



National Aeronautics and Space Administration

**Volume 3, NASA Enterprise Architecture:
Program Unique IT and Multi-Program /
Project IT Investment Category**

**Version # 3.0
August 25, 2004**

Table of Changes

Date of Change	Section(s) Affected	Brief Description of Change	Change Made By	Organization
December 22, 2003	Initial Version	Final Version 2.1	Chief Technology Officer, Code AO	NASA Office of the CIO
March 26, 2004	Minor editorial updates	Final Version 2.2	Chief Technology Officer, Code AO	NASA Office of the CIO
July 2, 2004	Minor editorial updates	Final Version 2.3	Chief Technology Officer, Office of the CIO	NASA Office of the CIO
August 3, 2004	Version 3 updates; updates to all content	Version 3.0 Draft	Bob Stauffer, Melissa McCarty	EA Core Team
August 25, 2004	Formatting	Version 3.0	Tressa Reaggle	EA Core Team

Document Outline

NASA Enterprise Architecture: Volume 1, Overall Architecture and Governance

Executive Overview

Introduction

The NASA Enterprise Architecture

NASA IT Strategy, Goals and Objectives

Summary

“To be” Directions

Appendix A: Enterprise Architecture RoadMap

Appendix B: The Bell South Lifecycle Model

NASA Enterprise Architecture: Volume 2, Office Automation, IT Infrastructure, and Telecommunications Investment Category

Introduction

Center “As-is” Technical Architectures

NASA Enterprise Architecture: Volume 3, Program Unique IT Multi-Program / Project IT Investment Category

Introduction

Program Unique IT “As-is” Architectures

NASA Enterprise Architecture: Volume 4, Structure and Strategies

Introduction

Structure of the NASA Enterprise Architecture

Office Automation, IT Infrastructure, and Telecommunications Investment Category - Technical Summary Description

Program Unique IT and Multi-Program / Project IT Investment Category – Technical Summary Descriptions

NASA Enterprise Architecture: Volume 5, NASA To-Be Architecture, Approach to Design and Implementation.

(Building Out the Service and Technical Reference Models)

Introduction

Structure of the NASA Enterprise Architecture

Office Automation, IT Infrastructure, and Telecommunications Investment Category - Technical Summary Description

Program Unique IT and Multi-Program / Project IT Investment Category – Technical Summary Descriptions

“To be” Directions

Summary

NASA Enterprise Architecture Volume 6: Policies and Procedures

Introduction

Summary Approach

Abbreviations and Acronyms

ADA	American with Disabilities Act
ACDS	Administrative Contacts Database System
ACS	Advisory Committee System
ACTS	Advisory Council Tracking System
ADM	Administrative
ADS	Art Database System
ADSC	Application Development Support Contract
ADSI	Active Directory Services Interface
AHS	Application Hosting Service
AHU	Air Handling Unit(s)
ALIS	Ames Locator Information Service
AMES or ARC	Ames Research Center
AMS	NASA Acquisition Management System
APD	Ames Policy Directive
API	Application Programming Interface
ARC	Ames Research Center
ARCLAN	Ames Research Center Local Area Network
ARRS	Agency Reimbursable Reporting System
ARS	Access Request System
ASAL	Administrative Services Address Labeling System
ATM	Asynchronous Transfer Mode
AV	Audio Visual
AWCS	Agency-Wide Coding Structure
BCP	Best Current Practices
BES	Blackberry Enterprise Server
BESS	Budget Execution Support System
BGP	Border Gateway Protocol
BNC	British Naval Connector
BPS	Budget Preparation System
BRI	Basic Rate Interface
BRIC	Knowledge Information Center-Code BR
BRT	Business and Restricted Technology
BUMS	Business Management System
CAD	Computer Aided Design
CADB	Copernicus Art Database (Test and Deploy)
Caltech	California Institute of Technology
CATS II	Corrective Action Tracking System
CATV	Cable Television
CBR	Constant Bit Rate
CBS	Chief Billing Systems
CBX	Central Branch Exchange
CCB	Configuration Control Board
CCC/Harvest	A change management tool by Platinum Technology
CCCB	Center level Configuration Control Board
CCMIS	Call Center Management Information System
CCSDS	Consultative Committee for Space Data
CCTV	Closed Circuit Television

CEE	Collaborative Engineering Environment
CEF	Central Engineering Files
CENTRX	Central Exchange
CFB-R506	Code CFB Reimbursable 506
CG	Character Generator
CI SSMM	Code CI Senior Staff Meeting Minutes
CIBS	Code CI Budget
CIFS	Common Internet File System
CIO	Chief Information Officer
CLASICS	Contact List and Special Interest Computing System
CMM	Capability Maturity Model
CMMS	Corrective Maintenance and Management System
CMOS	Complimentary Metal Oxide Semi-conductor
CMOTS	Career Management Office Tracking System
CMS	Correspondence Management System
CNE	Center Network Environment
COBRA	Cost/Obligations Budgeting Resource Allocation
Code CI - POCs	Point of Contact
Code R-POC	Code R - Point of Contact Database
CODECS	Coder Decoder
COFEDB	Centennial of Flight Event Database
CONG MAPS	Congressional Maps System
COPPA	Child Online Privacy Protection Act
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-The-Shelf
CRCS	Central Resources Control System
CRLF	Carriage Return / Line Feed
CS	Civil Service
CSDB	Customer Services DataBase
CSO	Computer Security Official
CSOC	Consolidated Space Operations Contract
CVS	A version management tool
DAR	Designated Agency Representative
DBA	Database Administrator
DBAT	Design, Build, Assemble, and Test
DCMS	Discrimination Complaints Management System
DDMS	Design Data Management System
DES	Data Encryption Standard
Designer	Toolset to model, generate and capture the requirements and design of applications
Destination Earth	What On Earth? ESE For Kids Only Game
DFMS	Direct Financial Management System
DFRC	Dryden Flight Research Center
DFRC	Dryden Flight Research Center
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name Systems
DNS	Domain Name Service

DoD	Department of Defense
DoS	Denial of Service
DSN	Defense Systems Network
DSN	Deep Space Network
DTA	Data Access Service
DTV	Digital Television
DV	Digital Video
DVD	Digital Video Disk
DVE	Digital Video Editor
EADS	EADS North America, Inc. PointSpan 6880 PABX switch manufacturer
EAWG	Enterprise Architecture Working Group
EBS	Emergency Broadcast System
ECAL-R	Enterprise Calendar-Code R
ECRS	Environmental Compliance and Restoration System
ECS	The Enterprise Control Server for the PABX
ECS/EMS	Event Management System
EDMS	Electronic Document Management System
EDS	Exhibits Database System
EFF	Electronic Frontier Foundation
EIA	Electronic Industries Alliance
EIA	Electronics Industry Association
ELS	Electronic Library Service
ELVCom	Expendable Launch Vehicle Compendium
EMA	E-Mail Assistant
EMACS	Extensible, customizable, self-documenting real-time display editor
EMCS	Energy Management Control System
EO	Executive Order
EOC	SSC Emergency Operations Center
ERA	Electronic Registration Application
ERASMUS	NASA Financial Dashboard
ERP	Enterprise Resource Portal
ERRMIS	Training, Awards and Travel Mgmt. Information System
ERWIN	Data Modeler , by AllFusion
e-SPACE	Electronic Strategic Planning and Consensus Engagement
ESSEX	Centrex Type arrangement directly with RBOC
ESX	Earth Science Extranet
F2MS	Freedom2Manage Survey
FAAD	Federal Assistance Award Data System
FACF	Financial and Contractual Status System, Financial
FACT	Financial and Contractual Status, Tables Maintenance System
FAS	Funds Availability System
FAST	Financial Accounting System/Teleprocessing
FASTCASH	FAST Cash Management System
Fax	Facsimile
FCACM	Full Cost Accounting Content Manager
FCA-HP	NASA Full Cost Initiative Homepage
FCC	Federal Communications Commission
FEDTAG	FEDTAG Federal Transportation Advisory Group
FHDS	Facilities Help Desk System

