	(546) Portfolio Management	All	32, 33, 37, 42
Business Management Services	(724) Supply Chain Management	(549) Sourcing Management	All	12, 30, 52
Digital Asset Services	(732) Document Management	(563) Document Imaging and OCR	EASS	33, 36, 37, 42, 59
Digital Asset Services	(732) Document Management	(564) Document Referencing	EASS	33, 36, 37, 42, 59
Digital Asset Services	(732) Document Management	(565) Document Revisions	EASS	33, 36, 37, 42, 59
Digital Asset Services	(732) Document Management	(566) Library / Storage	EASS	33, 36, 37, 42, 59
Digital Asset Services	(732) Document Management	(567) Document Review and Approval	EASS	33, 36, 37, 42, 59
Digital Asset Services	(732) Document Management	(568) Document Conversion	EASS	33, 36, 37, 42, 59
Digital Asset Services	(732) Document Management	(569) Indexing	EASS	33, 36, 37, 42, 59
Digital Asset Services	(732) Document Management	(570) Classification	EASS	33, 36, 37, 42, 59
Digital Asset Services	(733) Knowledge Management	(571) Information Retrieval	EASS	33, 36, 37, 42
Digital Asset Services	(733) Knowledge Management	(574) Categorization	EASS	33, 36, 37, 42
Business Analytical Services	(744) Business Intelligence	(595) Demand Forecasting / Management	All	15, 21, 22, 23
Back Office Services	(754) Asset / Material Management	(636) Computer / Automation Management	EUSS	31, 39, 49

Service Domain	Service Type	Service Component	Business Area	Opportunity Supported
Back Office Services	(755) Development and Integration	(637) Legacy Integration	EASS	37, 42, 59
Back Office Services	(755) Development and Integration	(638) Enterprise Application Integration	EASS	35, 37, 42, 43, 55, 56, 57, 58, 59
Back Office Services	(755) Development and Integration	(639) Data Integration	EASS	35, 37, 42, 59
Back Office Services	(755) Development and Integration	(641) Software Development	EASS	35, 37, 42, 55, 56, 57, 59
Support Services	(761) Security	(648) Identification and Authentication	TSS, EASS	18, 19, 34, 41, 57, 58, 59
Support Services	(761) Security	(649) Access Control	TSS, EASS	18, 19, 34, 41, 47, 56, 58, 59
Support Services	(761) Security	(652) Intrusion Prevention	TSS	24, 41, 46, 51
Support Services	(761) Security	(653) Intrusion Detection	TSS	24, 41, 45
Support Services	(761) Security	(654) Incident Response	TSS, MSSS	24, 41, 45, 48
Support Services	(761) Security	(655) Audit Trail Capture and Analysis	All	24, 41, 45, 49, 50
Support Services	(761) Security	(656) Certification and Accreditation	All	41
Support Services	(761) Security	(657) FISMA Management and Reporting	EUSS, TSS, MSSS	41, 54
Support Services	(761) Security	(658) Virus Protection	EUSS, TSS, MSSS	41
Support Services	(762) Collaboration	(659) Email	TSS	11, 32, 40
Support Services	(762) Collaboration	(661) Document Library	TSS	11, 40

Service Domain	Service Type	Service Component	Business Area	Opportunity Supported
Support Services	(764) Communication	(670) Audio Conferencing	TSS	16, 40
Support Services	(764) Communication	(671) Video Conferencing	TSS	17, 40
Support Services	(764) Communication	(672) Event / News Management	TSS	17, 40
Support Services	(764) Communication	(674) Computer / Telephony Integration	TSS	16, 40
Support Services	(764) Communication	(675) Voice Communication	TSS	16, 40
Support Services	(765) Systems Management	(676) License Management	MSSS	38
Support Services	(765) Systems Management	(677) Remote Systems Control	MSSS	1, 2, 4, 6, 7, 8, 10, 38
Support Services	(765) Systems Management	(678) System Resource Monitoring	MSSS	1, 2, 7, 8, 9, 10, 38
Support Services	(765) Systems Management	(680) Issue Tracking	MSSS	35, 38

4.4 Target State Data Architecture

The role of the IT Infrastructure segment is to provide support to the operational environments of business-driven segments within SBA. The major components of this segment are hardware, network equipment, and supporting software. The software components within this segment are all commercial off-the-shelf (COTS) software packages that have self-contained databases and do not rely on other systems to perform their functions. Since the IT Infrastructure segment pertains to hardware/networking equipment and software to support operations, data architecture is not required and will not be part of the IT Infrastructure segment architecture. Interoperability with the utilization of SOA and the use of data warehouses and marts will be addressed in the pending IT Information Sharing segment architecture, which will include components supporting data and knowledge management. In addition, this segment will also include capabilities for ad-hoc reporting and search, which are more closely aligned to information sharing.

4.5 Target State Technology Architecture

The technical architecture provides a view into the key software and hardware technologies that provide the infrastructure for the services. Table 17 provides a mapping of the services and the supporting key technologies.

TABLE 17: MAP OF SERVICE COMPONENTS (SRM) WITH THE TECHNOLOGY COMPONENTS

Service Components	Technology
(510) Call Center Management	CA Unicenter Service Desk
(511) Customer Analytics	CA Unicenter Service Desk
(515) Customer/Account Management	CA Unicenter Service Desk
(516) Contact and Profile Management	CA Unicenter Service Desk
(518) Customer Feedback	ColdFusion application
(519) Surveys	Raosoft Survey Software (InterForm)
(523) Online Help	TBD
(528) Assistance Request	CA Unicenter Service Desk
(535) Change Management	CA Unicenter Service Desk
(536) Configuration Management	MS Excel, NETPRO - Configuration & Change Management Software License & Maintenance
(538) Program / Project Management	MS Project
(539) Governance / Policy Management	TBD
(540) Quality Management	TBD
(544) Network Management	Internet Access, Hosting Service, Internet Protocol Version 4 (IPv4), Internet Protocol Version 6 (IPv6) Maintenance, WAN – Internet Protocol (IP), Big-IP Load Balancer
(545) Strategic Planning and Management	TBD
(546) Portfolio Management	TBD
(549) Sourcing Management	TBD
(563) Document Imaging and OCR	TBD
(564) Document Referencing	TBD
(565) Document Revisions	TBD
(566) Library / Storage	TBD
(567) Document Review and Approval	TBD
(568) Document Conversion	TBD
(569) Indexing	TBD
(570) Classification	TBD
(571) Information Retrieval	TBD
(574) Categorization	TBD

Service Components	Technology
(595) Demand Forecasting / Management	TBD
(636) Computer / Automation	CA Unicenter Service Desk
(637) Legacy Integration	TBD
(638) Enterprise Application Integration	TBD
(639) Data Integration	TBD
(641) Software Development	TBD
(648) Identification and Authentication	PIV card
(649) Access Control	PIV card, NetVersant - LAN Room Security access cards and Readers, Remote Access / Tokens, Juniper NetScreen VPN/Firewall
(652) Intrusion Prevention	NetSec Verizon, NetForensics
(653) Intrusion Detection	NetSec Verizon, NetForensics
(654) Incident Response	NetForensics, NetSec Verizon. CA Unicenter Service Desk
(655) Audit Trail Capture and Analysis	NetForensics, UNIX, Internet Monitoring
(656) Certification and Accreditation	TBD
(657) FISMA Management and Reporting	NetForensics, MS Word, MS Excel
(658) Virus Protection	McAfee - Anti Virus Software License & Maintenance
(659) Email	Intelligence Communications Solutions - Blackberry technology support, Message One - Blackberry Failover Software License & Maintenance, MX Logic - Anti Spam Software License & Maintenance, Yancy Assoc. - E-mail Archival
(661) Document Library	MS SharePoint, Intranet
(670) Audio Conferencing	Teleconference Service
(671) Video Conferencing	Teleconference Service
(672) Event / News Management	TBD
(674) Computer / Telephony Integration	WAN Support – NOC, Cisco Routers

Service Components	Technology
(675) Voice Communication	Desk Top Fax, Fax Operator, Fax Service, Network Support, Telephone Customer Service / Maintenance Support, PDA Blackberry & Cellular, Local Telephone Calling Service, Long Distance Calling Service, Monitor Telecommunication Services, Telephone Dial Tone, Voicemail
(676) License Management	NETPRO - Configuration & Change Management Software License & Maintenance, MS Excel
(677) Remote Systems Control	CA Unicenter Service Desk
(678) System Resource Monitoring	Syslog
(680) Issue Tracking	CA Unicenter Service Desk

There are service components that have the supporting technology yet to be defined. OCIO will need to evaluate these service components and determine whether they are purely manual processes. In addition, there will be the need to identify the scope and requirements for the service components that need technology support so that the evaluation process could be established to select the appropriate technologies.

Table 18 includes the FEA Technical Reference Model Service Areas, Service Categories, and Service Standards as well as a cross-reference to the corresponding technology used in the target state solution.

TABLE 18: MAP OF THE TECHNOLOGY COMPONENTS WITH THE TRM

Service Area	Service Category	Service Standards	Technology Used
Service Access & Delivery	Access Channels	(851) Wireless / PDA	PDA Blackberry & Cellular
		(852) Collaboration / Communications	Teleconference Service, Desk Top Fax, Fax Operator, Fax Service, Network Support, Telephone Customer Service / Maintenance Support, NETPRO -

Service Area	Service Category	Service Standards	Technology Used
			Configuration & Change Management Software License & Maintenance, Spectrum
	Delivery Channels	(854) Internet	Internet Access, TCP/IP
		(855) Intranet	TCP/IP
		(857) Peer to Peer (P2P)	NTVI Help Desk & LAN Support
		(858) Virtual Private Network (VPN)	NTVI Help Desk & LAN Support, Remote Access / Tokens, Juniper NetScreen VPN/Firewall
	Service Requirements	(859) Legislative / Compliance	Hosting Service, Internet Monitoring
		(861) Hosting	Internal, External
	Service Transport	(862) Supporting Network Services	WAN Support - NOC
		(863) Service Transport	TCP / IPv4, IPv6, SMTP
	Service Platform and Infrastructure	Support Platforms	(865) Independent Platform
(866) Dependent Platform			Windows 2003, UNIX, Mainframe
Delivery Servers		(871) Web Servers	Apache, IIS
Hardware / Infrastructure		(877) Servers / Computers	Windows, UNIX, Mainframe
		(878) Embedded Technology Devices	Disk Array, CPU, RAM
		(879) Peripherals	Printer, Scanner

Service Area	Service Category	Service Standards	Technology Used
		(880) Wide Area Network (WAN)	WAN - Internet Protocol (IP)
		(881) Local Area Network (LAN)	Capital Computer Solutions - BPA - Micro Computer Equipment Maintenance Supplies, NETPRO - Configuration & Change Management Software License & Maintenance, NetVersant - LAN Room Security access cards and Readers, McAfee - Anti Virus Software License & Maintenance, Intelligence Communications Solutions - Blackberry technology support, Message One - Blackberry Failover Software License & Maintenance, MX Logic - Anti Spam Software License & Maintenance, Yancy Assoc. - E-mail Archival, NTVI - Infrastructure Support LAN & Help Desk
		(882) Network	Cisco Routers,

Service Area	Service Category	Service Standards	Technology Used
		Devices / Standards	Local Telephone Calling Service, Long Distance Calling Service, Monitor Telecommunication Services, Telephone Dial Tone, Voicemail, Big IP Load Balancer, Firewall
Component Framework	Security	(884) Certificates / Digital Signatures	SSL
		(885) Supporting Security Services	Security Operations Center, SAML

4.5.1 Target State Conceptual View

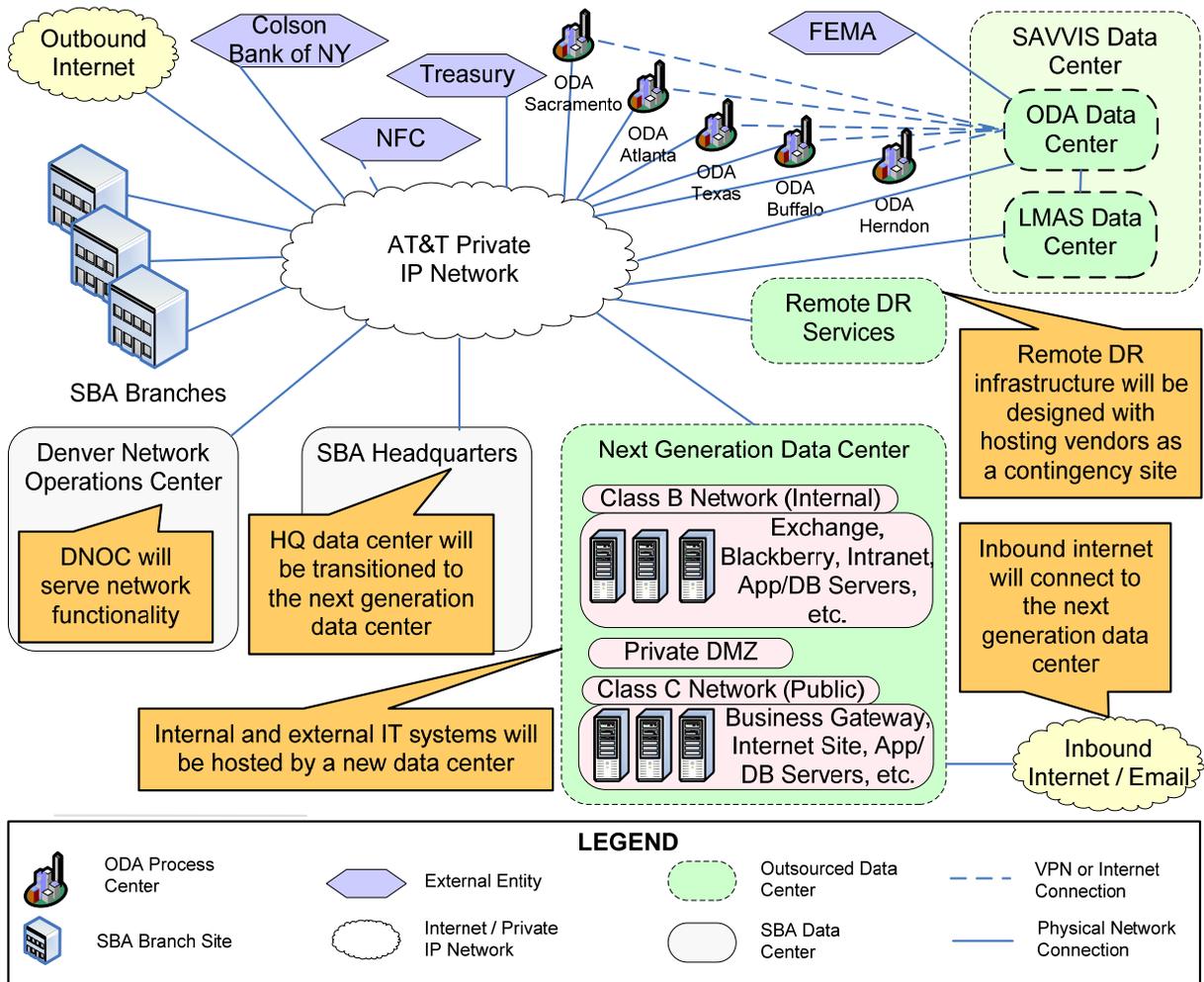
This section provides a conceptual view of the target state IT Infrastructure to address the key issues observed from the current state.

4.5.1.1 Network Infrastructure

The target state SBA network is comprised of the following operational entities:

- Three outsourced data centers for the Disaster Credit Management System (DCMS), and the Loan Management Accounting System (LMAS), and a next generation data center that will host both the internal and external IT systems that are currently hosted at the headquarters data center.
- Another facility to provide remote DR infrastructure capabilities.
- Headquarters entity that will provide network functionality.
- A network operations center at the Denver Network Operations Center (DNOC).
- Processing centers and field offices.

Figure 6 depicts the target state network infrastructure. It is intended to provide a high-level, simplified logical view of the SBA network with connections to key elements.

FIGURE 6: SBA TARGET STATE NETWORK INFRASTRUCTURE


The target state network infrastructure will address the following issues observed from the current state:

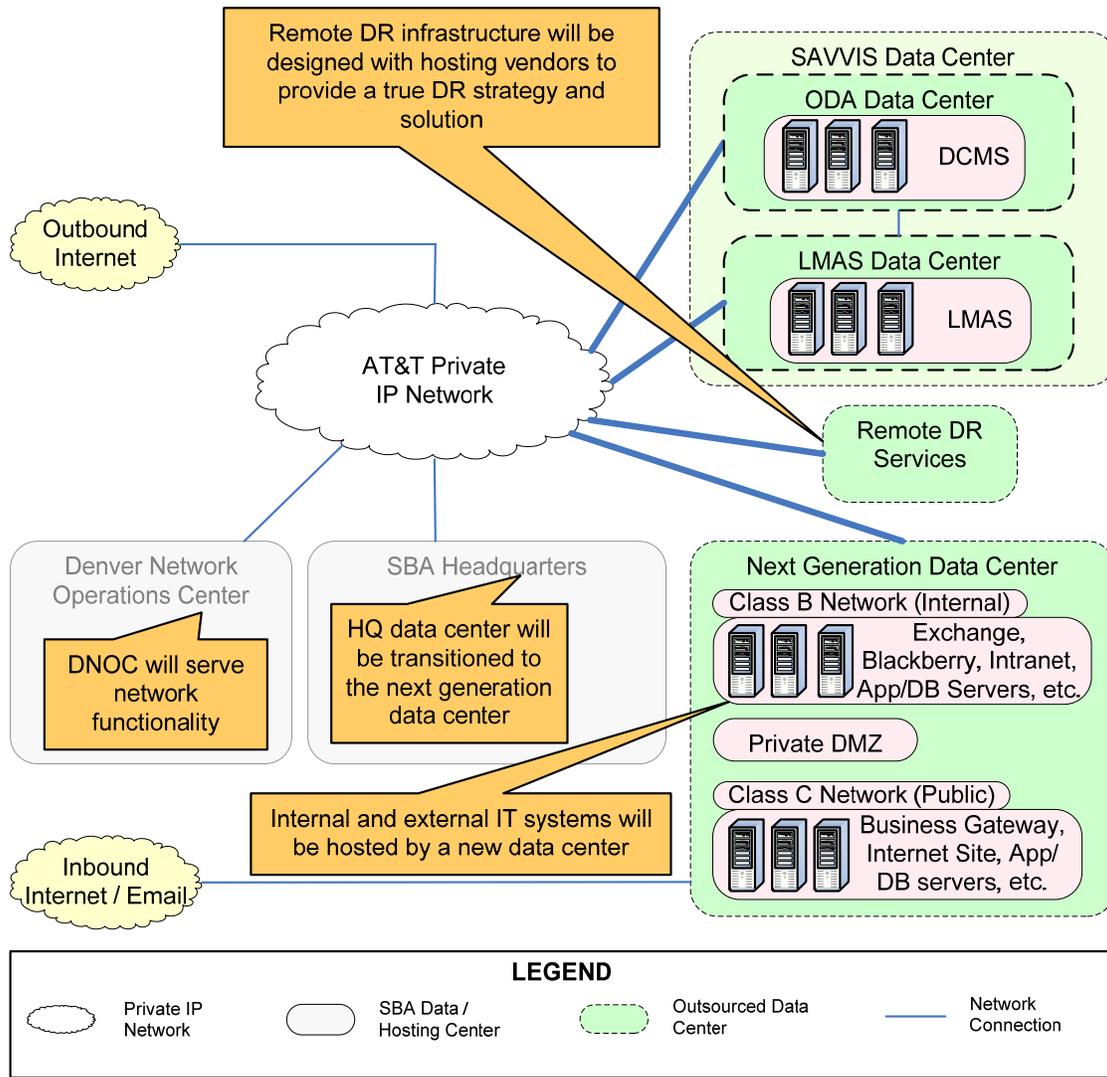
1. Network Analysis and Modernization – The initial findings from the network health initiative do not indicate any issues that require immediate action. OCIO will conduct the network analysis as an on-going process to identify areas for improvement in the network infrastructure.
2. Networkx – Networkx is a new government wide contract administered by GSA that replaces FTS2001 for telecom services. All agencies will have to transition to Networkx by 2010. This initiative is focusing on the procurement of telecom service contracts in order to realize cost savings for the agency. Transitioning telecom service providers will not cause major impacts to the existing network infrastructure (i.e., topology, operations, or security measures).
3. TIC – The purpose for the TIC initiative is to minimize the connections between the SBA network and the internet to ensure better security control and realize potential cost savings. During the current state assessment of the IT Infrastructure segment

architecture, there were still nine connections not considered to be TIC compliant. The target state network infrastructure will address these issues with the following approaches:

- The VPN connections from the four ODA processing centers at Herndon, Buffalo, Atlanta, and Texas to the ODA data center are legitimate and TIC compliant. These connections are to provide redundancy to ensure the connectivity between ODA processing centers and data center. Since VPN is not considered a public internet connection, they are TIC compliant.
 - The connections from FEMA, NFC, Treasury, and Colson are legitimate and TIC compliant. They are required for key business functions. These connections are either VPN or a dedicated line, not a public internet connection.
 - The DSL line connection to Verizon was for the test of video conferencing. It will be consolidated to a private IP network or eliminated after the transition to Networx.
4. IPv6 – SBA has completed the OMB mandated IPv6 milestones in June 2008. Since most of the external stakeholders of SBA are not yet operating in IPv6, SBA cannot transition its network to a full IPv6 operation until stakeholders are ready for the technology. To be ready for the IPv6 transition, SBA will need to perform a full scale assessment on the enterprise applications in its IT portfolio for IPv6 compliance as well as provide IPv4 routing capabilities during the transition. The impacts on the network security, network topology, and overall network operations will have to be assessed.
5. IT Security – The implementation of a security operations center (SOC) has recently been completed. Functioning as a centralized data collector for information from the sensors and security checkpoints, the SOC will enable centralized logging and auditing as well as application and database intrusion detection for all field offices and headquarters. It will help to ensure that formal operational processes for incident management are being followed and expand the incident response capability with the integration of incident management between SBA field offices and headquarters.

4.5.1.2 Data Center Operations

Figure 7 depicts the target state Headquarters, DNOC, outsourced ODA and LMAS Data Centers, and a new next generation data center hosting both internal and external IT systems. It also includes a brief list of applications hosted at each data center. The highlighted parts of the figure represent the data center components and the network infrastructure they leverage.

FIGURE 7: SBA TARGET STATE DATA CENTERS AND NETWORK INFRASTRUCTURE


1. Data Center

- Due to its higher level of service requirements and availability demands, DCMS is hosted by a specialized vendor, SAVVIS, at a facility in Herndon, Virginia.
- LMAS will be hosted by SAVVIS at the same facility.
- With the implementation of LMAS, the Joint Administrative Accounting Management System (JAAMS) will be migrated to the same SAVVIS facility and integrated with LMAS. The Corio data center that hosts JAAMS will be rationalized.
- The Unisys data center at Eagan, Minnesota hosts the legacy mainframe systems that will be replaced by LMAS. The Unisys data center will be rationalized.
- The current state HQ Data Center hosts network operations, business applications, and IT systems for external customers. It has limited capacity and will need improvements to meet more stringent standards and requirements. Although the plan for the next generation data center is undetermined yet, it is highly recommended that SBA seeks a specialized vendor to outsource the HQ Data Center services. The new next generation data center will host both the internal and external IT systems to provide improved redundancy and availability. It will

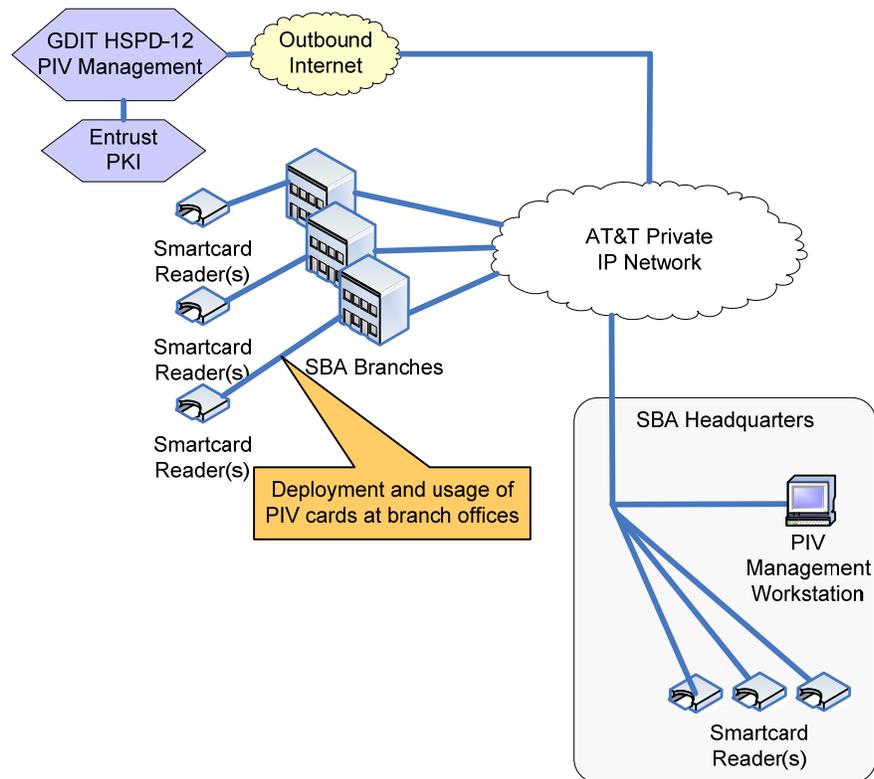
also enable better security capabilities and support Green IT initiatives, reducing SBA's carbon footprint. With the hosting services outsourced, the HQ Data Center facility will only provide network functionality in the target state.

- Currently, DNOC serves many critical network functions for SBA field personnel. It also serves as an alternate facility for HQ network operations and contingency site for Exchange and Blackberry servers. With the establishment of the next generation data center and the remote DR infrastructure, DNOC will transition the messaging services to the new hosting facility, but may continue to serve other network functionality to SBA field personnel.
 - ODA currently hosts its own Exchange and Trio servers. With a formalized SLA process and fault-tolerant infrastructure for Exchange and Blackberry services, ODA will consolidate its messaging services with OCIO in the next generation data center.
2. Remote DR Infrastructure – Since SBA is outsourcing the data center hosting services for its mission-critical systems, it is necessary to work with the hosting vendors to determine the infrastructure for remote disaster recovery. The design should be integrated with the SBA network and data center infrastructure. Small scale and ad hoc solutions may not be an effective approach for a remote DR strategy. A business impact analysis and DR solution analysis will have to be conducted.

4.5.1.3 HSPD-12

The short term objectives for HSPD-12 are to deploy the infrastructure and increase the issuance of personal identification verification (PIV) cards. There is a potential to utilize the PIV cards for logical access control and further leverage the HSPD-12 platform to consolidate the use of security tokens or other IP security solutions. With a potential full deployment of the HSPD-12 platform, PIV cards could also be used for physical access control and in addition, a potential enterprise-wide identity vault, which the HSPD-12 initiative would fall under, could be leveraged to standardize the process for identity management and serve as the master data repository.

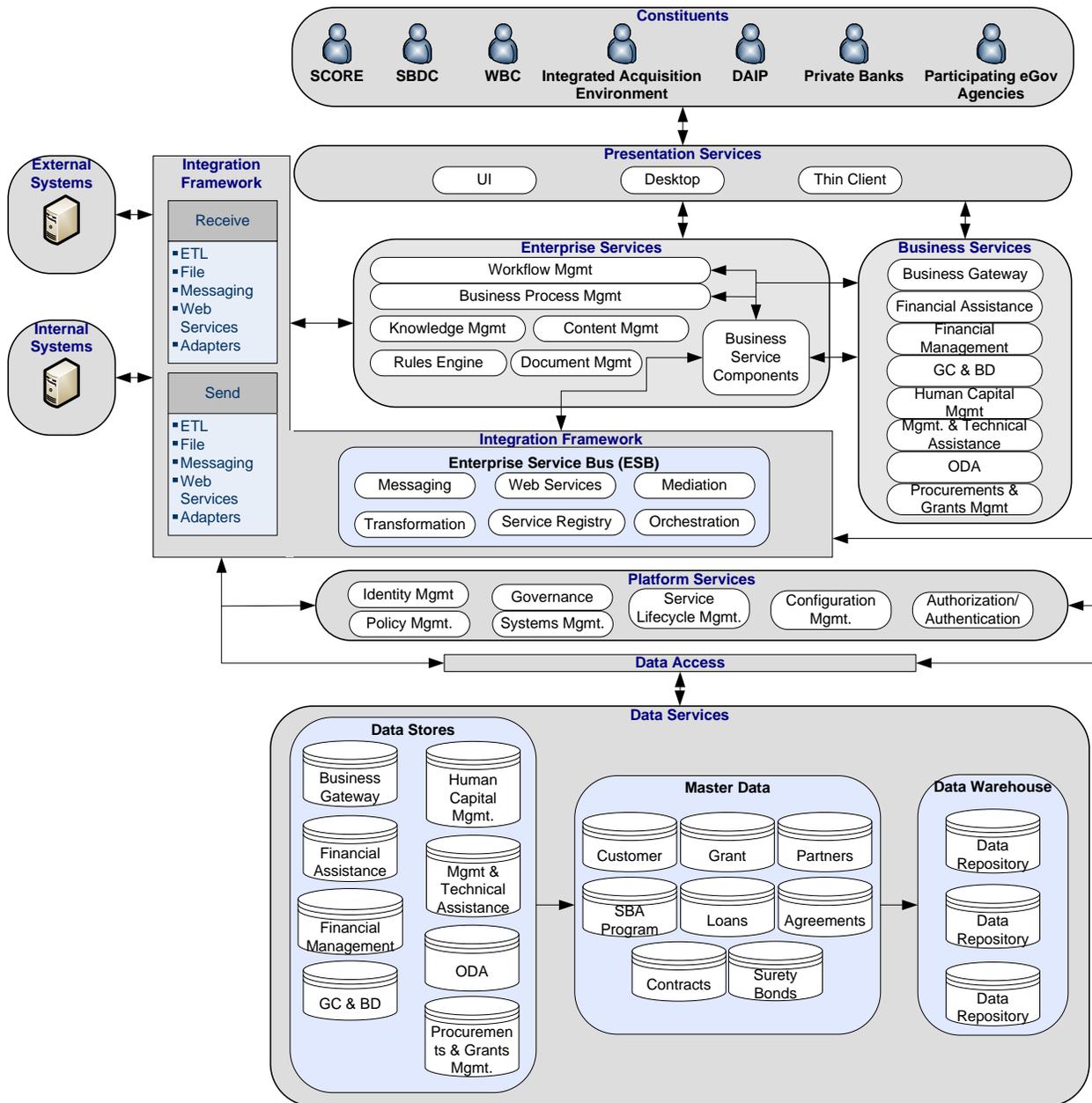
Figure 8 depicts how the PIV authentication services leverage the SBA network infrastructure to connect to the external PIV management services and the target state deployment of PIV cards to the branch offices.