FIPS	Federal Information Processing Standards
FM	Frequency Modulation
FOIA	Freedom of Information
FOIA	Freedom Of Information Act Database
FOIA - 94/95	Freedom of Information Act - History Database
FORM 295	Form 295 Database
FORM 6 - CFS	Form 6 - Code CFS
FOSC	Facilities Operating Services Contractor
FPDS	Federal Procurement Data System
FQDN	Fully Qualified Domain Name
FRMT	Fairmont
FSOP	Financial Status of Programs
FSS	Facility Sustainment System
FTE	Full Time Equivalent
FTP	File Transfer Protocol
FTR/PR	Financial Transaction Report/Procurement Report
FTS	Federal Telecommunications System
FUS	Facility Utilization System
FY	Fiscal Year
GB	GigaBits
GBLT	Greenbelt
Gbps	Gigabits per second
GISS	Goddard Institute for Space Studies
GLAS	General Ledger Accounting System
GOS	Guest Operations Database System
GP	General Purpose (Desktop Seats)
GRC	Glenn Research Center at Lewis Field
GRIN	Great Images in NASA
GSA	General Services Administration
GSFC	Goddard Space Flight Center
GUI	Graphical User Interface
H.323	ITU Video Conferencing Standards (H Series)
HAMS	Headquarters Account Tracking and Management System
HATS	Headquarters Action Tracking System
HCSS	Code H Customer Satisfaction Survey
HD	High Definition
HDTV	High Definition Television
HHAD	HQ Honor Awards Database
HHTI	Home and Home Technology Information Website
HLFC	Highlight Financial Cost
HONURS	HQ ODIN New User Request System
HPSS	Headquarters Personnel Security System
HQ	NASA Headquarters
HQ NEF Search	NASA Electronic Form Search
HQAEARS	Headquarters Affirmative Employment Analysis & Reporting System
HQDMS-A	Headquarters Document Management System
HQDMS-B	Code B Headquarters Document Management System
HQDMS-BWPCP	Headquarters Document Management System - Basis Web Password Change Page
HQDMS-CIC	CIC Headquarters Document Management System

HQDMS-CP	Headquarters Document Management System - Code CP
HQDMS-G	Headquarters Document Management System -Code G
HQDMS-GP / LDD	LDD Legal Documents Database
HQDMS-I	Code I Headquarters Document Management System
HQDMS-JE	HQ Document Mangement System - Code JE
HQDMS-LD	Headquarters Document Management System - Code LD
HQDMS-M	Headquarters Document Management System - Code M
HQDMS-Q	Headquarters Document Management System - Code Q
HQDMS-U	Code U Document Management System
HQDMS-ZH	ZH Headquarters Document Management System
HQDRW	Headquarters Data Reconciliation Warehouse
HQDSW-CFB	Headquarters Decision-Support Warehouse - Code CFB
HQeD	Headquarters e-Directory
HQLI	Headquarters Line Item Database
HR	House Resolution
HRTS	Human Resources Tracking System
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
IADS	International Agreements Database System
IBM	International Business Machines Corporation
IBMP	Institute for BioMedical Problems
ICONS	Inventions and Contributions System
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFM	Integrated Financial Management
IFMP	Integrated Financial Management Program
IFM-UIDB	NASA HQ IFM User Information Database
IG I	nspector General
IMAP	Internet Message Access Protocol
IMAP4	Internet Message Access Protocol version 4
IMPASS	Imagery, Media, and Public Affairs Support Services
IMR	Inbound Message Relay
IP	Internet Protocol
IPSec	IP Security
IRIS	Incident Report Information System
IRS	Infocom Reader Survey
IS	Information Systems
ISAS	Institutional Services and Support (IT support contract)
ISCP	Inside Cable Plant
ISD	Information Systems Directorate
ISDN	Integrated Services Digital Network
ISO	International organization for standardization
ISO9000	ISO 9000 Project Implementation System
ISP	Internet Service Provider
IT	Information Technology
ITS	Information Technology Security
ITSM	IT Security Manager
ITSP	

ITU	International Teleconferencing Union
IV&V	NASA Independent Verification and Validation Facility
IVR	Interactive Voice Response System
IWMS	ISEM Work Management System
IXC	Interexchange Carrier Access
JAVA	Portable programming language or platform consists of pre-defined set of JAVA classes
JCSS	Code J Customer Satisfaction Survey
JDBC	Sun's database-independent SQL-level API for database connection
JENS	JSC Emergency Notification System
JPL	Jet Propulsion Laboratory
JSC	Johnson Space Center
JumpStart	Automatic installation of the SUN Solaris operating systems and additional software
Kbps	Kilobits per second
KIC-A	Knowledge Information Center-Code AE (KIC-AE)
KIC-FT	Knowledge Information Center-Code FT
KIC-ISEM	Knowledge Information Center for ISEM
KIC-J	Code J Knowledge Information System
KIC-M	Knowledge Information Center-Code M
KIC-Q	Knowledge Information Center - Code Q (KIC Q)
KIC-R	Knowledge Information Center-Code R
KIC-Z	KIC-Z Knowledge Information Center CATF
Kmail	Kennedy Mail System
KSC	Kennedy Space Center
KVM	Keyboard Video Mouse
LADS	Legislative Affairs Database
LAN	Local Area Network
LARC or LaRC	Langley Research Center
LaRC TV	Langley Television
LaRCNET	Langley Local Area Network
LaRCViN	Langley Video Network
LBV	Low-Bandwidth Videoconference unit
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
LESCO	Contractor Name
LIMS	Logistics Technology Automation Network
LPAR	Logical Partition
LTS	Agency-Wide Litigation Tracking System
M&O	Management and Operations
MA	Maintenance (Desktop Seats)
MAF	Michoud Assembly Facility
MAN	Metropolitan Area Network
MAPI	Messaging Application Programming Interface
MAPS	Mail Abuse Prevention System
MBPD	Master Buy Plan Database
Mbs	Megabits per second
MCU	Multipoint Control Unit
MFI	Major Facility Inventory
M-HATS	OSF Web HATS Interface

MIC	Meeting in conference
MIME	Multi-purpose Internet Mail Extensions
Minority Outreach Web Site	Minority Outreach Web Site
MIPS	Millions of Instructions Per Second
MM	Multi-mode fiber
MODIS	Moderate Resolution Imaging Spectroradiometer
MOU	Memorandum of Understanding
MPEG	Moving Pictures Experts Group
MR	Material Request
MS	Message Store
MSDS	Media Services Database System
MSFC	Marshall Space Flight Center
MSN	Mission Information
MSP	Managed Service Provider
MTA	Message Transfer Agent
MUA	Mail User Agent
MX	Mail Exchange
NACC	NASA ADP Consolidation Center
NAD	Network Active Device (Desktop Seats)
NAIS	NASA Acquisition Internet Service
NAS	Network Access Server
NASA	National Aeronautics and Space Administration
NASA HPEDIT	NASA Homepage Editor
NCC	Nasa Clearance Clearinghouse
NCCS	NASA Communications and Computing Services
NCIS	NASA Commercial Information System
NCRS	Name Check Request System
NCTN	NASA Commercial Technology Network Homepage
NDES	NASA Data Entry System
NEC	Neptune Event Calendar
NEC	Nippon Electric Corporation
NEMS	NASA Equipment Management System
NFMS	NASA Functional Management System
NIS II	Office of Inspector General Nationwide Information System II
NISN	NASA Integrated Services Network
NISSU	NASA Information Systems Services Utility
NMC	Network Monitoring Center
NOC	Network Operations Center
NOVIS	Naked-eye Orbital Visibility Information System
NPD	NASA Policy Directive
NPDMS	NASA Property Disposal Management System
NPG	NASA Procedures and Guidelines
NPMS	NASA Procurement Management System
NPPS T&A	NASA Personnel and Payroll System Time & Attendance
NPSS	NASA Personnel Security System
NRL	Naval Research Laboratory
NSMS	NASA Supply Management System
NTLM	NT LAN Manager (Windows NT Challenge/Response authentication)

NTP	Network Time Protocol
NTSC	National Television Standard Committee - Commission
NVSS	NASA Vendor Survey System
OAO	Orbiting Astronomical Observatory
OAT HP	Office of Aerospace Technology Website
OAT-IN	Office of Aerospace Technology Intranet
OCI	A library of standard database access and retrieval functions for C interface
Octel 300	Octel 300 Serenade voicemail system
ODBC	Open database connectivity, an API with which to access Data Sources
ODIN	Outsourcing Desktop Initiative for NASA
OFSA	Office of Safety and Facility Assurance
OMB	Office of Management Budget
OPSEC	Open Platform for Secure Enterprise Connectivity
ORACLE	Corporation with products for database, application, and development tools
ORR	Operations Readiness Review
OS	Operating System
OSCP	Outside Cable Plant
OSDBU	Office of Small and Disadvantaged Business Utilization
OSF-IN	Office of Space Flight Intranet
OSI	Open Systems Interconnection
OWEB	ODIN WEB Seat Ordering Application
PA	Public Address
PABX	EADS PointSpan 6880 Switch (Rev 2.0.Z)
PBMA	PBMA Process Based Mission Assurance
PBS	Public Broadcasting Service
PBX	Private Branch Exchange
PC	Personal Computer
PCITS	Principal Center for Information Technology Security
PCTR	Personnel Ceiling Transation Report
PDS	PDS Personnel Database System
PERL	A portable programming language mostly used in system and web services
PFSS	Parking and Fare Subsidy System
PIO	Process Improvement Opportunity
PIP	Premium Service
PKI	Public Key Infrastructure
PLDS	Photo Library Database System
PMAS	Code R Program Management Accomplishment System
POP	Post Office Protocol
POP3	Post Office Protocol version 3
PRC	Program Review Center
PRDB	Procurement Request Database (Code U)
PRI	Primary Rate Interface
PRN	Printer (Desktop Seats)
PSLA	Project Service Level Agreement
PSRS (Web-Based)	Web-Based Program Status Review System
PTD	Propulsion Test Directorate
PUB	Public Access
QoS	Quality of Service
R150	A nearline storage by Network Appliance

R.W.A	Registration Site Web Application
RADIUS	Remote Access Dial In User Service
RAM	Random Access Memory
RAMIS DL-MAC	RAMIS DL-MAC RAMIS Downloader - Macint
RAS	Remote Access Service
RBL	Real-time Blackhole List
RBOC	Regional Bell Operating Company
RBS-GSFC	Reimbursable Billing System-GSFC
RBS-JPL	Reimbursable Billing System-JPL (RBS-JPL)
RCM	Remote Communications Modules
RDBMS	Relational Database Management System
RDMS	Relational Database Management System
RDN	Relative Distinguished Name
RF	Radio Frequency
RFC	Request for Comment (Internet Society or IETF draft)
RIB	Code R Image Bank
RIDERS	RIDERS
RIID	Records Inventory and Information Directory
RISO BB	Code R ISO 9000 Bulletin Board
RISO DD	OAT Documents and Data
RISO OJT	OAT On-the-Job Training (OJT) Materials
RISO OWI	Code R Approved OWI's (Working Files)
RISO REP	Code R Repository
RISO TT	This 'n That
RITA	Relocation Income Tax Allowance
RMRS	Resource Management Reporting System
RPI	Real Property Inventory
RSS	Relay Spam Stopper
RTCMD	Recording Tracking Classified Material Destruction
RTIFM	Road to IFM
RWES	RSVP Web E-mail System
SA	System Administrator
SAN	Storage Area Network
SAP	Status of Approval Programs
SASL	Simple Authentication Security Level
SBAR	Speaker's Bureau Asset Repository
SBC	SBC Communications
SBDS	Speaker's Bureau Database System
SBR	Small Business Report
SD	Standard Definition
SDC	Stennis Data Center
SDTV	Standard Definition Television
SEDB	Special Event Database System
SEDSA	Schedule of Estimated Distribution of Selected Accounts
SFA	Space Flight Awareness Honoree Database
SIDD	Shuttle-Interagency Debris Database
SLI	Space Launch Initiative
SMB	Server Message Block
SMIME	Secure Multipurpose Internet Mail Extensions

SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOLAR	Site for On-line Learning and Resources
SQL	Structured Query Language
SRFR	Secure Remote File Site
SRL	SAFE AND ROOM LOCATION
SSC	Stennis Space Center
SSH	Secure Shell Protocol
SSL	Secure Socket Layer Protocol
St Dept Word Macro	St. Department Word Macro
STADS	SAP Time and Dollars System
STD	Standard
STI	Scientific and Technical Information
SUDO	A tool which allows SA to give certain user(s) to run some commands as root.
TCP	Transmission Control Protocol
TDD	Telecommunications device for the deaf
TGIR	Turning Goals Into Reality Registration
TIA	Telecommunications Industry Association
TIMS	Token Information Management System
TLC	Time and Labor Collection
TLS	Transport Layer Security
TMS	Travel Management System
TOIP	Telecommunications over Internet Protocol
TOS	Type of Service
TSU	Travel System-U
TTL	Time to Live
TTSC	Test and Technical Services Contactor
TV	Television
UBE	Unsolicited Bulk Email
UCE	Unsolicited Commercial Email
UDP	User Datagram Protocol
UIS	User Information System
UMC	Universal Modular Chassis
UMIS	University Management Information System
Unix	Unix Operating System
UPATS	Unit Price Agreement Tracking
UPS	Un-interruptible Power Source
URI	Uniform Resource Identifiers
UTNS	User Training Needs Survey
UUCP	Unix-to-Unix Copy Protocol
VAFB	Vandenberg Air Force Base
VBS	Video Bridging Services
VCR	Video Cassette Recorder
VCRS	Video Conference Request System
VDA	Virtual Private Network
VFDS	Video File Database System
VIP	Virtual IP
Visual Cafe	Development/integration tool for JAVA by Symantec
ViTS	Video Teleconferencing System

VLAN	Virtual Local Area Network
VOIP	Voice over Internet Protocol
VoTS	Voice Teleconferencing Services
VPN	Virtual Private Network
VRA	ViTS Roll-About
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor Specific Attribute
VTC	Video Teleconferencing Center
VTR	Video Tape Recorder
W2K	Windows 2000
WAN	Wide Area Network
W-AO OCIO	Office of the Chief Information Officer Home Page
Web Tads – Web access Time	and Attendance
Website-AFU	Code AF Updates
Website-CIS	Code CI Services
Website-Code AE	Website-Code AE
Website-Code CI	Website-Code CI
Website-Code CP	Website-Code CP
Website-Code FP	Website-Code FP
Website-Code G	Website-Code G
Website-Code I	Website-Code I
Website-Code ID	Website-Code ID (Export Control)
Website-Code JM	Code JM/ARL Home Page
Website-Code K	Website-Code K
Website-Code RG	Website-Code RG Code RG Aerospace Website
Website-Code Z	Code Z Website
Website-CPUB	Web-Based Response to Public Queries
Website-ECP	Website -ECP-TBD
Website-FOIA	Website-FOIA
Website-OSF	Office of Space Flight Website
Website-SPB	Website-SPB Speaker's Bureau Website
Website-VITS	Website-VITS VITS Web Page
Websphere	Software platform by IBM
WFF	Wallops Flight Facility
W-HQ ITC	HQ Information Technology & Communications Division Home Page
WIMS	Workforce Information Management System
WITS	Washington Interagency Telecommunications Service
W-P NWP	Code P NASA Web Page (HQ Web Page)
WSTF	White Sands Test Facility
W-U PWS	Code U Public Website
W-UM SSC	W-UM SCC Code U&M Space Station Commercialization Web Site
WWW	World-Wide-Web
WYE	Workyear Equivalent
X.500	Directory Access Protocol (ISO/TSU-T suite of standards)
X.500 BACKSTORE	X.500 BACKSTORE
X.509	Version 3 Public-Key Certificate (ISO/TSU-T suite of standards)
XML	eXtensible Markup Language

Table of Contents

1	OFFICE AUTOMATION, IT INFRASTRUCTURE, AND TELECOMMUNICATIONS INVESTMENT CATEGORY OVERVIEW.....	8
1.1	COMMUNICATION SERVICES.....	8
1.1.1	Wide Area Network (WAN).....	8
1.1.2	Local Area Network (LAN).....	9
1.1.3	Voice.....	9
1.1.4	Video.....	9
1.2	COMPUTING SERVICES.....	9
1.2.1	Desktop Hardware and Software.....	9
1.2.2	Application Services.....	9
1.2.3	Data Center.....	10
1.1	ELECTONIC WORK ENVIRONMENT.....	10
1.2.4	Messaging and Collaboration.....	10
1.2.5	World Wide Web.....	11
1.2	CROSS-CUTTING PORTFOLIO.....	11
1.2.6	XML.....	11
2	PROGRAM UNIQUE IT AND MULTI-PROGRAM / PROJECT IT INVESTMENT CATEGORY....	12
3	AMES RESEARCH CENTER (ARC) - AEROSPACE TECHNOLOGY SUPPORT SYSTEM.....	15
1.3	PROJECT DESCRIPTION.....	15
1.4	ARCHITECTURE.....	18
3.1.1	Business.....	18
3.1.2	Data.....	18
3.1.3	Application and Technology.....	19
3.1.4	Security and Privacy.....	21
3.1.5	Government Paperwork Elimination Act.....	22
4	AMES RESEARCH CENTER (ARC) – NASA HIGH END COMPUTING COLUMBIA	22
1.5	PROJECT DESCRIPTION.....	22
1.6	ARCHITECTURE.....	23
4.1.1	Business.....	23
4.1.2	Data.....	24
4.1.3	Application and Technology.....	24
4.1.4	Security and Privacy.....	31
4.1.5	Government Paperwork Elimination Act.....	32
5	GODDARD SPACE FLIGHT CENTER (GSFC) – EARTH OBSERVING SYS DATA INFO SYSTEMS.....	32
1.7	PROJECT DESCRIPTION.....	32
1.8	ARCHITECTURE.....	34
5.1.1	Business.....	34
5.1.2	Data.....	36
5.1.3	Application and Technology.....	37
5.1.4	Security and Privacy.....	46
5.1.5	Government Paperwork Elimination Act.....	48
6	GODDARD SPACE FLIGHT CENTER (GSFC) – HUBBLE SPACE TELESCOPE MISSION OPS IT	48
1.9	PROJECT DESCRIPTION.....	48
1.10	ARCHITECTURE.....	49
	6.1.1