FIGURE 8: PIV SERVICES LEVERAGING SBA NETWORK INFRASTRUCTURE


4.5.1.4 Service Oriented Architecture

SOA Platform – In order to promote better reuse of service components and achieve business flexibility, SBA could potentially utilize an SOA-based delivery approach to technology solutions. Within OCIO, applications and data are running on various platforms and siloed within each line of business and program. There are currently no application and data integration components in place at OCIO that may promote reuse and sharing within a line of business or even across lines of business. ODA leverages components for integration and messaging, but currently may not be mature and integrate well with OCIO for sharing of services and information. Both OCIO and ODA have developed a limited set of web services that are used on an ad-hoc basis to integrate with external parties. Further analysis and decomposition of business services can be conducted to identify commonalities for reuse.

Figure 9 outlines a high-level, conceptual SOA platform model that utilizes common SOA-related technology components. This figure only serves as a model to provide a conceptual view into the end state architecture, which may take more than five years to fully mature. Proper planning and collaborative relationships between OCIO and the business segments will have to be achieved in order to deliver an SOA capability that is driven by business needs and requirements. As outlined in Section 4.2.1, adherence to formal processes for SOA Governance and Service Lifecycle/Portfolio Management will be needed to support the planning and execution of SBA's SOA delivery capability. Furthermore, there will have to be cognizance that SOA is not an out of the box technology that can be deployed to solve problems, but that it is a business driven, architectural approach that involves people, processes, and technologies in order to achieve business flexibility and cost savings through the reuse of services.

FIGURE 9: SOA CONCEPTUAL PLATFORM


Various areas of the SOA conceptual platform from Figure 9 are outlined below:

- **Presentation Services** - Corresponds to elements of the user interface such as text, checkbox, and user interaction such as keystrokes and mouse movements.
- **Business Services** – Corresponds to specific units of work that achieve business results. Business services will have to be further analyzed and decomposed for each segment.
- **Enterprise Services** – These services are common and may be shared enterprise-wide to support business services. Enterprise service components may include workflow management, business process management, and business service components. Tools that support workflow management and business

process management may not be needed within the early stages of an SOA, but may come under consideration as the SOA delivery capability matures and there is a business justification for more robust tools.

- **Integration Framework** – Refers to capabilities that enable integration between external parties and internal components. Within an SOA, web services using SOAP are commonly used as service interfaces to integrate between a service consumer and a service provider. A central component to the integration framework is an enterprise service bus (ESB), which provides the capabilities of messaging, transformation, mediation, and orchestration in order to integrate between entities. In addition, a Universal Description Discovery and Integration (UDDI) based service registry is another common component that is utilized for publishing and discovery of services as well as defining how services interact. A service registry can be maintained in a spreadsheet or on a web page during the infancy stages of an SOA, but as the delivery capabilities mature, evaluation of service registry tools may need to be considered.
- **Platform Services** – Corresponds to non-business focused services that support the complete lifecycle of an SOA delivery capability. Common components include governance, identity management, policy management, and service lifecycle management.
- **Data Services** – Refers to the services that retrieve data from the enterprise data entities. These can include data stores, master data, and a data warehouse.

4.6 Security

The security of SBA's information and associated systems must be integrated into the system design and managed throughout the system lifecycle in order to mitigate risks as best as possible. The core philosophy behind federal information security practices is to develop a comprehensive risk management strategy that provides proper protection for IT systems and information.

Please refer to the external document "SBA Security Framework" for details about the SBA security framework process methodology, gap analysis, recommendations, and systems security plan.

4.7 IPv6 Transition

SBA is planning for the transition of the current SBA network backbone from an IPv4-only network layer to a combined IPv4 and IPv6 network layer. The goal of this transition is to introduce the IPv6 protocol to the SBA network environment gradually over a period of time through a series of initiatives based on the guidance of the SBA Enterprise Architecture.

Please refer to the document "SBA IPv6 Transition Sequence Plan" for details about agency governance, architectural segments, concept of operations, IPv6 program major milestones and schedules, IPv6 capable definitions and requirements, and risk inventory and assessment.

5 Appendix A: Acronyms

TABLE 19: LIST OF ACRONYMS

Acronyms	Expansion
BIA	Business Impact Analysis
BRM	Business Reference Model
COOP	Continuity of Operations Plan
DCMS	Disaster Credit Management System
DME	Development, Modernization, and Enhancement
DNOC	Denver Network Operations Center
DR	Disaster Recovery
DRM	Data Reference Model
EAAF	Enterprise Architecture Assessment Framework
EASS	Enterprise Application Support Services
EUSS	End User Systems and Support
FDCC	Federal Desktop Core Configuration
FEA	Federal Enterprise Architecture
FTF	Federal Transition Framework
HSPD-12	Homeland Security Presidential Directive 12
ITILOB	IT Infrastructure Optimization Line of Business
JAAMS	Joint Accounting Administrative Management System
LMAS	Loan Management Accounting System
LOB	Line of Business
IPv6	Internet Protocol Version 6
LTO	Long Term Objective
MSSS	Mainframe and Server Services and Support
OCIO	Office of the Chief Information Officer
ODA	Office of Disaster Assistance

Acronyms	Expansion
OIG	Office of Inspector General
OMB	Office of Management and Budget
PES	Productivity Enhancement Staff
PMO	Program Management Office
SBA	Small Business Administration
SOA	Service Oriented Architecture
SOC	Security Operations Center
TIC	Trusted Internet Connections
TRB	Technical Review Board
TRM	Technical Reference Model
TSS	Telecom Systems and Support
UDDI	Universal Description Discovery and Integration

6 Appendix B: Segment Architecture Overview

Segment architecture provides a business-driven, results-oriented blueprint of a manageable portion of an enterprise. While the scope of an Enterprise Architecture focuses on aligning the agency resources with the agency's mission and strategic goals, segment architecture focuses on a particular mission area or business service within the agency

This segment architecture endeavor is a collaborative process between functions of the OCIO. It provides the critical bridge between the SBA's strategic vision and medium term business and IT plans. To do this, the segment architecture describes a baseline ("as-is", "current state") architecture, future ("to-be", "target") architecture, and a transition roadmap for IT Infrastructure.

6.1 Use of Segment Architecture

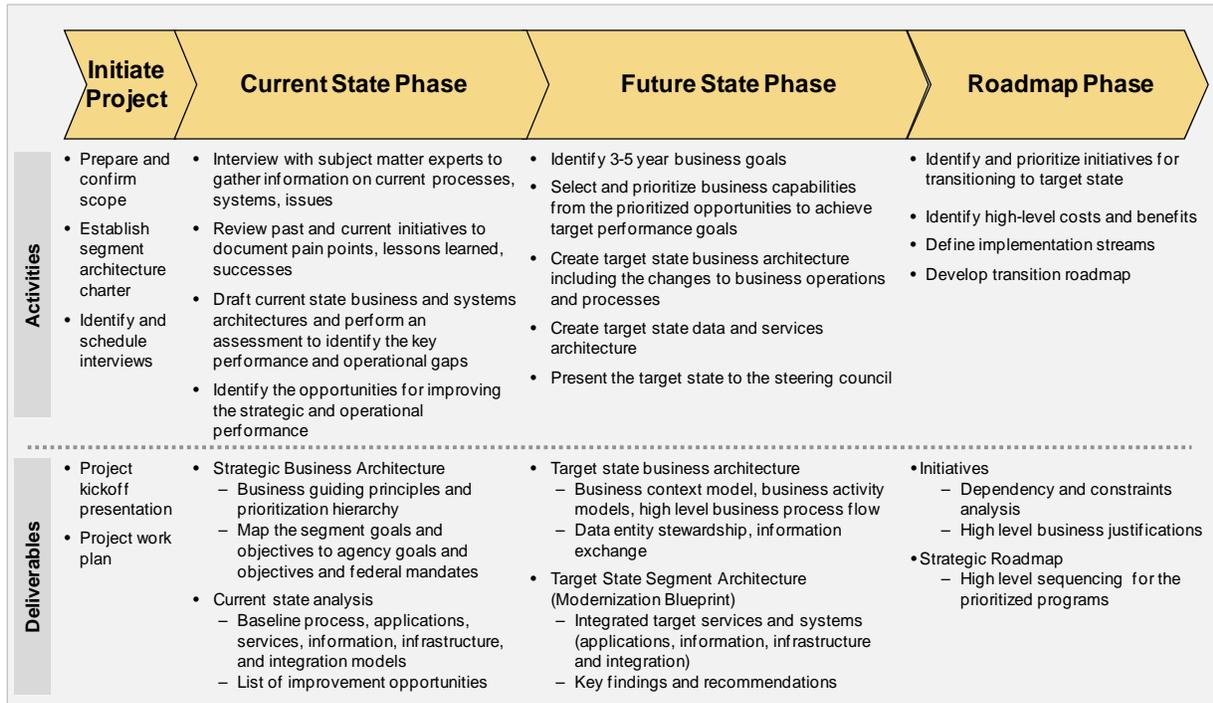
The segment architecture will be the "blueprint" to guide investment and implementation of information technology from the current environment to the future envisioned IT environment. The methodology used facilitates making informed decisions about the nature and priority of identified opportunities. The information derived throughout the process is used to plan and initiate business and information management solutions that will assist in the achievement of target performance goals.

6.2 Ownership

The segment architecture is owned, maintained, and used by business stakeholders of the segment, and it is created in collaboration with the EA program staff members. The segment architecture blueprint may evolve over time to reflect changing internal and external factors.

6.3 Stages of Segment Architecture Process

The IT Infrastructure segment architecture is being defined through a three-step methodology based on OMB's Segment Architecture guidance. First, the current state business and technology architecture are documented, based on stakeholder input and documented program processes, organization, and technology. The current state assessment forms the basis for the future, or desired, state. The future state is also influenced by internal and external business drivers. Finally, a transition roadmap is developed, enumerating a set of initiatives to close the gap between current and future states and guiding stakeholders through the transition. The future state and roadmap are future deliverables that will be forthcoming in Q3 2008. The overall methodology is illustrated in Figure 10.

FIGURE 10: SEGMENT ARCHITECTURE PROCESS


7 Appendix C: Organization and Stakeholders

The IT Infrastructure segment is a subset of the Office of the Chief Information Officer. As defined by the ITILOB, there are three components of infrastructure:

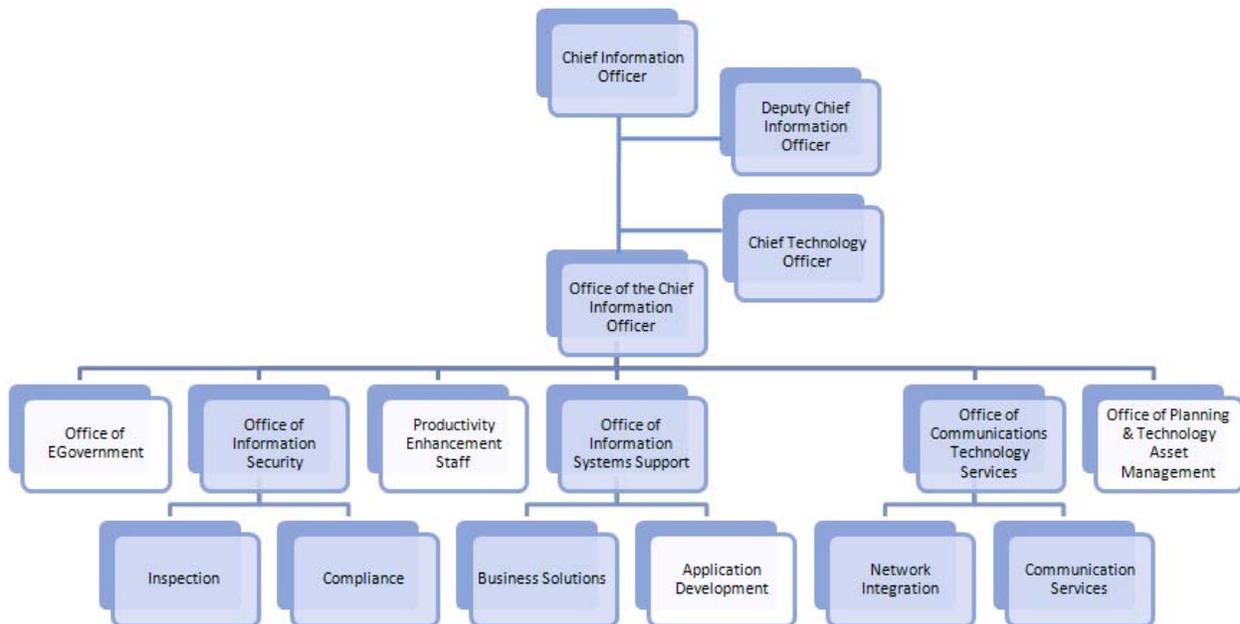
- End User Systems and Support (EUSS) - This area covers acquisition, deployment, and ongoing support (including Help Desk) for the technology associated with the desktop computing environment.
- Telecommunications Systems and Support (TSS) - This area covers the hardware, software, and communication services for data exchange including networks and telephone systems.
- Mainframe and Server Services and Support (MSSS) - This area covers the equipment and software for the process, storage, and management of data and information.

Outside of the ITILOB, there is the additional component of:

- Enterprise Application Support Services (EASS) – This area covers the software, processes, and services for the management and support of enterprise applications. The segment architecture will focus on SOA-related topics for this component.

The OCIO organizational structure is shown in Figure 11, with relevant IT infrastructure-related offices highlighted in blue. The hiring of the CTO is likely to change the OCIO organization slightly, but those changes are not yet formalized.

FIGURE 11: OCIO ORGANIZATION (IT INFRASTRUCTURE HIGHLIGHTED)



The primary offices responsible for IT Infrastructure are described below. The other offices of OCIO also help support IT Infrastructure, but are not directly involved:

- Office of Information Security (OIS) - This office is responsible for all aspects of IT security, including TIC and HSPD-12.

- Office of Information Systems Support (OISS) - This office manages and supports the data centers, including servers and mainframes. In addition, this office is responsible for application development and maintenance, which is outside the scope of the IT Infrastructure segment. It makes up MSSS.
- Office of Communications Technology Services (OCTS) - This office manages the network (LAN and WAN), network operations center, telephone/telecom services, and the Help Desk. It encompasses both EUSS and TSS.

Table 20: OCIO Interview List represents the OCIO staff members interviewed during the current and/or target state IT Infrastructure segment architecture analysis.