6.1.2	Data	49
6.1.3	Application and Technology	50
6.1.4	Security and Privacy.....	52
6.1.5	Government Paperwork Elimination Act.....	53
7	GODDARD SPACE FLIGHT CENTER (GSFC) – NASA CENTER FOR COMPUTATIONAL SERVICES (NCCS).....	53
1.11	PROJECT DESCRIPTION	53
1.12	ARCHITECTURE.....	55
7.1.1	Business	56
7.1.2	Data	56
7.1.3	Application and Technology	57
7.1.4	Security and Privacy.....	77
7.1.5	Government Paperwork Elimination Act.....	80
8	GODDARD SPACE FLIGHT CENTER (GSFC) – SPACE AND GROUND NETWORK IT SUPPORT	80
1.13	PROJECT DESCRIPTION	80
1.14	ARCHITECTURE.....	81
8.1.1	Business	81
8.1.2	Data	81
8.1.3	Application and Technology	82
8.1.4	Security and Privacy.....	85
8.1.5	Government Paperwork Elimination Act.....	86
9	JOHNSON SPACE CENTER (JSC) – FLIGHT OPERATIONS	86
1.15	PROJECT DESCRIPTION	86
1.16	ARCHITECTURE.....	87
9.1.1	Business	87
9.1.2	Data	87
9.1.3	Application and Technology	87
9.1.4	Security and Privacy.....	97
9.1.5	Government Paperwork Elimination Act.....	98
10	JOHNSON SPACE CENTER (JSC) – INTEGRATED PLANNING SYSTEM.....	99
1.17	PROJECT DESCRIPTION	99
1.18	ARCHITECTURE.....	100
10.1.1	Business	100
10.1.2	Data	101
10.1.3	Application and Technology	101
10.1.4	Security and Privacy.....	108
10.1.5	Government Paperwork Elimination Act.....	110
11	JOHNSON SPACE CENTER (JSC) – MISSION CONTROL CENTER	110
1.19	PROJECT DESCRIPTION	110
1.20	ARCHITECTURE.....	112
11.1.1	Business	112
11.1.2	Data	112
11.1.3	Application and Technology	112
11.1.4	Security and Privacy.....	116
11.1.5	Government Paperwork Elimination Act.....	118
12	JOHNSON SPACE CENTER (JSC) – SOFTWARE DEVELOPMENT / INTEGRATION LABORATORY.....	118
1.21	PROJECT DESCRIPTION	118
1.22	ARCHITECTURE.....	119

12.1.1	<i>Business</i>	120
12.1.2	<i>Data</i>	120
12.1.3	<i>Application and Technology</i>	120
12.1.4	<i>Security and Privacy</i>	133
12.1.5	<i>Government Paperwork Elimination Act</i>	135
13	JOHNSON SPACE CENTER (JSC) – SPACE SHUTTLE PROGRAM COCKPIT AVIONICS UPGRADE	135
1.23	PROJECT DESCRIPTION	135
1.24	ARCHITECTURE.....	135
13.1.1	<i>Business</i>	135
13.1.2	<i>Data</i>	136
13.1.3	<i>Application and Technology</i>	136
13.1.4	<i>Security and Privacy</i>	142
13.1.5	<i>Government Paperwork Elimination Act</i>	143
14	JOHNSON SPACE CENTER (JSC) – SPACE SHUTTLE PROGRAM FLIGHT SOFTWARE	143
1.25	PROJECT DESCRIPTION	143
1.26	ARCHITECTURE.....	145
14.1.1	<i>Business</i>	145
14.1.2	<i>Data</i>	145
14.1.3	<i>Application and Technology</i>	146
14.1.4	<i>Security and Privacy</i>	149
14.1.5	<i>Government Paperwork Elimination Act</i>	150
15	JOHNSON SPACE CENTER (JSC) – SPACE SHUTTLE PROGRAM PROGRAM INTEGRATION 150	
1.27	PROJECT DESCRIPTION	150
1.28	ARCHITECTURE.....	151
15.1.1	<i>Business</i>	151
15.1.2	<i>Data</i>	152
15.1.3	<i>Application and Technology</i>	152
15.1.4	<i>Security and Privacy</i>	164
15.1.5	<i>Government Paperwork Elimination Act</i>	166
16	JOHNSON SPACE CENTER (JSC) – SPACE STATION PRODUCTION FACILITY	166
1.29	PROJECT DESCRIPTION	166
1.30	ARCHITECTURE.....	166
16.1.1	<i>Business</i>	166
16.1.2	<i>Data</i>	167
16.1.3	<i>Application and Technology</i>	167
16.1.4	<i>Security and Privacy</i>	179
16.1.5	<i>Government Paperwork Elimination Act</i>	180
17	JOHNSON SPACE CENTER (JSC) – SPACE STATION TRAINING FACILITY	180
1.31	PROJECT DESCRIPTION	180
1.32	ARCHITECTURE.....	183
17.1.1	<i>Business</i>	184
17.1.2	<i>Data</i>	184
17.1.3	<i>Application and Technology</i>	185
17.1.4	<i>Security and Privacy</i>	193
17.1.5	<i>Government Paperwork Elimination Act</i>	195
18	KENNEDY SPACE CENTER (KSC) – GROUND OPERATIONS	195
1.33	PROJECT DESCRIPTION	195
1.34	ARCHITECTURE.....	195

18.1.1	<i>Business</i>	195
18.1.2	<i>Data</i>	196
18.1.3	<i>Application and Technology</i>	196
18.1.4	<i>Security and Privacy</i>	203
18.1.5	<i>Government Paperwork Elimination Act</i>	205
19	KENNEDY SPACE CENTER (KSC) – INTEGRATED LOGISTICS	205
1.35	PROJECT DESCRIPTION	205
1.36	ARCHITECTURE.....	206
19.1.1	<i>Business</i>	206
19.1.2	<i>Data</i>	207
19.1.3	<i>Application and Technology</i>	207
19.1.4	<i>Security and Privacy</i>	213
19.1.5	<i>Government Paperwork Elimination Act</i>	215
20	KENNEDY SPACE CENTER (KSC) – LAUNCH CONTROL SYSTEM (LCS).....	215
1.37	PROJECT DESCRIPTION	215
1.38	ARCHITECTURE.....	216
20.1.1	<i>Business</i>	216
20.1.2	<i>Data</i>	216
20.1.3	<i>Application and Technology</i>	216
20.1.4	<i>Security and Privacy</i>	223
20.1.5	<i>Government Paperwork Elimination Act</i>	224
21	KENNEDY SPACE CENTER (KSC) – OPERATIONAL TELEVISION SYSTEM MODERNIZATION	224
1.39	PROJECT DESCRIPTION	224
1.40	ARCHITECTURE.....	225
21.1.1	<i>Business</i>	225
21.1.2	<i>Data</i>	226
21.1.3	<i>Application and Technology</i>	226
21.1.4	<i>Security and Privacy</i>	227
21.1.5	<i>Government Paperwork Elimination Act</i>	228
22	KENNEDY SPACE CENTER (KSC) – SHUTTLE PROCESSING SUPPORT.....	228
1.41	PROJECT DESCRIPTION	228
1.42	ARCHITECTURE.....	229
22.1.1	<i>Business</i>	229
22.1.2	<i>Data</i>	229
22.1.3	<i>Application and Technology</i>	229
22.1.4	<i>Security and Privacy</i>	236
22.1.5	<i>Government Paperwork Elimination Act</i>	237
23	LANGLEY RESEARCH CENTER (LARC) – NASA TECHNOLOGY TRANSFER SYSTEMS (NTTS)	237
1.43	PROJECT DESCRIPTION	237
1.44	AS – IS	238
1.45	SYSTEMS DESCRIPTION AND OPERATIONAL CONCEPT.....	239
23.1.1	<i>eNTRe</i>	240
23.1.2	<i>TechTracS (TTS)</i>	240
23.1.3	<i>KIMS</i>	242
23.1.4	<i>TechFinder</i>	243
1.46	NTTS SUPPORT	243
23.1.5	<i>NASA Interfaces</i>	243
23.1.6	<i>External Interfaces</i>	244
1.47	PRODUCTION NETWORK DIAGRAM	245

1.48	SYSTEMS AND SUPPORT	247
1.49	FACILITIES	248
1.50	TECHNOLOGY FLASHPOINTS.....	248
1.51	COMPLIANCE	248
1.52	CAPABILITIES.....	251
1.53	TO - BE CONDITION.....	254
24	MARSHALL SPACE FLIGHT CENTER (MSFC) – PAYLOAD OPERATIONS AND INTEGRATION CENTER	254
1.54	PROJECT DESCRIPTION	254
1.55	ARCHITECTURE.....	254
24.1.1	<i>Business</i>	255
24.1.2	<i>Data</i>	255
24.1.3	<i>Application and Technology</i>	255
24.1.4	<i>Security and Privacy</i>	258
24.1.5	<i>Government Paperwork Elimination Act</i>	260
25	NASA ENTERPRISE ARCHITECTURE	260
1.56	PROJECT DESCRIPTION	260
1.57	ARCHITECTURE.....	261
25.1.1	<i>Business</i>	261
25.1.2	<i>Data</i>	262
25.1.3	<i>Application and Technology</i>	262
25.1.4	<i>Security and Privacy</i>	264
25.1.5	<i>Government Paperwork Elimination Act</i>	265
26	NASA INTEGRATED FINANCIAL MANAGEMENT PROGRAM (IFMP).....	265
1.58	PROJECT DESCRIPTION	265
1.59	ARCHITECTURE.....	268
26.1.1	<i>Business</i>	268
26.1.2	<i>Data</i>	270
26.1.3	<i>Application and Technology</i>	271
26.1.4	<i>Security and Privacy</i>	276
26.1.5	<i>Government Paperwork Elimination Act</i>	278
27	NASA OAIT UMBRELLA	279
1.60	PROJECT DESCRIPTION	279
1.61	ARCHITECTURE.....	284
27.1.1	<i>Business</i>	284
27.1.2	<i>Data</i>	285
27.1.3	<i>Application and Technology</i>	287
27.1.4	<i>Security and Privacy</i>	303
27.1.5	<i>Government Paperwork Elimination Act</i>	305

Figure References

FIGURE 1, U.S. PUBLIC	239
FIGURE 2, APPLICATION ARCHITECTURE	240
FIGURE 3, TECHTRACS APPLICATION ARCHITECTURE	242
FIGURE 4, NTTS SYSTEMS ARCHITECTURE	247

Reference of Tables

TABLE 1	12
TABLE 2	13
TABLE 3	19
TABLE 4	20
TABLE 5	24
TABLE 6	28
TABLE 7	37
TABLE 8	40
TABLE 9	50
TABLE 10	51
TABLE 11	57
TABLE 12	65
TABLE 13	82
TABLE 14	83
TABLE 15	87
TABLE 16	91
TABLE 17	101
TABLE 18	105
TABLE 19	113
TABLE 20	114
TABLE 21	120
TABLE 22L	126
TABLE 23	136
TABLE 24	140
TABLE 25	146
TABLE 26	148
TABLE 27	152
TABLE 28	157
TABLE 29	167
TABLE 30	172
TABLE 31	185
TABLE 32	188
TABLE 33	196
TABLE 34	200
TABLE 35	207
TABLE 36	211
TABLE 37	216
TABLE 38	221
TABLE 39	226
TABLE 40	226
TABLE 41	229
TABLE 42	234
TABLE 43, NTTS INTERFACES TO OTHER NASA SYSTEMS	244
TABLE 44, EXTERNAL INTERFACES.....	245
TABLE 45, NASA POLICIES, LEGISLATION, FEDERAL REGULATIONS SUPPORTED BY NTTS BY ELEMENT	248
TABLE 46	256
TABLE 47	257
TABLE 48	262
TABLE 49	263
TABLE 50	271
TABLE 51	274
TABLE 52	287
TABLE 53	300

1 Office Automation, IT Infrastructure, and Telecommunications Investment Category Overview

The NASA Enterprise Architecture is structured into three major components: Office Automation, IT Infrastructure, and Telecommunications IT, Multi-Program / Project IT, and Program Unique IT. The definitions for these components are:

Office Automation, IT Infrastructure, and Telecommunications: This category includes Office Automation investments that provide general purpose computing (e.g. email, desktops, help desk services) for both civil servants and contractor personnel, regardless of the program or project supported or fund source.

Multi-Program / Project IT: Multi-Program/Project IT is defined as IT infrastructure, products, and services that are not part of OAIT but do meet IT requirements that are not unique to a single program/project. These investments typically benefit multiple missions, programs or projects and “end of life” for a single project would not eliminate the need for the investment.

Program Unique IT: Program Unique IT is defined as infrastructure, products and services that are either physically embedded in a flight or test article, or exist solely to meet the requirements of a single specific program or project. These investments would typically not be needed after “end of life” of the unique program or project that generated the requirements for the investment.

Volume 3 focuses on the Program Unique IT and Multi-Program / Project IT components. First, a brief description of the Office Automation, IT Infrastructure, and Telecommunications is given.

NASA Portfolios

The NASA Enterprise Architecture clusters operational activities and improvement actions into three portfolio areas. Descriptions of each portfolio area and the components within each service area are described below.

1.1 Communication Services

The Communications Services component of the Program includes the agency’s voice, data, and video network infrastructure, exclusive of any infrastructure elements that are unique to mission operations.

1.1.1 Wide Area Network (WAN)

This project consists of a set of wide area networks that support production services, as well as services provided by several Internet Service Providers (ISPs).

1.1.2 Local Area Network (LAN)

The LAN component incorporates all IT investments required to provide networking services within a building, campus, data center or Center, including hardware, software, and services (including wireless LANs, remote access, Domain naming services, network management, X500/directory services)

1.1.3 Voice

The Voice component includes all elements that provide voice services to users including hardware, software, services and communications that are not provided by NASA WANs. The voice element includes local and long distance telephone services, cell phone service, satellite phone service, teleconferencing, voice mail, fax, and ancillary services such as two way radios, emergency warning systems, and public address systems.

1.1.4 Video

This category includes investments required to support video and video distribution and video conferencing services used by Agency to include hardware, software and support services - not including LAN or WAN.

1.2 Computing Services

Included in this service area are desktop hardware and software service, application services, and those services provided by agency or Center multi-purpose data centers. Although there are a number of ongoing operational activities within this service area, there are no new agency-wide projects proposed at this time. This service area incorporates ODIN and NACC, activities independently managed in the past.

1.2.1 Desktop Hardware and Software

Desktop computing services to users include all general purpose, desktop computing hardware and software (OS, applications and utilities) components and services (including design, build, operations, support and maintenance services) Includes peripherals/printers. Not included is email and calendaring client & servers or desktops whose primary uses are mission specific. This includes multipurpose help desks.

1.2.2 Application Services

Application services provide an end service to end-users. Applications services include the development, operations and maintenance of applications that are not desktop services. Included

are IT investments in hardware (not a part of a data center), software and services required to provide application services remote from a desktop and not provided by a data center. This includes design, development, help and other support, operations and maintenance.

1.2.3 Data Center

A data center is a collection of IT hardware and software used for multiple purposes. These resources are usually funded and operated as a shared resource with management dedicated to operating the center. Mass storage systems are normally included as a data center unless the mass storage is integrated into some other IT facility. Included is data storage (digital data storage services, including hardware, software and services). Public Web hosting services are not included.

Electronic Work Environment

The Electronic Work Environment is a set of inter-related efforts that provide the NASA workforce with tools that improve the ability to work together and coordinate with NASA partners across all disciplines. This service area includes messaging systems that provide email and/or calendaring, collaboration tools that support virtual teaming, document and records management, and tools like XML that support and promote data interoperability across NASA, other agencies, and NASA partners.

1.2.4 Messaging and Collaboration

This component includes IT investments to provide Email, instant messaging, and collaborative tools.

An extensive integrated e-mail and collaboration study was produced at NASA detailing the requirements of NASA messaging & collaboration and the technologies that could be used to address those requirements. The results favored Microsoft Exchange to provide the features those users wanted and required to fulfill their jobs (integration of mail, task management, calendaring, file sharing, and correspondence management). The results were briefed to the NASA Administrator and subsequently lead to an extensive pilot project for NASA HQ being initiated. Exchange provides: email, calendaring, instant messaging, PKI encryption, Blackberry support, collaboration, and other features.

In the area of Team Collaboration, the pilot project evaluated a number of tools, selected WebEx for synchronous virtual team meeting support, and conducted an extensive two year implementation supporting a wide variety of NASA teams. The tool was provisioned in a fully outsourced Application Service Provider (ASP) business model. The tool was widely accepted and just recently the decision was made to create a collaborative services seat as an option on the ODIN desktop outsource contract. In this way, the collaboration capability will be provided as an agency level service, still using a form of ASP business model, and utilizing a convenient and existing funding model and implementation contract.