TABLE 20: OCIO INTERVIEW LIST

Interviewees	Title	Validated
Christine Liu	Chief Information Officer	
Charles McClam	Deputy Chief Information Officer	
Paul Christy	Chief Technology Officer	
Richard Coffee	Chief Architect	
David McCauley	Chief Information Security Officer, OIS	
Ronald Whalen	Director, OISS	Current State - Figure 15: SBA Data Centers and Network Infrastructure Target State - Figure 7: SBA Target State Data Centers and Network Infrastructure
Sherry Hill	Director, OCTS	
Thomas Peretzman	IT Specialist, OCTS	
Linda Terrell	Chief, Network Integration Branch, OCTS	Current State - Figure 13: SBA Current State Network Infrastructure Target State - Figure 6: SBA Target State Network Infrastructure
Steve Kuhns	Telecom Specialist, OCTS	
Austin Porter	Computer Specialist, OISS	
Ravoyne Payton	IT Specialist, HSPD-12	Current State - Figure 14: PIV Services Leveraging SBA

Interviewees	Title	Validated
		Network Infrastructure Target State - Figure 8: PIV Services Leveraging SBA Network Infrastructure
Justin Newman (contractor)	IT Specialist, HSPD-12	
Michael Sorrento	Director, DCMS Operations Center, ODA	
Gale Wallace	IT Specialist, DCMS Operations Center, ODA	
Steve Stine	Project Manager, DCMS Operations Center, ODA	

8 Appendix D: SBA Goals and Objectives

Table 21: SBA Strategic Goals provides information on the strategic goals outlined in the SBA Strategic Plan.

TABLE 21: SBA STRATEGIC GOALS

Goal#	Goal	LTO#	Long Term Objective
1	Expand America's ownership society, particularly in underserved markets	1.1	Improve access to SBA programs and services by small businesses to drive business formation, job growth, and economic activity
		1.2	Support entrepreneurship in markets with higher poverty and unemployment, and in our military community
		1.3	Ensure stewardship and accountability over taxpayer dollars through prudent financial portfolio management and oversight
2	Provide timely financial assistance to homeowners, renters, nonprofit organizations and businesses affected by disaster	2.1	Respond quickly, efficiently and effectively to disaster applicants
3	Improve the economic environment for small business	3.1	Protect, strengthen and effectively represent the Nation's small businesses to minimize the regulatory burden
		3.2	Foster a more small-business friendly environment
4	Ensure management and organizational excellence to increase responsiveness to customers, streamline processes, and improve compliance and controls	4.1	Deploy a skilled workforce capable of executing high-quality programs
		4.2	Provide a safe and secure information system environment to support business decisions and Agency operations
		4.3	Provide financial and performance management services to support efficient and effective program delivery

9 Appendix E: Key Business Drivers

The OCIO Infrastructure segment architecture is affected by internal and external business drivers, listed below. Internal drivers reflect the Agency's own needs and goals; external drivers originate from sources outside of the SBA, including regulatory bodies, industry standards organizations, and customer groups.

9.1.1 Internal Drivers

- Dispersed and Mobile Workforce – SBA's workforce is located in dozens of field offices across the country. Also, in times of disaster response, the Agency may add a significant number of employees, who need remote network access (e.g., wireless) out in the field. Across many sectors of the SBA workforce, demand for mobile computing and mobile devices is growing.
- Expiring Contracts - Several existing contracts for infrastructure operations or support are up for renewal in the upcoming months. This presents the SBA with options to change course and realize cost savings from other vendors or renegotiated contracts.
- Security and Privacy – The Inspector General identified several security challenges in the last several audits and OIS has been continually working to address them all. With the implementation of Web 2.0/collaborative tools and wireless network access, the SBA IT Infrastructure needs to have a secure environment with policies, physical/logical access controls, and environmental controls in place in order to mitigate threats and risks.
- New Development, Modernization, and Enhancement (DME) Investment – One of SBA's largest IT investments in the next several years will be for the Loan Management and Accounting System (LMAS) which will be one of SBA's primary mission-oriented systems, responsible for loan origination, servicing, and liquidation. SBA's infrastructure must support the new system; at the same time, SBA will look for opportunities to reuse LMAS investments for the benefit of the Agency.
- Robust Infrastructure – SBA is seeking a robust and scalable IT infrastructure that can provide the foundation for the implementation of Web 2.0 tools, interoperability with SOA, information sharing with data marts and warehouses, and sufficient network bandwidth for multicasting streaming video. In addition, the IT infrastructure should also be robust enough to meet the needs of emerging technologies (e.g., cloud computing, grid computing, etc). A robust IT infrastructure can enable these capabilities, which provide cost savings and increase efficiency of work.

10 Appendix F: External Directives

- Government Wide Initiatives - There are a large number of government-wide initiatives that will require changes to the SBA's IT Infrastructure. These initiatives, primarily driven by OMB, are seeking to optimize IT government-wide, and make the entire IT infrastructure more secure, interoperable across agencies, and cost effective. At the same time, they seek to promote collaboration and resource sharing.
 - ITILOB – This LOB will develop an effective and efficient IT infrastructure enabling government-wide customer-centric services.
 - TIC – TIC is defined in OMB Memorandum M-08-05. The initiative is designed to reduce the number of individual external Internet connections in use by the federal government.
 - HSPD-12 – Homeland Security Presidential Directive 12 requires a common identification standard for Federal employees and contractors. This covers logical access to networks and systems.
 - IPv6 - This initiative was first described in OMB Memorandum M-05-22. It is designed to ensure an orderly and secure transition across the federal government from Internet Protocol Version 4 (IPv4) to IPv6.
 - Networx - Networx is the new government wide contract administered by GSA that replaces FTS2001 for telecom services. All agencies will have to transition to Networx by 2010.
- Green IT - The rapid rise in energy costs, a growing move toward environmental conservation, and recent Federal guidance all are putting pressure on the SBA to reduce its carbon footprint and energy usage by minimizing electricity usage and heat output in IT operations.
- Budget Environment - Though federal IT spending has increased, at least modestly, for the past several years, IT budgets for the next several years are likely to be severely constrained, due to the greater economic downturn and the high cost of associated government programs, leaving little budget available for discretionary spending.

11 Appendix G: Prioritized Opportunities

Target state opportunities are the basic units of improvement that drive overall organizational performance. The OCIO IT Infrastructure opportunities have been grouped into the following categories:

- **Customer Satisfaction (CS)** – improvements in OCIO’s ability to support mission functions throughout the Agency.
- **Green IT (G)** – improvements to comply with environmental initiatives to reduce the energy consumption, carbon footprint, and encourage use of sustainable practices in OCIO.
- **Operational Efficiency (OE)** – improvements in OCIO’s efforts that support the Agency’s day-to-day functions.
- **Performance Measurement and Monitoring (PMM)** – improvements to better manage and evaluate performance metrics from an enterprise-wide perspective in order to track OCIO performance improvements.
- **Security and Privacy (SP)** – improvements to OCIO security and privacy measures in order to actively mitigate threats and vulnerabilities.

In addition, these opportunities have been prioritized by stakeholders into the following categories:

- **Building the Foundation** – Opportunities in this category should be implemented in the immediate term as they require low effort and have high business impact.
- **Enabling Improvement** – Opportunities in this category should be implemented in the midterm as resources allow. These opportunities are critical to mid- and long-range success of the Infrastructure segment.
- **Fulfill Vision** – These are longer term opportunities due to the difficulty to implement. As time passes, the IT Infrastructure segment will have to collect metrics to determine criticality and confirm business value.
- **Defer** – There is insufficient business reason to justify the cost of pursuing these opportunities unless government mandates, compliance, or legal issues are the drivers. Develop workarounds as necessary.

Table 22 shows how each opportunity is prioritized, as well as its category.

TABLE 22: PRIORITIZED OPPORTUNITIES

Foundational	Enablement	Visionary	Defer
28. Define and Formalize Help Desk Processes (OE)	3. Integration of DR Planning (CS)	2. DR for Messaging Capabilities at ODA (CS)	
29. Include ODA in HQ Infrastructure Decision Making (OE)	5. True Data Center at HQ (CS)	7. Optimization of Server Config (G)	
43. Overall Metric Capturing and Reporting (OE) (PMM)	6. Virtualization (G)	14. Mainframe Contingency Before LMAS (OE)	
44. HSPD-12 Planning and Governance (OE)	11. Archive and Retrieve Emails (OE)	34. Integration of HSPD-12 w/ HCM Systems (OE)	
49. Monitor Usage and Software (OE)	21. Storage Capacity Monitoring and Forecasting (OE)	31. 100% Compliance w/ FDCC (OE)	
27. Enforce Formal Operational Processes (OE)	26. ITIL Governance (OE)	35. Incident Report Consolidation (OE)	
10. Proactively Manage Power Usage (G)	23. Network Bandwidth Monitoring and Forecasting (OE)	36. Shared Infrastructure Services (OE)	
22. Environmental Requirement Monitoring and Forecasting (OE)	38. MSSS Metrics (PMM)	42. SOA Metrics (PMM)	
	39. EUSS Metrics (PMM)	59. SOA Security (SP)	
	40. TSS Metrics (PMM)	57. Leverage HSPD-12 to Streamline Network Auth (SP)	
	41. Security Metrics (PMM)	46. TIC Security (SP)	
	12. Leverage Network (OE)	54. NIST Security Compliance (SP)	
	13. Training to Properly Route Help Desk Calls (OE)	56. Leverage HSPD-12 to Streamline Access Control (SP)	



Foundational	Enablement	Visionary	Defer
	15. Data Center Consolidation (OE)	58. Leverage HSPD-12 to Simplify App Auth and Control (SP)	
	20. ITIL Planning (OE)	57. Leverage HSPD-12 to Streamline Network Auth (SP)	
	33. Share Tools Between OCIO and ODA (OE)	55. Leverage HSPD-12 to Standardize Security (SP)	
	48. Improved Incident Response	17. Simulcast of Streaming Video (OE)	
	50. Centralized Auditing System (SP)	19. Wireless Network Access (OE)	
	51. Follow TIC Guidance (SP)	32. Rationalize ODA Messaging Servers (OE)	
	52. Include Security w/ Outsourcing Contracts (SP)	37. SOA Delivery Capability (OE)	
	53. Application Security Measures and Standards (SP)	47. Wireless Network Access w/ Full Security (SP)	
	9. Monitor and Measure Energy Utilization (G)	18. Constant Wireless Evolution (OE)	
	1. Remote DR for HQ (CS)	8. Cloud Computing (G)	
	25. Network Health Analysis (OE)		
	30. Tech-focused Procurement Group (OE)		
	4. Reconstitution at HQ (CS)		
	45. Centralized Security Monitoring (SP)		
	24. Plan for Broader IPv6 Scope (OE)		
	16. Transition to VoIP (OE)		

Opportunities for improvement were uncovered through stakeholder interviews and group discussion. These opportunities were prioritized based on business need and difficulty by stakeholders. A business need rating of 10 indicates highest priority; the lower the rating, the less important it is to the organization. An implementation difficulty rating of 1 indicates straightforward implementation; the higher the difficulty rating, the greater the complexity and cost to implement.

Scales: Business Need Rating (1=Not Important, 10=Important), Implementation Difficulty Rating (1=Low Difficulty, 10=High Difficulty)

TABLE 23: OPPORTUNITY DETAILS

#	Category	Title	Description	Business Need	Implementation Difficulty
1	Customer Satisfaction	Remote DR for HQ	The ability to have a solid remote DR infrastructure for HQ	8.75	7.38
2	Customer Satisfaction	DR Infrastructure for ODA Messaging	The ability to provide DR infrastructure and capabilities for messaging at ODA	2.20	6.61
3	Customer Satisfaction	Integration of DR Planning	The ability to integrate the DR/remote backup recovery planning efforts with the next generation data center infrastructure planning	9.38	6.13
4	Customer Satisfaction	Reconstitution at HQ	The ability to allow the information system to be recovered and reconstituted to the system's original state after a system disruption or failure at HQ	8.38	7.38
5	Customer Satisfaction	True Data Center at HQ	The ability to have access to a true data center at HQ	9.75	7.50
6	Green IT	Virtualization	The ability to host multiple applications in one physical server to save space and cost	6.43	6.86
7	Green IT	Optimization of Server Config	The ability to optimize the size and configuration of servers	6.75	4.86
8	Green IT	Cloud Computing	The ability to transition to cloud computing (at least a "federal cloud") if/when it	5.13	6.29

#	Category	Title	Description	Business Need	Implementation Difficulty
			becomes available in the future		
9	Green IT	Monitor & Measure Energy Utilization	The ability to better monitor and measure data center energy utilization	5.63	5.57
10	Green IT	Proactively Manage Power Usage	The ability to proactively manage power usage in the overall IT infrastructure	4.71	5.00
11	Operational Efficiency	Archive & Retrieve Emails	The ability to archive and retrieve emails	8.88	5.38
12	Operational Efficiency	Leverage Network	The ability to leverage Network and government-wide capabilities to save cost	7.25	5.38
13	Operational Efficiency	Training to Properly Route Help Desk Calls	The ability to provide agency-wide communication and training to have help desk calls routed properly	7.00	5.25
14	Operational Efficiency	Mainframe Contingency Before LMAS	The ability to provide contingency for mainframe systems before LMAS is ready	8.29	6.86
15	Operational Efficiency	Data Center Consolidation	The ability to consolidate the current state processing for data centers	7.00	6.25
16	Operational Efficiency	Transition to VoIP	The ability to transition the telephone service to VoIP	5.63	5.50
17	Operational Efficiency	Simulcast of Streaming Video	The ability to provide streaming video to the entire agency simultaneously	6.88	5.63
18	Operational Efficiency	Constant Wireless Evolution	The ability to adapt to constantly evolving wireless devices and standards	8.00	5.75
19	Operational Efficiency	Wireless Network Access	The ability to provide wireless network access (as needed) throughout the agency, regardless of location	7.38	5.50
20	Operational Efficiency	ITIL Planning	The ability to better plan for implementation of ITIL service management processes.	7.25	5.13

#	Category	Title	Description	Business Need	Implementation Difficulty
21	Operational Efficiency	Storage Capacity Monitoring & Forecasting	The ability to have proactive storage capacity monitoring and forecasting	8.00	5.50
22	Operational Efficiency	Environmental Requirement Monitoring & Forecasting	The ability to have proactive environmental requirement monitoring and forecasting	5.50	5.38
23	Operational Efficiency	Network Bandwidth Monitoring & Forecasting	The ability to have proactive network bandwidth monitoring and forecasting	7.50	5.25
24	Operational Efficiency	Plan for Broader IPv6 Scope	The ability to plan for a broader scope IPv6 assessment to address issues such as software compatibility, network security, and IPv4/IPv6 dual stack network infrastructure design	6.13	6.75
25	Operational Efficiency	Network Health Analysis	The ability to provide a network health analysis and identify areas for upgrades or re-design	6.88	5.63
26	Operational Efficiency	ITIL Governance	The ability to enhance or initiate governance procedures to oversee ITIL service management services	7.25	4.63
27	Operational Efficiency	Enforce Formal Operational Processes	The ability to ensure formal operational processes (e.g., incident management) are being followed	8.38	4.88
28	Operational Efficiency	Define & Formalize Help Desk Processes	The ability to define and formalize help desk processes	8.38	4.75
29	Operational Efficiency	Include ODA in HQ Infrastructure Decision Making	The ability to include ODA infrastructure teams in HQ decision-making	8.13	4.38
30	Operational Efficiency	Tech-focused Procurement Group	The ability to utilize the expertise of a tech-focused procurement group, either within the government or private industry	8.25	3.63