1.2.5 World Wide Web

This component includes Center and agency-wide development and hosting services focused on providing web access for the public to information about NASA – whether for business opportunities, for general public awareness, for educational purposes, or for dissemination of knowledge gained from NASA research and operations. NASA publishes more than two-million web pages devoted to space science in its fulfillment of the Space Act that established the Agency. The Internet is the ideal medium for NASA in the dissemination and exchange of ideas.

Cross-Cutting Portfolio

1.2.6 XML

As one of the Program’s near term initiatives, the XML initiative supports data interoperability across NASA, other agencies, and NASA partners. XML is a family of standards and technologies that addresses the issue of achieving data integration. In the past, the solution was largely to develop central databases formed out of back-end legacy systems. Because of the complexity of such systems, little was gained from that approach. More recently, distributed databases and various middleware packages addressed distributed heterogeneous data. However, the time to develop the solution often seemed endless and the cost quite high.

XML offers a better, lower-cost alternative. XML has become a universal, vocabulary-based standard that uses a set of rules, guidelines and conventions for designing text formats in a way that produces Web-enabled files that are easy to produce and read. Systems based on current XML formats are able to deliver data in a manner all platforms can readily interpret, transfer, and store. Because of its universality, OMB has dictated that all e-Gov Initiatives should define and implement an approach for using XML. Where new developments or re-developments are pursued, XML must be considered as the default format for highly structured data as well as relatively less highly structured information, particularly at the User Interface layer but also at the Enterprise Repositories level as well. For legacy repositories that do not directly support XML, legacy to XML mapping and data transformation is to be explored for supporting interoperability across the data architecture. Use of voice XML (VXML) will be considered at the user interface level, especially for Government to Citizen (G2C) initiatives.

NASA has entered into an agreement with DOD/DISA to use their XML Registry to store NASA XML information. This project will advance the implementation of XML standards across NASA. The goals of the project are to:

- “Future proof” information against periodic technology change, facilitate integration and promote collaboration.
- Reduce the cost of integrating data, replication of data and warehousing (where these are clearly needed).
- Allow communication between applications running on different Web servers

2 Program Unique IT and Multi-Program / Project IT Investment Category

NASA’s Vision and Mission are its guiding principles. They represent NASA’s fundamental contributions to the Nation and the world, and they provide us with a clear, unified, and long-term direction for all of our activities. To achieve the new Vision and Mission, Agency goals were established to outline what NASA will achieve in the coming decades. They also will provide the context for planning and program development. The goals will be achieved by NASA’s six Enterprises of Space Science, Earth Science, Biological and Physical Research, Aerospace Technology, Education and Space Flight. The goals will also be supported by organizations through a series of objectives. The programs and tasks that implement the objectives are funded through eighteen themes, which represent the Agency structure for budget planning, management, and performance reporting. The relationship between each theme and Enterprise is shown in the following table.

Table 1

Theme	Enterprise
Solar System Exploration (SSE)	Space Science
Mars Exploration (MEP)	Space Science
Astronomical Search for Origins (ASO)	Space Science
Structural and Evolution of the Universe (SEU)	Space Science
Sun-Earth Connection (SEC)	Space Science
Earth System Science (ESS)	Earth Science
Earth Science Applications (ESA)	Earth Science
Biological Sciences Research (BSR)	Biological and Physical Research
Physical Sciences Research (PSR)	Biological and Physical Research
Research Partnerships and Flight Support (RPFS)	Biological and Physical Research
Aeronautics Technology (AT)	Aerospace Technology
Education Programs (EP)	Education
International Space Station (ISS)	Space Flight
Space Shuttle Program (SSP)	Space Flight
Space and Flight Support (SFS)	Space Flight

Space Launch Initiative (SLI)	Aerospace Technology
Mission and Science Measurement Technology (MSM)	Aerospace Technology
Innovative Technology Transfer Partnerships (ITTP)	Aerospace Technology

Furthermore, each program’s corresponding theme and Enterprise is shown in the next table. Also, their roles as Program Unique IT or Multi-Program / Project IT are listed.

Table 2

Mission/Program	Enterprise	Theme	Program Unique IT or Multi-Program / Project IT
ARC: Aerospace Technology Support System	Aerospace Technology	Aerospace Technology(AT), Space Launch Initiative(SLI), Mission and Science Measurement Technology (MSM), Innovative Technology Transfer Partnerships(ITTP)	Multi-Program / Project IT
ARC: NASA High End Computing Columbia	Aerospace Technology	Aerospace Technology(AT), Space Launch Initiative(SLI), Mission and Science Measurement Technology (MSM), Innovative Technology Transfer Partnerships(ITTP)	Multi-Program / Project IT
GSFC: Earth Observing Sys Data Info Sys	Earth Science	Earth System Science(ESS)	Multi-Program / Project IT
GSFC: NASA Center for Computational Services	Earth Science	Earth System Science(ESS)	Multi-Program / Project IT

GSFC: Hubble Space Telescope Mission Ops IT	Space Sciences	Astronomical Search for Origins(ASO)	Program Unique IT
GSFC: Space and Ground Network IT Support	Earth Sciences	Earth System Science(ESS)	Multi-Program / Project IT
JSC: Flight Operations	Space Flight	Space & Flight Support(SFS)	Multi-Program / Project IT
JSC: Mission Control Center	Space Flight	Space & Flight Support(SFS)	Multi-Program / Project IT
JSC: Space Station Production Facility	Space Flight	International Space Station(ISS)	Program Unique IT
JSC: Space Shuttle Program Flight Software	Space Flight	Space Shuttle Program(SSP)	Program Unique IT
JSC: Software Development/Integration Laboratory	Space Flight	International Space Station(ISS)	Program Unique IT
JSC: Space Shuttle Program Cockpit Avionics Upgrade	Space Flight	Space & Flight Support(SFS)	Program Unique IT
JSC: Space Station Training Facility	Space Flight	Space & Flight Support(SFS)	Program Unique IT
JSC: Integrated Planning System	Space Flight	Space & Flight Support(SFS)	Multi-Program / Project IT
JSC: Space Shuttle Program Program Integration	Space Flight	Space & Flight Support(SFS)	Program Unique IT
KSC: Operational Television System Modernization	Space Flight	Space Shuttle Program (SSP)	Program Unique IT
KSC: Launch Control System	Space Flight	Space & Flight Support(SFS)	Program Unique IT
KSC: Shuttle Processing Support	Space Flight	Space Shuttle Program (SSP)	Program Unique IT
KSC: Ground Operations	Space Flight	Space Shuttle Program (SSP)	Program Unique IT
KSC: Integrated Logistics	Space Flight	Space Shuttle Program (SSP)	Program Unique IT

**MSFC: Payload
Operations and
Integration**

**Biological and
Physical
Research**

**Research
Partnerships &
Flight Support
(RFPS)**

**Program
Unique IT**

The above relationships provide a direct link between NASA's Vision and Mission to specific programs and missions. This in turn yields a clear connection to the following Mission Specific information.

The Integrated Financial Management system deserves some additional comment. Strictly speaking, Resource and Financial management would not ordinarily be considered a Program Unique IT or Multi-Program / Project IT system for an Agency like NASA. However, several factors lead NASA to include IFM in this context at this time. First, this is consistent with identification of Financial Management by NASA as a Mission Area in the NASA budget submission to the Office of Management and Budget. Second, with the emphasis placed on Financial and Resources management by NASA and the Administration in recent years and the importance to a mission-driven agency like NASA of excellent financial and resources management, the designation is warranted. Finally, IFM is the first suite of applications to be deployed as a NASA-wide suite across all Centers and NASA Enterprises.

IFM also has extra significance with respect to the NASA Enterprise Architecture. Just as NASA seeks to define and provide an Office Automation, IT Infrastructure, and Telecommunications Infrastructure that will enable and provide integrated leverage to other Program Unique IT functions, NASA seeks to integrate and leverage IFM and the Office Automation, IT Infrastructure, and Telecommunications Infrastructure. NASA has established an IFM Integration Steering Committee (ISC). The ISC is chaired by the NASA CIO and includes other senior IT management from around the Agency. The IFM Program has developed and documented a Resources Management Architecture which is reviewed and concurred upon by the CIO and the IFM ISC, and that document is included in its entirety as Appendix A of this Volume. As the Agency moves forward on developing a fully integrated "To Be" Enterprise IT Architecture, IFM will be addressed in this effort in the same context as the Office Automation, IT Infrastructure, and Telecommunications, Multi-Program / Project IT and Program Unique IT systems.

3 Ames Research Center (ARC) - Aerospace Technology Support System

Project Description

Fiscal Year 2004 is the FINAL YEAR of this system.