#	Category	Title	Description	Business Need	Implementation Difficulty
31	Operational Efficiency	100% Compliance w/ FDCC	The ability to have 100% compliance with FDCC	7.63	6.75
32	Operational Efficiency	Rationalize ODA Messaging Servers	The ability to rationalize ODA Trio and Exchange servers	5.50	4.38
33	Operational Efficiency	Share Tools Between OCIO & ODA	The ability to leverage tools (e.g., Cognos) between OCIO and ODA	7.00	3.75
34	Operational Efficiency	Integration of HSPD-12 w/ HCM Systems	The ability to coordinate HSPD-12/PIV cards with the HCM systems	7.71	6.71
35	Operational Efficiency	Incident Report Consolidation	The ability to consolidate incidents reporting through one help desk portal	7.25	5.38
36	Operational Efficiency	Shared Infrastructure Services	The ability to identify and reuse shared infrastructure services	7.00	6.25
37	Operational Efficiency	SOA Delivery Capability	The ability to implement processes, tools, and governance for a technology SOA delivery capability	6.57	5.86
38	Performance Measurement & Monitoring	MSSS Metrics	The ability to define and measure performance metrics for MSSS	7.88	5.00
39	Performance Measurement & Monitoring	EUSS Metrics	The ability to define and measure performance metrics for EUSS	8.00	5.25
40	Performance Measurement & Monitoring	TSS Metrics	The ability to define and measure performance metrics for TSS	8.13	5.00
41	Performance Measurement & Monitoring	Security Metrics	The ability to define and measure performance metrics for Security	8.50	5.88

#	Category	Title	Description	Business Need	Implementation Difficulty
42	Performance Measurement & Monitoring	SOA Metrics	The ability to define and measure performance metrics for SOA	7.14	6.00
43	Performance Measurement & Monitoring	Overall Metric Capturing & Reporting	The ability to provide overall metric capturing and monitoring	8.25	6.63
44	Security & Privacy	HSPD-12 Planning & Governance	The ability to communicate HSPD-12 requirements, processes, and lead time for processes to SBA staff and executives to ensure that HSPD-12 processes are not compromised	7.88	4.88
45	Security & Privacy	Centralized Security Monitoring	The ability to provide centralize logging and auditing as well as application and database intrusion detection	7.63	6.13
46	Security & Privacy	TIC Security	The ability to coordinate TIC with IP based security restrictions	6.63	6.88
47	Security & Privacy	Wireless Network Access w/ Full Security	The ability to provide remote/wireless access to the SBA network with full security	3.16	7.31
48	Security & Privacy	Improved Incident Response	The ability to improve incident response capabilities	1.58	6.38
49	Security & Privacy	Monitor Usage & Software	The ability to monitor software usage restrictions and user installed software	0.20	4.07
50	Security & Privacy	Centralized System Auditing	The ability to compile audit records from multiple components throughout the system into a system-wide, time-correlated audit trail	2.37	6.15

#	Category	Title	Description	Business Need	Implementation Difficulty
51	Security & Privacy	Follow TIC Guidance	The ability to follow the TIC guideline to identify internet connections that should be removed, modify the network topology, and plan for contingency to address the identified connections to be removed	2.96	5.92
52	Security & Privacy	Include Security w/ Outsourcing Contracts	The ability to ensure that security compliance and measures are included in outsourcing contracts	1.20	5.23
53	Security & Privacy	Application Security Measures & Standards	The ability to ensure applications meet security measures and standards	0.20	6.15
54	Security & Privacy	NIST Security Compliance	The ability to comply with all NIST security guidelines	2.76	7.77
55	Security & Privacy	Leverage HSPD-12 to Standardize Security	The ability to leverage the HSPD-12 platform to standardize the IT security framework	3.16	8.46
56	Security & Privacy	Leverage HSPD-12 to Streamline Access Control	The ability to leverage HSPD-12 platform to streamline physical and logical access control processes	3.16	8.00
57	Security & Privacy	Leverage HSPD-12 to Streamline Network Auth	The ability to leverage the HSPD-12 platform to streamline the network authentication process	2.37	8.00
58	Security & Privacy	Leverage HSPD-12 to Simplify App Auth & Control	The ability to leverage the HSPD-12 platform for simplified authentication and access control to SBA enterprise applications	3.36	8.23
59	Security & Privacy	SOA Security	The ability to integrate security and policies throughout the SOA planning and implementation processes.	2.17	8.23

12 Appendix H: Current State Business Architecture

12.1 Performance Analysis Summary

From the metrics referenced in Section 4.1.4, the current state performance metrics were not as comprehensive, but business performance metrics from the ITILOB 5 Year Optimization Plan were analyzed to identify metrics that achieved targets and discover potential performance gaps. Metrics cover the areas of EUSS, TSS, and MSSS, but there are no EASS metrics in place for the current state.

Target Achieved

- EUSS
 - Cost per primary device
 - Cost per user
- MSSS
 - Mainframe cost per MIPS
 - Mainframe availability
 - Cost per server
 - Server availability
- TSS
 - WAN availability
 - LAN availability
 - Internet network availability
 - Phone availability (local and long distance)

Overall, SBA demonstrates good performance in the areas of network, phone, and server availability as well as cost per primary device, servers, and MIPS.

Performance Gaps

- EUSS
 - Cost per Help Desk handle contact
 - Help Desk speed of answer
- MSSS
 - UNIX cost per server
- TSS
 - WAN cost per device
 - LAN cost per port
 - Internet access cost
 - Long distance cost
 - Cellular cost

- Local phone cost

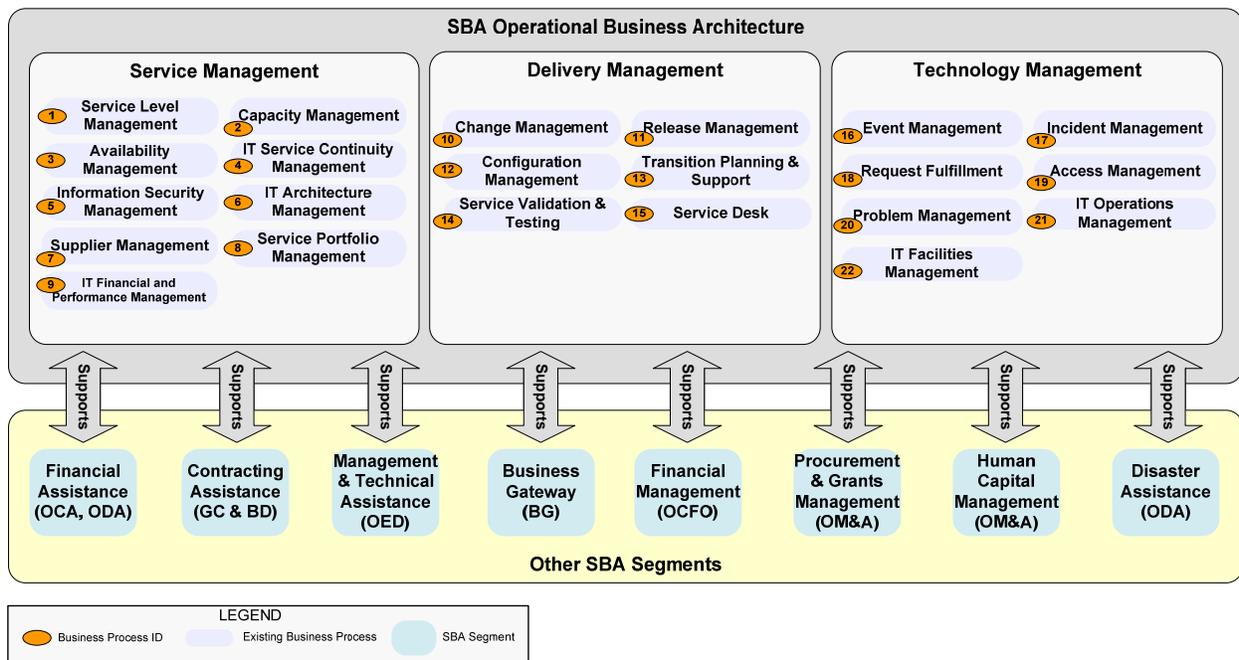
The performance gaps in the areas of high cost of the Help Desk, high cost of UNIX servers, and high cost of all telecommunications services indicate that these are potential opportunity areas for improvements to increase efficiency.

12.2 Operational Business Architecture

The IT Infrastructure operational business architecture, as shown in Figure 12, outlines the processes for the operations of the IT Infrastructure that supports the other SBA business segments (e.g., Financial Assistance, Procurement & Grants Management, etc.). It provides a framework to manage and support the IT infrastructure and related services while also mitigating risk in order to meet the service targets of the business. The IT Infrastructure operational business architecture leverages processes from the IT Infrastructure Library (ITIL) version 3 in the areas of:

- **Service Management** covers the definition of services, creating suitable measures, and a go-to-citizen strategy.
- **Delivery Management** ensures a proper interface back to customers of IT Infrastructure, including work intake mechanisms and reporting and client management functions.
- **Technology Management** places emphasis on simplifying technical operations and ensuring a highly available environment.

FIGURE 12: IT INFRASTRUCTURE OPERATIONAL BUSINESS ARCHITECTURE



The tables below provide information on the processes of the IT Infrastructure operational business architecture, focusing on the key functions, participants, input, and output.

12.2.1 Service Management

12.2.1.1 Service Level Management

TABLE 24: SERVICE LEVEL MANAGEMENT

Key Function	<ul style="list-style-type: none"> Negotiate and document service level agreements with the business for the agreed upon infrastructure service targets Ensure all operational level agreements and underpinning contracts are appropriate as well as monitor and report on targets
Participants	OISS, OIS, OCTS Directors, Procurement Specialist, IT Operations Manager, IT Specialist
Input	Definition of metrics; data regarding performance; verification of data validity
Output	Consistent measurement of all infrastructure services, fulfilling: <ol style="list-style-type: none"> Service level agreements (SLAs) Operational level agreements (OLAs)

12.2.1.2 Capacity Management

TABLE 25: CAPACITY MANAGEMENT

Key Function	<ul style="list-style-type: none"> Ensure that the capacity of IT infrastructure and related services are able to deliver on the agreed service level targets
Participants	OISS, OIS, OCTS Directors, IT Specialist
Input	Business requirements for network bandwidth and infrastructure component capacity; data on usage of network and hardware/software components
Output	Technology and management reports to support: <ol style="list-style-type: none"> Provisioning of capacity to support business requirements Ongoing capacity performance models

12.2.1.3 Availability Management

TABLE 26: AVAILABILITY MANAGEMENT

Key Function	<ul style="list-style-type: none"> Forecast, establish, and manage IT infrastructure and related services availability Ensure all IT infrastructure and related services are appropriate
--------------	--

	for the agreed upon service level targets
Participants	OISS, OIS, OCTS Directors, OCIO Managers, IT Operations Manager, IT Specialist
Input	Service level agreements; business impact; risk management analysis
Output	Reduced risks for maintaining high availability for: <ol style="list-style-type: none"> 1. Reliability 2. Maintainability 3. Serviceability

12.2.1.4 IT Service Continuity Management

TABLE 27: IT SERVICE CONTINUITY MANAGEMENT

Key Function	<ul style="list-style-type: none"> • Manage risks from disaster events that may seriously impact IT infrastructure and related services and help ensure minimum agreed upon service level agreements can be met • Plan for the recovery of IT infrastructure and related services
Participants	OISS, OIS, OCTS Directors, OIS Directors, IT Operations Manager, IT Specialist
Input	Business requirements; disaster recovery plans; security information; network diagrams
Output	Plans and policies to manage risk reduction measures and recovery options for IT infrastructure: <ol style="list-style-type: none"> 1. Risk reduction 2. Recovery options

12.2.1.5 Information Security Management

TABLE 28: INFORMATION SECURITY MANAGEMENT

Key Function	<ul style="list-style-type: none"> • Align IT infrastructure security with business security and ensure that information security is managed in all systems and processes
Participants	OISS, OIS, OCTS Directors, CISO, IT Security Manager, IT Security Specialist, IT Operations Manager, IT Specialist
Input	Information access, usage approvals, and reports; security and breach policies

Output	1. Controls and metrics for policy enforcement
--------	--

12.2.1.6 IT Architecture Management

TABLE 29: IT ARCHITECTURE MANAGEMENT

Key Function	<ul style="list-style-type: none"> Define a blueprint for the future of the technological landscape, aligning the IT infrastructure and related services with business requirements
Participants	OISS, OIS, OCTS Directors, Chief Architect, IT Operations Manager, IT Specialist
Input	Strategic plans; current state architecture; processes and standards; system inventory
Output	1. Strategic blueprint of the technological landscape

12.2.1.7 Supplier Management

TABLE 30: SUPPLIER MANAGEMENT

Key Function	<ul style="list-style-type: none"> Ensure all contracts with suppliers meet the needs of the business and that all suppliers meet their contractual commitments
Participants	OISS, OIS, OCTS Directors, IT Specialist, Procurement Specialists
Input	Purchase orders; contracts; SLAs, OLAs
Output	<ol style="list-style-type: none"> Evaluation and establishment of new suppliers and contracts Review and outcome of contractual obligations of suppliers

12.2.1.8 Service Portfolio Management

TABLE 31: SERVICE PORTFOLIO MANAGEMENT

Key Function	<ul style="list-style-type: none"> To decide on a strategy to serve OCIO's customers and develop service offerings and capabilities
Participants	CISO, OISS Directors, OCTS Directors, Chief Architect, Program Managers
Input	Strategic goals, IT strategic goals, program goals and objectives, service offerings

Output	<ol style="list-style-type: none"> 1. Strategic service assessment of current service offerings and program needs 2. Service strategy definition to the define the overall goals OCIO should pursue in its development and identify what services will be offered to the programs 3. Service portfolio update based on changes identified in the service assessment and service strategy definition 4. Strategic planning to define, execute, and measure the service strategy
--------	--

12.2.1.9

12.2.1.10 *IT Financial and Performance Management*

TABLE 32: IT FINANCIAL AND PERFORMANCE MANAGEMENT

Key Function	<ul style="list-style-type: none"> • To manage OCIO’s budgeting, accounting, and charging requirements for services provided
Participants	OISS Directors, OCTS Directors, OCFO Directors
Input	Service catalog, Costs, SLAs, OLAs
Output	<ol style="list-style-type: none"> 5. Definition of structures for the management of financial planning data and costs as well as allocation of costs to services 6. Financial planning to determine and allocate the required financial resources over a planning period 7. Financial analysis and reporting of the structure of service provisioning cost and benefits 8. Financial management metrics to measure and assess performance

12.2.2 Delivery Management

12.2.2.1 *Change Management*

TABLE 33: CHANGE MANAGEMENT

Key Function	<ul style="list-style-type: none"> • Ensure that changes are recorded, evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner. • Ensure that standardized methods are used for the efficient and prompt handling of all changes, that all changes are recorded
--------------	---

	in the Configuration Management System and that overall business risk is optimized
Participants	OISS, OIS, OCTS Directors, IT Operations Manager
Input	Requests for change
Output	<ol style="list-style-type: none"> 1. Change record 2. Change schedule 3. Post implementation review

12.2.2.2 Configuration Management

TABLE 34: CONFIGURATION MANAGEMENT

Key Function	<ul style="list-style-type: none"> • Provide accurate information and control across all assets and relationships that make up the SBA's infrastructure • Identify, control and account for service assets and configuration items, protecting and ensuring their integrity across the service life cycle
Participants	OISS, OIS, OCTS, Project Manager, IT Operations Manager, IT Specialist
Input	Requirements and specifications about configuration items
Output	<ol style="list-style-type: none"> 1. Updates made into documents or spreadsheets to maintain the configuration management

12.2.2.3 Transition Planning and Support

TABLE 35: TRANSITION PLANNING AND SUPPORT

Key Function	<ul style="list-style-type: none"> • Plan and coordinate resources to deploy a major release within the predicted cost, time, and quality estimates. • Identify, manage, and control the risks of failure and disruption across transition activities.
Participants	OISS, OIS, OCTS, Project Manager, IT Operations Manager, IT Specialist
Input	Project plan; project history log
Output	<ol style="list-style-type: none"> 1. Service Transition Report