The ARC Aerospace Technology Support System provides Ames Research Center's Information Technology support of Aerospace Technology Enterprise programs. IT resources include computers from specialized, small desktop and instrument control computers to powerful, large

supercomputers, as well as specialized networking hardware. Software includes commercial science and technology applications and tools, as well as ad hoc, custom-built programs and objects. Services include maintenance, system and network administration, operational support and software maintenance. These investments are in the operations phase of the NASA Capital Planning and Investment Control process and are managed as part of the supported NASA Aerospace Enterprise programs under the NASA Procedures and Guidance (NPG) 7120 program management process.

Fiscal Year 2004 is the FINAL YEAR of this system. The ARC Aerospace Technology Support System provides Ames Research Center's Information Technology support of Aerospace Technology Enterprise programs. This Enterprise no longer exists and the IT resources of each of its programs are reported and managed individually by those programs, as of FY2005.

The ARC Aerospace Technology Support System is a loosely related collection of IT products and services in support of Ames Research Center's projects and activities that are part of NASA's Aerospace Technology Enterprise. These IT products and services are mission-specific, i.e., they are acquired independently by each project or activity to meet its own requirements, and are required in addition to the center-wide IT infrastructure.

The ARC Aerospace Technology Support System provides IT products and services for more than 25 Aerospace Technology Enterprise projects and activities at Ames Research Center. These projects and activities are listed in I.A.1.b, described briefly in I.B, and described more fully in the 2004 Ames Implementation Plan:

<http://www.arc.nasa.gov/aboutames-2004amesimplementationplan.cfm>.

The IT products and services provided by the ARC Aerospace Technology Support System include:

- desktop computers that display scientific and engineering data in graphic and pictorial formats, including three-dimensional
- computers that control instruments, data acquisition systems, and autonomous systems
- powerful supercomputers (partially funded by other NASA enterprises) that process scientific and engineering simulations
- specialized telecommunications systems that provide high-speed networking and networking of multimedia data
- commercial software tools, such as MATLAB, that science and technology applications require to do their work
- ad hoc, custom built software that models systems being investigated by the Aerospace Technology Enterprise projects and activities
- services such as hardware and software maintenance, system and network administration, operational support and software development.

Aerospace Technology Enterprise projects and activities supported at Ames Research Center by the ARC Aerospace Technology Support System are:

Advanced Air Transportation Technologies Project (NASA goals 2,3,6,7)

Efficient Aircraft Spacing Project (new in FY 2004, NASA goals 2,3,6,7)

Efficient Flight Path Management Project (new in FY 2004, NASA goals 2,3,6,7)
Virtual Airspace Modeling and Simulation Project (NASA goals 2,3)
Strategic Airspace Usage Project (new in FY 2004, NASA goals 2,3,6,7)
Human Measures and Performance Project (NASA goals 2,3,6,7)

Aviation System Monitoring and Modeling Project (NASA goals 2,3)
System-Wide Accident Prevention Project (NASA goals 2,3)
System Vulnerability Detection Project (new in FY 2004, NASA goals 2,3)

Support in four areas of the NASA Next-Generation Launch Technology Program (NASA goals 6,7,8)

- Integrated Vehicle Health Management
- Crew Cockpit Technology and Human-Factors Research
- Systems Studies and Tool Development for Systems Studies
- Thermal Protection Systems

Support in two areas of the NASA Orbital Space Plane (NASA goals 6,7,8)

- Thermal Protection System
- Wing Leading Edge Thermal Protection System for X-37 Research Aircraft

Information Technology Strategic Research Project (NASA goals 9,10)

Support in three areas of the Information Technology Strategic Research Project (NASA goals 2,3)

- Adaptive Flight Control Systems
- Health Monitoring and Diagnostics Technologies
- Outer-Loop Methods

Intelligent Systems Project (NASA goals 9,10)

Computing, Networking, and Information Systems Project (NASA goals 9,10)

Major support for research into nanotechnology, as performed by Ames Research Center's Center for Nanotechnology (NASA goals 9,10)

Resilient Systems and Operations Project (NASA goals 6,7,9,10)

Knowledge Engineering for Safety and Success Project (NASA goal 10)

Support in two areas of Jet Propulsion Laboratory's System Reasoning and Risk Management Project (NASA goals 6,7,9,10)

- Investigation Methods and Tools
- Core Risk Research

Support in two activities of the NASA Innovative Technology Transfer Partnerships Theme (NASA goals 1-10)

- Office of Technology Transfer Partnerships
- Consolidated Supercomputing Management Office

Descriptions of all these Aerospace Technology Enterprise projects and activities may be found in the 2004 Ames Implementation Plan,

<http://www.arc.nasa.gov/aboutames-2004amesimplementationplan.cfm>.

Architecture

3.1.1 Business

3.1.1.1 Process simplification/reengineering/design projects

The ARC Aerospace Technology Support System is currently in the mission operations phase. Process simplification/reengineering/design projects have been accomplished throughout the life cycle of the supported NASA Aerospace Technology Enterprise programs.

3.1.1.2 Major organization restructuring, training and change management projects

The ARC Aerospace Technology Support System is currently in the mission operations phase. Organizational restructuring, training and change management have been accomplished throughout the life cycle of the supported NASA Aerospace Technology Enterprise programs.

3.1.2 Data

3.1.2.1 Types of Data

Data types used in the ARC Aerospace Technology Support System include Mission data, such as schedule, planning, command and control data; and Scientific, Engineering and Research data, such as length, strain, velocity, acceleration, mass, weight, pressure, temperature, voltage, current and power.

3.1.2.2 Existing Data Access

The programs supported by the ARC Aerospace Technology Support System usually generate their own data. But they also use certain classes of existing data. For example, Air traffic control and flight simulations use existing databases of terrain, airport configurations and airplane appearances in simulating ground movements, takeoffs and landings, and flight. Simulations of aerodynamic flows use existing databases of airplanes or other objects “flying” in the flows; and use existing databases of gas properties in calculating reactions of the aerodynamic flows. Wind tunnel and other experimental tests use existing theoretical or experimental results to corroborate the test results.

These databases may have been created by NASA, may have been purchased from commercial sources, or may have been obtained from research by non-NASA organizations, e.g., universities, government agencies or private research organizations. The supported programs continually monitor related work done elsewhere and are prepared to use existing data when it is found. Of course, where the data are significant, NASA-generated research reports cite the source.

3.1.3 Application and Technology

3.1.3.1 Relationship to Service Component Model

Table 3

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
				<p>Service Component Reference Model elements relevant to the ARC Aerospace Technology Support System include:</p>
				<p>Digital Asset Services -- Content Management -- Content Authoring, Content Review and Approval, and Content Publishing and Delivery; and Digital Asset Services -- Knowledge Management -- Information Retrieval, Information Sharing, Knowledge Capture, Knowledge Discovery, and Knowledge Distribution and Delivery. These services support the Aerospace Technology programs and projects by storing, maintaining and retrieving project documents and information; and by facilitating the identification, gathering and transformation of project data and information into knowledge.</p>
				<p>Back Office Services -- Data Management -- Data Exchange, Data Cleansing, Loading and Archiving, and Data Classification. The ARC Aerospace Technology Support System uses, processes and administers the raw material -- data -- required by the Content Management and Knowledge Management services.</p>

Support Services -- Security Management -- Access Control, Verification, and Role / Privilege Management; and Support Services -- Systems Management -- System Resources Monitoring, and Software Distribution. These services protect, administer and maintain the ARC Aerospace Technology Support System so that it is ready and able to support the Aerospace Technology programs and projects.

3.1.3.2 Relationship to Technology Component Model

Table 4

Service Area	Service Category	Service Standard	Relation to SRM of FEA
--------------	------------------	------------------	------------------------

Technical Reference Model elements relevant to the ARC Aerospace Technology Support System include all those listed in v1.0 of the model. Some have greater relevance, including, for example in the Service Access and Delivery area, Access Channels/Web Browser/(Internet Explorer and Netscape Communicator); Access Channels/Collaboration and Communications/Electronic Mail; Delivery Channels/(Internet, Intranet and Virtual Private Network); Service Requirements/Legislative and Compliance/(Section 508 and Security); Service Transport/Supporting Network Services/(IMAP, POP3, MIME, SMTP, LDAP, Directory Services and DNS); and Service Transport/Service Transport/(TCP, IP, HTTP and HTTPS).

NASA Standards required and used by this investment include: Internet Explorer and Netscape Navigator, SMTP/NASA MIME profile, IMAP4, POP3 and HTML 4.0.

Service specifications used by the ARC Aerospace Technology Support System include: Internet, Intranet and Virtual Private Network delivery channels, TCP, IP, HTTP and HTTPS service transports, and LDAP, Directory Services and DNS supporting network services.

NASA software and hardware standards require

Section 508 compliance and IT security services.