12.2.2.4 Service Validation and Testing

TABLE 36: SERVICE VALIDATION AND TESTING

Key Function	<ul style="list-style-type: none"> • Provide objective evidence that the new/changed service supports the business requirements, including the agreed SLAs • Verify that IT operation is able to support the new service.
Participants	OISS, OIS, OCTS, OIS, IT Operations Manager, IT Security Manager, User
Input	Test build; development / installation / QA documentation; test script, test model
Output	<ol style="list-style-type: none"> 1. Test report 2. Service design validation report

12.2.2.5 Release Management

TABLE 37: RELEASE MANAGEMENT

Key Function	<ul style="list-style-type: none"> • Assemble and position all aspects of services into production and establish effective use of new or changed services • Plan, schedule and control the movement of release to test and live environments • Ensure that the integrity of the live environment is protected and that the correct components are released
Participants	OISS, OIS, OCTS, Project Manager, IT Operations Manager, IT Specialist
Input	Requests for change
Output	<ol style="list-style-type: none"> 1. Release record 2. Release policy 3. Release plan 4. System/application build with release changes

12.2.2.6 Service Desk

TABLE 38: SERVICE DESK

Key Function	<ul style="list-style-type: none"> • Provide a single point of contact for the business to manages incidents, problems, and service requests • Record changes and provide status updates on incidents, problems, and services along as well as handle complaints and improve customer service
Participants	OISS, OIS, OCTS, Help Desk Manager, Help Desk Specialist
Input	Incident records; service request records
Output	<ol style="list-style-type: none"> 1. Resolution and closure of incidents and service requests as well as reports 2. Communication to users to inform them about service failures

12.2.3 Technology Management

12.2.3.1 Event Management

TABLE 39: EVENT MANAGEMENT

Key Function	<ul style="list-style-type: none"> • Monitoring and notifications from IT infrastructure components for normal activities and service disruptions • Filtering, categorizing, and responding to events
Participants	OISS, OIS, OCTS, IT Operations Manager, IT Specialist
Input	Service disruption notifications; normal activity notifications
Output	<p>Response to an event and determine appropriate actions. Categorize event as one of the following:</p> <ol style="list-style-type: none"> 1. Incident 2. Problem 3. Change 4. Normal activity

12.2.3.2 Incident Management

TABLE 40: INCIDENT MANAGEMENT

Key Function	<ul style="list-style-type: none"> To manage the lifecycle of incidents Restore IT infrastructure services to users as quickly as possible and minimize the adverse impact to business operations
Participants	OISS, OIS, OCTS, Help Desk Manager, Help Desk Specialist
Input	Incidents; service disruption notifications
Output	<ol style="list-style-type: none"> Resolution and closure of incidents as well as incident management reports Communication to users to inform them about service failures. If the correction to the root cause of an incident is not possible, a Problem Record is created and the error correction is transferred to the Problem Management process

12.2.3.3 Request Fulfillment

TABLE 41: REQUEST FULFILLMENT

Key Function	<ul style="list-style-type: none"> Fulfill service requests (minor, standard changes) or requests for information
Participants	OISS, OIS, OCTS, Help Desk Manager, Help Desk Specialist
Input	Service requests
Output	<ol style="list-style-type: none"> Resolution and closure of service requests as well as request fulfillment reports

12.2.3.4 Access Management

TABLE 42: ACCESS MANAGEMENT

Key Function	<ul style="list-style-type: none"> • Provide the rights for users to access an IT infrastructure service or group of services, while preventing access for non-authorized users • Execute policies defined in the IT Security Management process
Participants	OISS, OIS, OCTS, OIS, Help Desk Manager, Help Desk Specialist, IT Operations Manager, IT Specialist
Input	Incident records; data collected by other service management processes to identify trends or significant problems
Output	<ol style="list-style-type: none"> 1. Managing and maintaining appropriate user access privileges and rights based on roles and responsibilities 2. Managing user requests by appropriately maintain and granting user privileges and rights

12.2.3.5 Problem Management

TABLE 43: PROBLEM MANAGEMENT

Key Function	<ul style="list-style-type: none"> • Prevent problems and resulting incidents from happening, eliminate recurring incidents, and minimize impact of incidents that can be prevented • Diagnosing cause of incidents, determining the resolution, and ensuring that the resolution is implemented
Participants	OISS, OIS, OCTS, Help Desk Manager, IT Operations Manager, IT Specialist
Input	Incident records; problem records
Output	<ol style="list-style-type: none"> 1. Resolution and closure of problems 2. Review of major problems to prevent reoccurrence and verify elimination of problems 3. Communication to stakeholders of outstanding problems, status, and any existing workarounds

12.2.3.6 IT Operations Management

TABLE 44: IT OPERATIONS MANAGEMENT

Key Function	<ul style="list-style-type: none"> • Monitor and control IT infrastructure and related services • Execution of routine daily tasks (e.g., job scheduling, backup/restore activities, routine maintenance) related to the operation of infrastructure components and activities
Participants	IT Operations Manager, IT Specialist
Input	Monitoring notifications and logs; schedule of daily maintenance and support activities
Output	<ol style="list-style-type: none"> 1. Daily maintenance and support related to the operation of infrastructure components and activities 2. Execution of scheduled maintenance activities

12.2.3.7 IT Facilities Management

TABLE 45: IT FACILITIES MANAGEMENT

Key Function	<ul style="list-style-type: none"> • Manage the data center and physical environment (e.g., power and cooling, building access management, environmental monitoring) where the IT infrastructure is hosted
Participants	OISS, OIS, OCTS, IT Operations Manager, IT Specialist, Data Center Facilities Manager
Input	Monitoring notification and logs; user access roles and privileges
Output	<ol style="list-style-type: none"> 1. Daily maintenance and support related to the operation of the facilities 2. Execution of scheduled facilities maintenance activities and closure of facilities failures/requests

12.2.4 Infrastructure Business Process to BRM Business Service Mapping

Table 46 below maps the operational business architecture processes, as outlined above, to the appropriate BRM business services.

TABLE 46: BUSINESS PROCESS TO BUSINESS SERVICE MAPPING

Business Process	Business Service
Service Level Management	(139) IT Infrastructure Maintenance (263) System & Network Monitoring
Capacity Management	(139) IT Infrastructure Maintenance (263) System & Network Monitoring
Availability Management	(139) IT Infrastructure Maintenance (263) System & Network Monitoring
IT Service Continuity Management	(094) Contingency Planning (095) Continuity of Operations (096) Service Recovery
Information Security Management	(140) Information Security
IT Architecture Management	(139) IT Infrastructure Maintenance
Supplier Management	(119) Facilities, Fleet, and Equipment Management
Change Management	(139) IT Infrastructure Maintenance (137) Lifecycle Change Management
Configuration Management	(139) IT Infrastructure Maintenance (137) Lifecycle Change Management
Transition Planning and Support	(139) IT Infrastructure Maintenance (137) Lifecycle Change Management
Release Management	(139) IT Infrastructure Maintenance (137) Lifecycle Change Management
Service Desk	(120) Help Desk Services

Business Process	Business Service
Service Validation and Testing	(139) IT Infrastructure Maintenance
Event Management	(120) Help Desk Services (139) IT Infrastructure Maintenance (263) System & Network Monitoring
Incident Management	(120) Help Desk Services (263) System & Network Monitoring
Request Fulfillment	(120) Help Desk Services
Access Management	(120) Help Desk Services (140) Information Security
Problem Management	(120) Help Desk Services (263) System & Network Monitoring
IT Operations Management	(263) System & Network Monitoring (139) IT Infrastructure Maintenance (140) Information Security
IT Facilities Management	(119) Facilities, Fleet, and Equipment Management

12.3 IT Infrastructure Current Investments

OCIO has invested in several ongoing initiatives, as described in their FY2010 Exhibit 300 and 53s, outlined in Table 47: OCIO Infrastructure Current Investments.

TABLE 47: OCIO INFRASTRUCTURE CURRENT INVESTMENTS

Funded Initiative	Description	Status
OATI UPI Code: 028-00-02-00- 01-7001-00	This is the consolidated 300 for all of the SBA's common user systems, communication, and computing, which encompasses office automation, infrastructure, networks, and telecom. It is comprised of sub-investments in MSSS, TSS, and EUSS as described in the subsequent rows.	Most of the funds in OATI are for operations and maintenance, with little DME.
MSSS	This investment is a subset of OATI. It supports mainframe and servers, including	

Funded Initiative	Description	Status
	hosting contracts for the Disaster Credit Management System (DCMS) supported by ODA.	
TSS	This investment is a subset of OATI. It supports telecom services (data and voice) and projects that support common user systems and communications.	
EUSS	This investment is a subset of OATI. It supports Help Desk services and desktop support.	
IT Security Program UPI Code 028-00-01-06-02-7002-00	This investment supports the SBA's IT Security Program within OCIO, including security solutions, incident response, training, and FISMA requirements.	Exhibit 53 submitted.
EA Program UPI Code 028-00-03-00-02-8001-00	While not directly part of the IT Infrastructure, the EA Program is a critical component of planning, including for the infrastructure.	Exhibit 53 submitted.

12.4 Business Architecture Key Observations

Optimization of the SBA's infrastructure is affected by several critical business and performance considerations:

1. Metrics - The SBA does not capture the data necessary to develop, track and report on key IT infrastructure performance metrics. Without proper metrics, the SBA cannot properly manage its infrastructure, effectively measure performance, and truly identify priority areas.
2. Lack of Standardized Processes – IT Infrastructure design, deployment, and management are commodity type services with standard processes (i.e., as defined by ITIL, for example). Several of these processes are performed at an immature level or missing at SBA:

Immature

- IT Financial and Performance/Service Portfolio Management – A formal level of processes and procedures to financially manage, budget, and plan for the acquisition of IT infrastructure assets as well as prioritize the need for related services can be better enforced and executed.
- Service Level Management - The SBA does not have formal SLAs or OLAs with its key stakeholders. This prevents the SBA from documenting or justifying the

performance of its infrastructure and leads to frustration on the part of program offices seeking IT support.

- Capacity Management - The SBA does not have formalized processes for capacity management and planning or developing projections for future capacity requirements. This can result in ad hoc purchases to address immediate and urgent issues, but prevents a coherent long term integrated infrastructure plan to support future growth.
- Availability Management – Without SLAs, it is impossible to determine whether the infrastructure has adequate availability to meet needed service levels. In addition, there is no forecasting of future availability projections.
- IT Service Continuity Management – The IT infrastructure and related services operated by OCIO at SBA HQ do not have a formal contingency site and remote DR strategy. In the event of a disaster, ODA may not be able to meet the business needs of its stakeholders and provide continuity of service for its messaging infrastructure (i.e., email). A business impact analysis (BIA) and DR strategy can be conducted in order to identify recovery objectives for the messaging infrastructure.
- Change Management – While the SBA has strict change and configuration management in some areas, it is inconsistent across the enterprise. Formal levels of governance and enforcement need to be adhered to.
- Service Desk/Request Fulfillment/Incident Management/Problem Management – The SBA has inconsistent processes for logging, tracking, and resolving help desk calls and requests. Some users/program offices follow “official” processes and go through the Help Desk, but others go directly to the Help Desk Specialist who they know will provide assistance. As a result, the actual data to demonstrate Help Desk performance is absent.

Missing

- Service Catalogue Management – SBA does appear to have formal processes where a single, consistent inventory of IT infrastructure related services with their availability, details, and status is maintained and widely available to the business and stakeholders. A centralized catalogue is missing or inconsistent documentation is maintained.

13 Appendix I: Current State System Architecture

13.1 Current State Service Component Architecture

The mapping of service components and the business services of IT Infrastructure they support are provided in Table 48.

TABLE 48: MAPPING OF BUSINESS FUNCTIONS TO SERVICE COMPONENTS AND SRM ALIGNMENT

Service Domain	Service Type	Service Components	Business Services
Customer Services	(701) Customer Relation Management	(510) Call Center Management	(120) Help Desk Services
Customer Services	(701) Customer Relation Management	(511) Customer Analytics	(120) Help Desk Services
Customer Services	(701) Customer Relation Management	(515) Customer/Account Management	(120) Help Desk Services
Customer Services	(701) Customer Relation Management	(516) Customer and Profile Management	(120) Help Desk Services
Customer Services	(701) Customer Relation Management	(518) Customer Feedback	(120) Help Desk Services
Customer Services	(701) Customer Relation Management	(519) Surveys	(120) Help Desk Services
Customer Services	(703) Customer Initiated Assistance	(523) Online Help	(120) Help Desk Services
Customer Services	(703) Customer Initiated Assistance	(528) Assistance Request	(120) Help Desk Services
Business Management Services	(721) Management of Process	(535) Change Management	(137) Lifecycle / Change Management
Business Management Services	(721) Management of Process	(536) Configuration Management	(137) Lifecycle / Change Management
Business Management Services	(722) Organizational Management	(544) Network Management	(139) IT Infrastructure Maintenance

Service Domain	Service Type	Service Components	Business Services
			263 System and Network Monitoring
Back Office Services	(754) Asset / Material Management	(636) Computer / Automation Management	(119) Facilities, Fleet and Equipment Management
Support Services	(761) Security	(648) Identification and Authentication	(140) Information Security
Support Services	(761) Security	(649) Access Control	(140) Information Security
Support Services	(761) Security	(652) Intrusion Prevention	(140) Information Security
Support Services	(761) Security	(653) Intrusion Detection	(140) Information Security
Support Services	(761) Security	(654) Incident Response	(139) IT Infrastructure Maintenance (140) Information Security
Support Services	(761) Security	(655) Audit Trail Capture and Analysis	(140) Information Security
Support Services	(761) Security	(656) Certification and Accreditation	(140) Information Security
Support Services	(761) Security	(657) FISMA Management and Reporting	(140) Information Security
Support Services	(761) Security	(658) Virus Protection	(140) Information Security
Support Services	(762) Collaboration	(659) Email	(139) IT Infrastructure Maintenance
Support Services	(762) Collaboration	(661) Document Library	(139) IT Infrastructure Maintenance
Support Services	(764) Communication	(670) Audio Conferencing	(139) IT Infrastructure

Service Domain	Service Type	Service Components	Business Services
			Maintenance
Support Services	(764) Communication	(671) Video Conferencing	(139) IT Infrastructure Maintenance
Support Services	(764) Communication	(672) Event / News Management	(139) IT Infrastructure Maintenance
Support Services	(764) Communication	(674) Computer / Telephony Integration	(139) IT Infrastructure Maintenance
Support Services	(764) Communication	(675) Voice Communication	(139) IT Infrastructure Maintenance
Support Services	(765) Systems Management	(676) License Management	(119) Facilities, Fleet and Equipment Management (139) IT Infrastructure Maintenance
Support Services	(765) Systems Management	(677) Remote Systems Control	(094) Contingency Planning (095) Continuity of Operations (096) Service Recovery (139) IT Infrastructure Maintenance (263) System and Network Monitoring
Support Services	(765) Systems Management	(678) System Resource Monitoring	(139) IT Infrastructure Maintenance (263) System and Network Monitoring

Service Domain	Service Type	Service Components	Business Services
Support Services	(765) Systems Management	(680) Issue Tracking	(120) Help Desk Services (139) IT Infrastructure Maintenance

13.1.1 Service Component Architecture Key Observations

1. Reuse and Sharing of IT Infrastructure Services - ODA has different operating standards and service level requirements than OCIO. ODA uses both OCIO and its own IT services to support the infrastructure. There are opportunities to consolidate duplicate service components between OCIO and ODA, such as email and computer management, and share these components within the SBA.
2. Formalize Service Level Agreements - Most of the OCIO service components do not have formally defined Service Level Agreements (SLA). This is an obstacle for segments that have strict obligations to their stakeholders, such as ODA, to adapt the service components provided by OCIO or other segments. The commitment to formal SLAs will promote the reuse and sharing of enterprise-wide service components.
3. Strategy for the Next Generation Data Center Services – The SBA’s HQ Data Center and the Denver Network Operations Center (DNOC), currently host network operations, business applications, SBA websites, and other critical network functions. There are operational constraints that limit their capacity and expandability. They do not meet certain standards (e.g., remote DR replication solution, full redundancy, optimal physical environment, etc.) in order to support the SBA’s Continuity of Operations Plan (COOP) or the mission-critical IT systems. It is very important to have a strategy for the next generation of data center services.
4. Process Compliance – The SBA’s IT Infrastructure may have policies or mandates that impact processes in other segments. For example, the IT security requirements should be part of all procurement and development processes. Existing processes should be assessed and processes revised to ensure the policy compliance.
5. Alignment and Integration - Some of the IT infrastructure initiatives may have impacts on other initiatives. For example, initiatives such as IPv6, Network Analysis and Modernization, IT Security Framework, and HSPD-12 may impact each other’s implementation. The SBA may need to extend the role of a Configuration Control Board (CCB), Technical Review Board (TRB), or Business Technology Investment Committee (BTIC) to facilitate the communication and resolve potential conflicts in design, architecture, and project sequencing.

13.2 Current State Data Architecture

The role of the IT Infrastructure segment is to provide support to the operational environments of business-driven segments within SBA. The major components of this segment are hardware, network equipment, and supporting software. The software components within this segment are all commercial off-the-shelf (COTS) software packages that have self-contained databases and do not rely on other systems to perform their functions.

Since the IT Infrastructure segment pertains to hardware/networking equipment and software to support operations, data architecture will not be part of this segment architecture. Interoperability with the utilization of SOA and the use of data warehouses and marts will be addressed in the IT Information Sharing segment architecture, which will include components supporting data and knowledge management as well as capabilities for ad-hoc reporting and search.

13.3 Current State Technical Architecture

The technical architecture provides a view into the key hardware and network technologies that provide the infrastructure for the services components.

Table 49 provides a mapping of the services and the supporting key technologies.

TABLE 49: MAP OF SERVICE COMPONENTS (SRM) WITH THE TECHNOLOGY COMPONENTS

Service Component	Technology
(510) Call Center Management	CA Unicenter Service Desk
(528) Assistance Request	CA Unicenter Service Desk
(535) Change Management	NETPRO - Configuration & Change Management Software License & Maintenance, Excel
(536) Configuration Management	NETPRO - Configuration & Change Management Software License & Maintenance, Excel
(544) Network Management	Internet Access, Hosting Service, Internet Protocol Version 6 (IPv6) Maintenance, WAN – Internet Protocol (IP), Big-IP Load Balancer
(636) Computer / Automation Management	CA Unicenter Service Desk
(649) Access Control	NetVersant - LAN Room Security access cards and Readers, Remote Access / Tokens, Juniper NetScreen VPN/Firewall
(652) Intrusion Prevention	NetSec Verizon, NetForensics
(653) Intrusion Detection	NetSec Verizon, NetForensics
(654) Incident Response	NetSec Verizon, NetForensics, Spectrum
(655) Audit Trail Capture and Analysis	NetForensics, UNIX, Internet Monitoring
(657) FISMA Management and Reporting	NetForensics, MS Word, MS Excel
(658) Virus Protection	McAfee - Anti Virus Software License & Maintenance
(659) Email	Intelligence Communications Solutions - Blackberry technology support, Message One - Blackberry Failover Software License & Maintenance, MX Logic - Anti Spam Software License & Maintenance, Yancy Assoc. - E-mail Archival
(670) Audio Conferencing	Teleconference Service
(674) Computer / Telephony Integration	WAN Support – NOC, Cisco Routers

(675) Voice Communication	Desk Top Fax, Fax Operator, Fax Service, Network Support, Telephone Customer Service / Maintenance Support, PDA Blackberry & Cellular, Local Telephone Calling Service, Long Distance Calling Service, Monitor Telecommunication Services, Telephone Dial Tone, Voicemail
(676) License Management	NETPRO - Configuration & Change Management Software License & Maintenance, Excel
(677) Remote Systems Control	CA Unicenter Service Desk
(678) System Resource Monitoring	Syslog

Table 50 provides a mapping of the technology components with the Technology Reference Model (TRM).

TABLE 50: MAP OF THE TECHNOLOGY COMPONENTS WITH THE TRM

Service Area	Service Category	Service Standard	Technology
Service Access & Delivery	Access Channels	(851) Wireless / PDA	PDA Blackberry & Cellular
		(852) Collaboration / Communications	Teleconference Service, Desk Top Fax, Fax Operator, Fax Service, Network Support, Telephone Customer Service / Maintenance Support, NETPRO - Configuration & Change Management Software License & Maintenance, Spectrum

Service Area	Service Category	Service Standard	Technology	
	Delivery Channels	(854) Internet	Internet Access, TCP/IP	
		(855) Intranet	TCP/IP	
		(857) Peer to Peer (P2P)	CA Unicenter Service Desk	
		(858) Virtual Private Network (VPN)	CA Unicenter Service Desk Remote Access / Tokens, Juniper NetScreen VPN/Firewall	
	Service Requirements	(859) Legislative / Compliance	Hosting Service, Internet Monitoring	
		(861) Hosting	Internal, External	
	Service Transport	(862) Supporting Network Services	WAN Support - NOC	
		(863) Service Transport	TCP / IPv4, SMTP	
	Service Platform and Infrastructure	Support Platforms	(865) Independent Platform	Linux
			(866) Dependent Platform	Windows 2003, UNIX, Mainframe
Delivery Servers		(871) Web Servers	Apache, IIS	
Hardware / Infrastructure		(877) Servers / Computers	Windows, UNIX, Mainframe	
		(878) Embedded Technology Devices	Disk Array, CPU, RAM	
		(879) Peripherals	Printer, Scanner	
		(880) Wide Area Network (WAN)	WAN - Internet Protocol (IP)	
(881) Local Area Network (LAN)	Capital Computer Solutions - BPA - Micro Computer			

Service Area	Service Category	Service Standard	Technology
			Equipment Maintenance Supplies, NETPRO - Configuration & Change Management Software License & Maintenance, NetVersant - LAN Room Security access cards and Readers, McAfee - Anti Virus Software License & Maintenance, Intelligence Communications Solutions - Blackberry technology support, Message One - Blackberry Failover Software License & Maintenance, MX Logic - Anti Spam Software License & Maintenance, Yancy Assoc. - E- mail Archival, NTVI - Infrastructure Support LAN & Help Desk
		(882) Network Devices / Standards	Cisco Routers, Local Telephone Calling Service, Long Distance Calling Service, Monitor

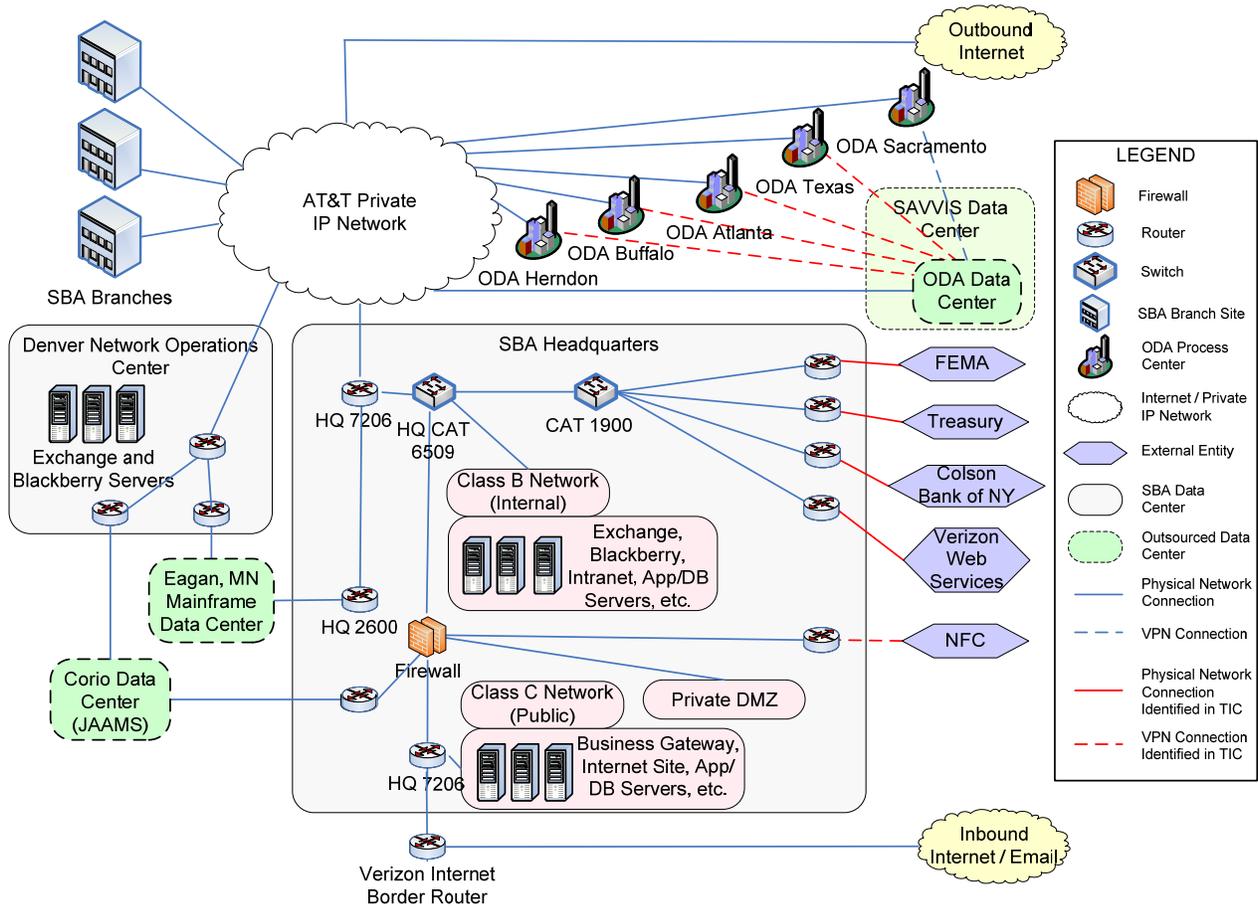
Service Area	Service Category	Service Standard	Technology
			Telecommunication Services, Telephone Dial Tone, Voicemail, Big IP Load Balancer, Firewall
Component Framework	Security	(884) Certificates / Digital Signatures	SSL
		(885) Supporting Security Services	Security Operations Center, SAML

13.3.1 Network Infrastructure

The SBA network is comprised of the following operational entities:

- Three outsourced data centers for DCMS, Joint Accounting Administrative Management System (JAAMS), and mainframe systems.
- Data center at headquarters
- Denver network operations center (DNOC)
- Processing centers and field offices

Figure 13 depicts the current state network infrastructure. It is intended to provide a high-level, simplified logical view of the SBA network with connections to key elements, as described below.

FIGURE 13: SBA CURRENT STATE NETWORK INFRASTRUCTURE


Local Area Network

The local area networks (LANs) at all SBA sites connect to the AT&T private IP network. The LAN at outsourced data centers connect to the SBA Headquarters LAN, Denver Network Operations Center LAN, or the private IT network.

Inbound Internet Connectivity

The inbound internet is served by Verizon, which connects to SBA Headquarters. It serves all incoming public internet traffic into the SBA network, including email, access to SBA websites, and applications.

Outbound Internet Connectivity

The outbound internet is served by AT&T, which connects to the Dallas hosting center. All outbound internet traffic originating from SBA sites is funneled through the AT&T private IP network into the Dallas hosting center, and then goes to the public internet.

SBA also has network connections to partners in government agencies, banks, and vendors. They all connect to Headquarters through a Virtual Private Network (VPN) or dedicated network.

There are some point-to-point network connections between certain sites, such as the VPN connection between ODA Herndon to the ODA data center. These connections could either serve as a redundant or alternative path to the private IP network to provide better network bandwidth.

The sections below provide information on the current state architecture and observations with the Network Analysis and Modernization, Networkx, TIC, HSPD-12, IPv6, Remote DR Infrastructure, Data Center, IT Security, and SOA initiatives.

13.3.2 Network Analysis and Modernization Observations

OCIO is undergoing a network health initiative to examine network usage and capacity in order to identify bottlenecks. The outcome of the initiative will help SBA to balance its network bandwidth and identify opportunities for upgrades and network topology design. An initial outcome of the analysis is the use of Voice over IP (VoIP) technology, which has improved and matured over years. Adapting the technology could result in significant cost savings for SBA.

OCIO is performing an evaluation of VoIP technology and will pilot VoIP in FY 2010. The existing network infrastructure will be leveraged to carry both data and voice. The network capacity requirement for VoIP is relatively small compared to data communication requirements. Therefore, the impact on the network infrastructure is expected to be minimal.

13.3.3 Networkx Observations

Networkx is the new government wide contract administered by GSA that replaces FTS2001 for telecom services. All agencies will have to transition to Networkx by 2010. This initiative is mainly focused on the procurement of telecom service contracts in order to realize cost savings for the Agency. Replacing the telecom service providers will not cause major impacts to the existing network infrastructure, including its topology, operations, or security measures.

13.3.4 TIC Observations

The purpose for the TIC initiative is to minimize the connections between the SBA network and the internet to ensure better security control and potential cost savings. In May 2008, OCIO identified 14 connections that have implications for TIC, as outlined in Table 51.

TABLE 51: TIC CONNECTIONS

ID	Name of connection	SBA Office	Type of Connection (approx size)	Bureau / SubAgency Supported by connection	Target Consolidated Environment		
					Target connections	Procurement Vehicle	Date of completed migration
1	VPN (DCMS)	ODA Herndon	45MB	SBA/ODA			
2	VPN	ODA	1.5 MB	SBA/ODA			



ID	Name of connection	SBA Office	Type of Connection (approx size)	Bureau / SubAgency Supported by connection	Target Consolidated Environment		
					Target connections	Procurement Vehicle	Date of completed migration
	(DCMS)	Buffalo					
3	VPN (DCMS)	ODA Atlanta	1.5 MB	SBA/ODA	Cloud	P.O.	
4	VPN (DCMS)	ODA Texas	12MB	SBA/ODA			
5	CTHTCA2 2N00	ODA Sacramento	Full T1 1.5M X 1.5M	DCMS Ops Center	DCMS Ops Center	P.O.	9/2/2008
6	SBA Internet Access	SBA HQ	Full T3	SBA HQ	Cloud	Networx	5/31/2008
7	Email	SBA HQ	T3 6MB	SBA HQ	Cloud	Networx	5/31/2008
8	FEMA	SBA HQ		SBA/FEMA			
9	Verizon Web Services	SBA HQ (Steve Kuhns)	DSL	SBA HQ			
10	NFC	SBA HQ	56k	SBA/NFC			
11	Colson Services	SBA HQ		SBA/Bank of New York			
12	US Treasury	SBA HQ	56k	SBA/Treasury			
13	SRA VA	SBA HQ	56k				
14	Email	SBA Denver	T3 6MB	SBA Denver Finance	Cloud	Networx	5/31/2008

Four of these connections are converted to be TIC compliant. These include two SBA HQ connections, ODA Sacramento and SBA Denver. The Office of Communications Technology Services has also confirmed that the SRA VA connection no longer exists. The other nine connections are indicated as red lines in Figure 13. While some connections could be eliminated by increasing network bandwidth or redundant connections to the backbone, others

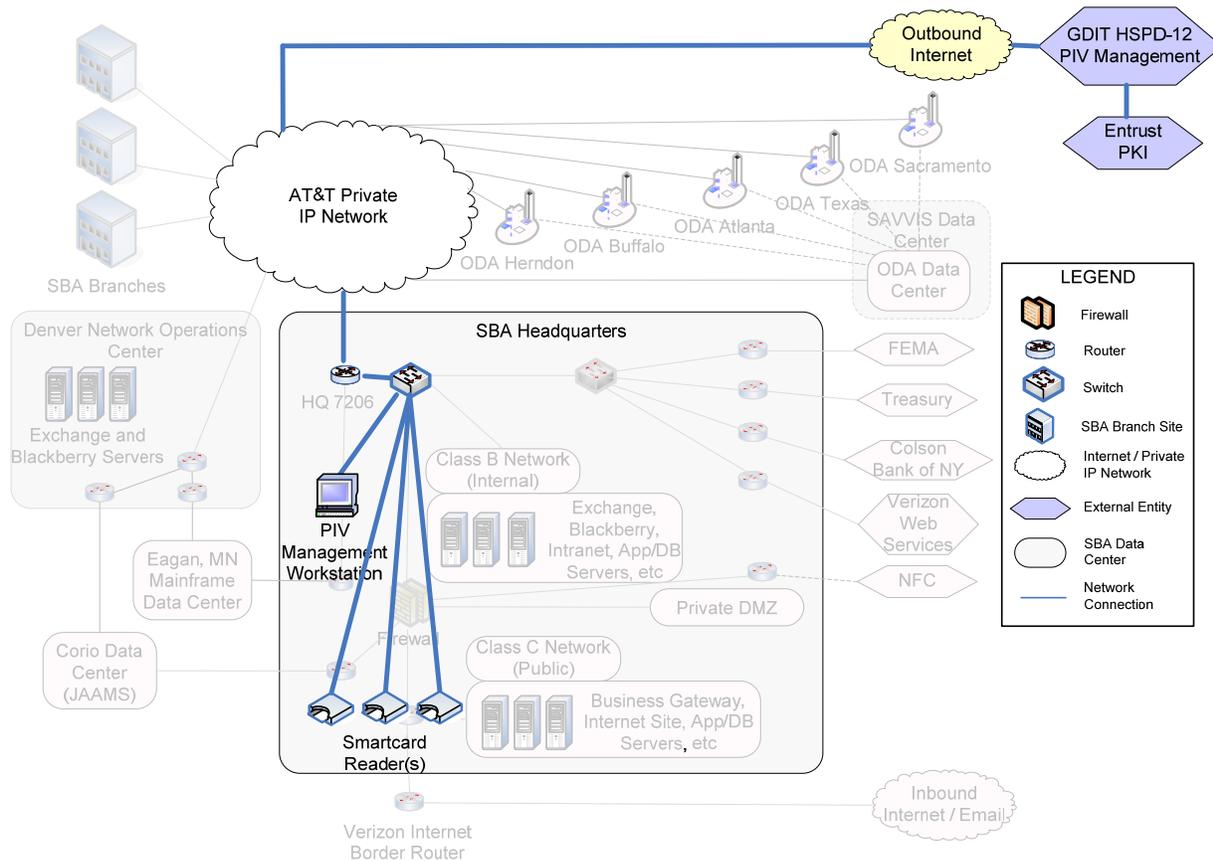
may be legitimate point-to-point connections to banks or other agencies that should continue to be maintained.

13.3.5 HSPD-12 Observations

SBA has no physical Public Key Infrastructure (PKI) for the HSPD-12 implementation. The personal identification verification (PIV) authentication services are hosted and managed by an outsourced vendor, General Dynamics IT (GDIT), so that SBA does not need to maintain its own PKI infrastructure. SBA only has work stations for general PIV card management, including the enrollment of cardholders and the issuance of the cards. Most of the system functions are enabled through web services with the backend services hosted at the shared service provider (GDIT). The work stations and PIV card readers use secure socket layer (SSL) channels over the standard internet to connect to the PIV servers at the shared service provider. There is no special requirement on the capacity or throughputs of the network connection with the PIV servers. However, delays and time outs during the use of PIV cards were observed. This is probably due to the network infrastructure (poor cabling) in the current SBA HQ building.

Figure 14 depicts how the PIV authentication services leverage the existing SBA network infrastructure to connect to the external PIV management services. The highlighted parts of the figure represent the HSPD-12 components and the network infrastructure it leverages.

FIGURE 14: PIV SERVICES LEVERAGING SBA NETWORK INFRASTRUCTURE



The short term objectives for HSPD-12 are to deploy the infrastructure and to increase the issuance of personal identification verification (PIV) cards. With a potential full deployment, PIV cards could be leveraged for physical and logical access control. Beyond improved security, the HSPD-12 initiative has great opportunities to add value to other initiatives or systems, including:

- Cross-agency authentication of PIV card and access control for all federal employees and contractors;
- Use of portable PIV card readers during emergencies to track and account for employees and contractors;
- Leverage HSPD-12 platform to replace security token or other IT security solutions; a
- Integrate HSPD-12 platform with network logon and enterprise application sign-on to promote single sign-on capabilities.

A potential enterprise-wide identity vault, which the HSPD-12 initiative falls under, could standardize the process for identity management and serve as the master data repository to synchronize other data services, such as telephone directories and personnel profiles.

13.3.6 IPv6 Observations

SBA has completed the OMB mandated IPv6 milestones in June 2008 by demonstrating the capability of IPv6 in a limited environment. SBA has also updated the hardware in its network infrastructure to be IPv6 compliant. However, most of the external stakeholders of SBA, including the banks, other federal agencies, and customers are not yet operating in IPv6. SBA cannot transition its network to an IPv6 operation until stakeholders are ready for the technology. Until the enterprise-wide IPv6 transition happens, there is no impact to the current network infrastructure.

As part of the planning efforts for the IPv6 transition, SBA will need to perform a full scale assessment on the enterprise applications in its IT portfolio for IPv6 compliance. The IPv6 transition may also have impacts on the network security, network topology, and overall network operations.

13.3.7 Remote Disaster Recovery Infrastructure Observations

SBA has its Exchange and Blackberry servers hosted at Headquarters and DNOC. The servers are mirror-configured with hot backup to provide the redundancy for disaster recovery.

Other enterprise-wide and public applications are hosted without the provision of redundancy in hardware or network infrastructure. Although the data centers may have a process for data backup, they are not qualified as disaster recovery infrastructure.

SBA has contracted a vendor to implement a small-scale remote disaster recovery infrastructure that provides five servers as redundancy for about twenty applications. That may help to ensure the continuous operations of the key SBA applications.

13.3.8 Data Center Observations

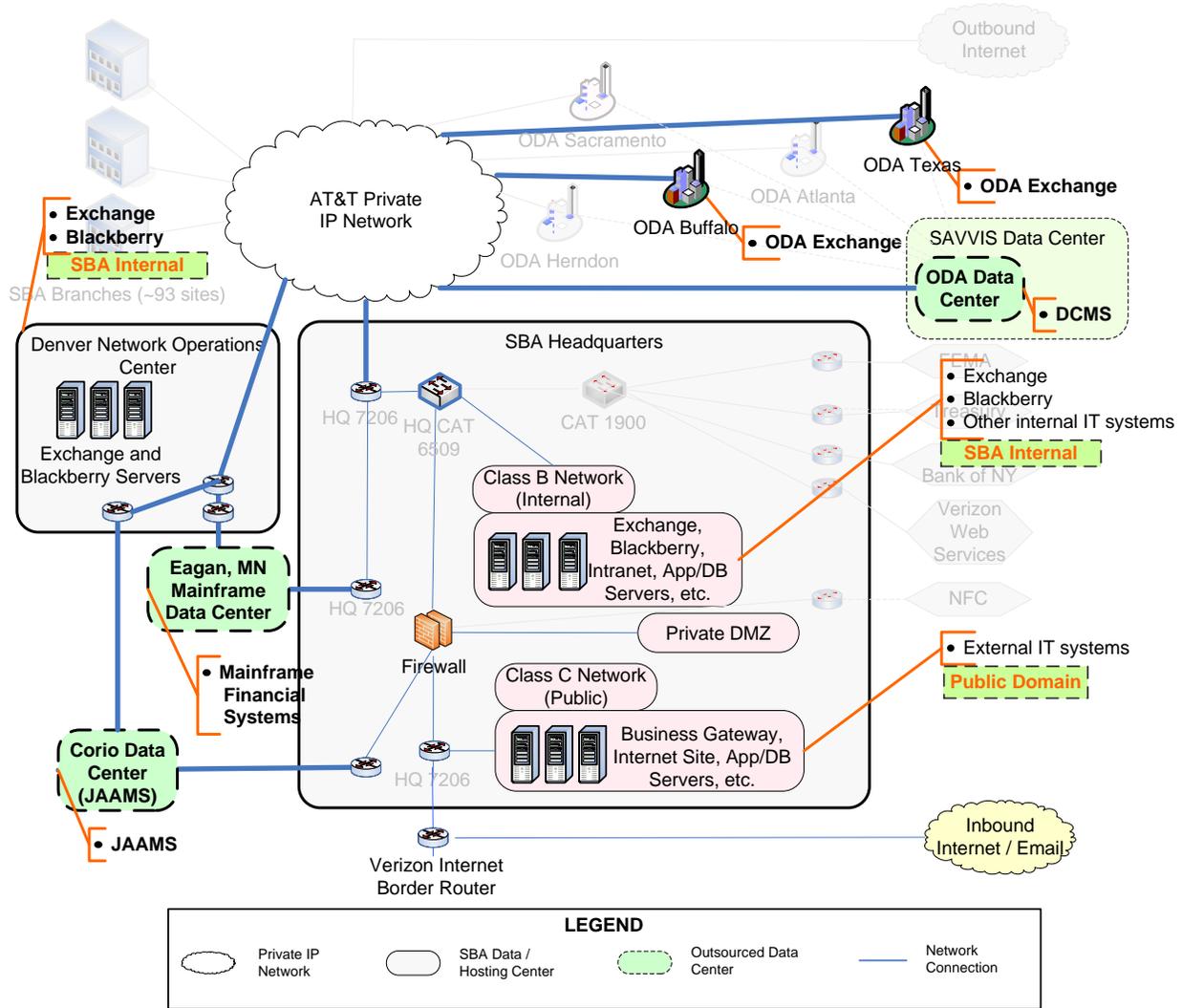
SBA's HQ Data Center hosts network operations, business applications and SBA websites. The Denver Network Operations Center (DNOC) serves many critical network functions for SBA field personnel. The DNOC also serves as an alternate facility for HQ network operations. Both facilities are in secure rooms and can only be accessed with a badge or entry code. Although the facilities may be compliant with SBA security standards, they may need improvements to meet more stringent data center security standards in the future. These facilities also have limits on capacity:

- DCMS has unusual availability demands beyond the capacity of the HQ data center and is hosted by a specialized vendor.

- The Corio/IBM data center hosts Joint Administrative Accounting Management System (JAAMS), the SBA financial system implemented with Oracle Federal Financial System.
- The Unisys data center at Eagan, Minnesota is hosting the legacy mainframe systems. The contract will expire on 2011.

Figure 15 depicts the Headquarters Data Center, Denver Network Operations Center, the outsourced ODA Data Center, Corio Data Center, and Eagan Data Center, and how they connect to the SBA network infrastructure. It also includes a brief list of applications hosted at each data center. The highlighted figure represents the data center components and the network infrastructure it leverages.

FIGURE 15: SBA DATA CENTERS AND NETWORK INFRASTRUCTURE



The HQ data center hosts dozens of internal and external business applications. However, the existing data center has significant constraints. Some mission critical business applications require a data center with additional capacity and functionality to support 24x7x365 uninterrupted services.

The SBA HQ data center provides services that support the program offices and organizations within SBA. However, there are no service level agreements (SLAs) between the data center and its clients. It is difficult to define the customer satisfaction level or measure the performance of the data center services without a mutually agreed SLA and performance measurement matrix.

The current state data center infrastructure does not provide necessary redundancy for key applications, other than Exchange and Blackberry. The Remote Disaster Recovery Infrastructure should be tightly integrated with the planning for a future data center.

13.3.9 IT Security Observations

One of the main goals for IT Security is to build a security operations center (SOC), which has recently been completed. It functions as a centralized data collector to gather information from the sensors or security checkpoints deployed on the existing IT infrastructure. The SOC will enable centralized logging and auditing as well as application and database intrusion detection for all field offices and headquarters. It will allow SBA to better monitor security threats and react to vulnerabilities as it further matures. In addition, the SOC could help ensure formal operational processes for incident management are followed and expand the incident response capability by integrating incident management between SBA field offices and headquarters.

13.3.10 SOA Observations

Within OCIO, applications and data are running on various platforms and siloed within each line of business and program. There are currently no application and data integration components in OCIO that promote reuse and sharing within a line of business or across lines of business. OISS and ODA currently develop ad hoc Web services to support communication with external parties or as needed, so their developers have some knowledge of technologies that help enable SOA. In addition, ODA is currently leveraging webMethods components for integration and messaging. Lessons learned and best practices could possibly be leveraged by OCIO from ODA's webMethods experience.

Even though OCIO and ODA have some experience with SOA-related technologies, SBA does not possess a true serviced based/modular approach to architecting and implementing technical solutions. Furthermore, the SBA technical architecture does not have the capabilities or infrastructure components that provide a foundation to enable an SOA delivery solution. Common SOA-related infrastructure technologies and components, such as a service registry/directory, enterprise service bus (ESB), and business process management systems (BPMS) are not present in the SBA enterprise.

In order to transition to SOA, SBA will have to undertake significant efforts, to develop a vision, high-level architecture, and strategy; define and implement an organizational foundation; define and implement a technical foundation; decompose processes into services; build services and composite applications; and operate the business with improved processes and services. These efforts along with governance, service lifecycle management, and metrics measurement throughout each step ensure continuous process improvement for delivery of an SOA capability. Further details and context to address these gaps will be provided in the target state IT Infrastructure segment architecture.

14 Appendix J: Documents Reviewed

The following represents the documents reviewed as part of the IT Infrastructure segment architecture analysis:

- SBA Strategic Plan FY 2008-2013
- SBA Performance Budget
- SBA IT Strategic Plan 2007-2011
- SBA Consolidated Five Year Plan Optimization Report August 2008
- SBA Enterprise Architecture Blueprint v2.04
- SBA EA Transition Plan v2.00
- FEA Practice Guidance, November 2007
- SBA Alignment and Integration of IPv6, TIC, and Network October 2008
- SBA Security Framework May 2008
- ITILOB Gartner Reports
 - Final Government-wide Data Analysis Report
 - SBA Data Analysis Report
 - SBA ODA Data Analysis Report
- ITILOB Common Solutions Document 2006
- FEA Consolidated Reference Model Document Version 2.3
- FEA Data Reference Model 2.0
- FSAM Segment Architecture Guidance and Templates
- SBA Exhibit 53s (FY10)
- SBA Exhibit 300s (FY10)
- www.sba.gov