3.1.3.3 Partnerships

NASA has numerous partnering agreements with academic, commercial and governmental organizations. To the extent that the ARC Aerospace Technology Support System supports programs with such agreements, the investment leverages those agreements. For example, NASA provides significant research and technology support to the Federal Aviation Administration (FAA) in air traffic management and air traffic control. The FAA funds some of the supporting IT resources, and some of the IT resources ultimately become FAA property.

3.1.4 Security and Privacy

3.1.4.1 How is it provided and funded?

The CIO provides significant IT Security support for the ARC Aerospace Technology Support System through the IT Infrastructure, Office Automation and Telecommunications investment. This general IT Security support is funded by General and Administrative (G&A) and service pool funds, all of which are provided indirectly by the supported programs. In addition, the programs supported by the ARC Aerospace Technology Support System directly provide IT Security support, primarily via system and network administration functions. This direct IT Security support is included in this investment.

3.1.4.2 How is security accomplished?

The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures; when NIST completes this process NASA will revisit its policy and procedures to conform to NIST new guidance.

In the ARC Aerospace Technology Support System, hostile probes continue to increase at an accelerated rate but fewer incidents are occurring. This is mostly due to stricter firewall rules and IT Security policy and enforcement. Processes and procedures are in place to conduct scanning and monitoring on a continual basis. The incident response capability uses the skills of the System Administrators across the Center in coordinating responses to IT security incidents and evaluating vulnerabilities that were exploited and by sharing information and solutions with responsible IT security personnel. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. All contractors of the ARC Aerospace Technology Support System

and of the programs and projects supported by the system are subject to the following: Contractors' IT Security Plans and Procedures are issued within the contractually specified time after contract award, are incorporated within the relevant program or project's IT Security Plan, and are required to be updated every three years. These plans are required to be compliant with NPG 2810.1, NASA Procedures and Guidance for the Security of Information Technology, and are reviewed by the Ames Research Center IT Security Manager and the cognizant program or project manager.

3.1.4.3 Effective use of security, controls and authentication tools

Most systems of the Ames Research Center Aerospace Technology Support System do not permit public access. Those that allow public access do not contain or collect private information.

3.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

4 Ames Research Center (ARC) – NASA High End Computing Columbia

Project Description

The NASA Advanced Simulation (NAS) Program supports the scientific and modeling requirements of the entire agency. The NAS provides an integrated environment for simulation that includes high speed access to the cutting edge High-end Computing (HEC) platforms, assistance with application porting and scaling, storage, pre and post processing support, visualizations, training and on line and help desk support. The center provides a numerical simulation capability that allows NAS to initiate the most demanding projects in science and engineering while providing a capacity that insures that all the enterprises can pursue their highest priority projects with minimum interference. The program will enable factor of 10-100 advances in vehicle, earth, space and life sciences modeling.

To achieve NASA's mission objectives, NASA must:

- Design and develop advanced aerospace systems;
- Develop an in-depth understanding of Earth, planetary, solar, and deep-space systems; and
- Ensure the safe and effective human presence in a broad range of space environments.

These tasks have in common the need to rapidly develop in-depth and quantitative understanding of complex systems (engineering, physical, and biological systems, respectively). When physical experimentation is not possible, the burden falls on theoretical analysis. The theory governing these processes are often coupled non-linear partial differential equations that are not

amenable to “back of the envelope” solution. As a result, developing high-resolution solutions to these equations involves performing trillions of computations. Since these computations must be performed within the time constraints of ongoing development activities (e.g., vehicle design), results are often needed in hours or, at most, a few days.

To deliver the benefit of such computational modeling and simulation it is essential to have a high-performance computing and communications system tailored to meeting the specific requirements of the NASA community. This system must include sufficient and appropriate computing and computer communication assets as well as the software to support the porting, optimization, and execution of the computational code and the post-processing of the computational results.

The NAS Program is in the Planning phase of NASA’s CPIC process. It was approved by NASA’s Executive Council in June, 2004.

E-GOVERNMENT STRATEGY REVIEW

The NASA Advanced Simulation (NAS) Program continuously updates its E-Government resources to promote accessibility and functionality for our using publics. The NAS E-Government strategy includes the following primary initiatives:

- **Web Accessibility.** NAS provides browser-access mechanisms for our electronic products of interest to both external and internal users including a description of the program and program elements, various research projects, user support information, research papers as well as general press releases and NAS news updates.
- **Access Infrastructure.** NAS provides, supports, or participates in initiatives that provide enhanced network infrastructure, with the purpose of enhancing accessibility and connectivity among customers. Connectivity is provided by the NASA Internet, the Federal Internet Exchange (FIX) West, CENIC, NREN, Abilene, and in the future the National Lambda Rail.
- **Performance.** NAS works to provide enhanced network bandwidth; storage capacity and functionality; and processor performance to support better performance across all applications and users.
- **Security.** NAS is constantly reviewing and frequently enhancing system and network security facilities, to protect the integrity and accessibility of data products, applications, and systems. The NAS runs vulnerability scans and patches any and all identified weaknesses at least quarterly and often monthly or more frequently.

Architecture

4.1.1 Business

4.1.1.1 Process simplification/reengineering/design projects

No major projects. The NAS Program builds on the designs and engineering processes that have already demonstrated major improvements in NASA’s critical Aerospace vehicle, Earth Science

Space Science and Life Science applications and models.

No major process simplification/reengineering/design projects will be required as a specific part of this IT investment. Process simplification/reengineering/design projects currently occur throughout the life cycle of all supported NASA Enterprise (Aeronautics, Earth Science Exploration Systems, Space Flight, Space Science) programs.

4.1.1.2 Major organization restructuring, training and change management projects

No major projects. The current organization will be used to implement project and to insure continuous operations. The current yearly NAS Operational Process will be modified to reflect the transition from the allocation of scarce resource based on an indirect charging to a model that allows the Enterprises to determine the allocation based on mission critical requirements and science priority. NAS provides regular courses and training as well as on line info and a Help Desk. Specific support is provided in Porting, Scaling, Visualization, data management and code optimization.

No major organizational restructuring, training, and change management projects are currently planned. The NAS augments the existing ARC Aerospace Technology Support System that provides NASA mission/program related operational services to meet evolving engineering and development requirements. Organizational restructuring, training, and change management projects will continue to be accomplished throughout the life cycle of all supported NASA Enterprise (Aeronautics, Earth Science, Exploration Systems, Space Flight, Space Science) programs.

4.1.2 Data

4.1.2.1 Types of Data

The data is diverse and voluminous. The predominant data is matrices of numbers representing but not limited to observations or models of Aircraft, Aerospace Vehicles (Shuttle and Station), Earth's atmosphere & oceans, Solar, Galactic and Cosmological Systems, Biological Systems and Nanostructures and devices.

4.1.2.2 Existing Data Access

4.1.3 Application and Technology

4.1.3.1 Relationship to Service Component Model

Table 5

Service	Service Type	Component	New	Relation to SCRM of FEA
----------------	---------------------	------------------	------------	--------------------------------

Domain		Component	
Business Analytical Services	Analysis and Statistics	Yes	<p data-bbox="982 247 1443 384">Key Service Domain/Service Type/Components for NAS HPC systems, and their potential for sharing, include the following:</p> <p data-bbox="982 422 1443 1556">*Business Analytical Services Domain/Analysis and Statistics Type/Components - Modeling; Predictive; Simulation; Mathematical. NAS users, but not the NAS itself, are Aerospace, Earth and physical scientists and engineers that use NAS platforms to run large numerical simulations of physical systems such as the Earth's atmosphere and oceans and physical models such as the Space Exploration Vehicle. The users, not NAS, own the applications. NAS provides hardware, software tools (development tools, debuggers, compilers, mathematical libraries, etc.) and technical assistance services that are a platform for very complex mathematical models. Large user applications, sometimes running on hundreds or thousands of processors for hundreds of hours, demand the large-scale platforms that NAS provides. NAS purchases and administers systems that are specifically tuned for efficient processing of these models.</p> <p data-bbox="982 1593 1443 1900">* Digital Asset Services Domain/Knowledge Management Type/Components - Information Retrieval; Information Sharing; Knowledge Discovery. NAS provides network infrastructure and related services that promote knowledge and</p>

information discovery, retrieval, and sharing. NAS platforms and network services allow efficient (speedy) sharing of very large data sets across a suite of high performance network backbones and switches, web-accessibility to raw data (e.g., satellite observations), assimilated and modeled data sets (data product such as cyclical models of the global atmosphere and oceans), and intellectual capital (scientific research papers and the like). Although NAS users own the data, the NAS provides the infrastructure that allows the data to be stored, retrieved, and shared.

* **Back Office Services Domain/Data Management Type/Components - Data Exchange; Data Warehouse; Extraction and Transformation; Loading and Archiving; and Data Classification.** The NAS mass storage subsystems have a total capacity exceeding 16 Petabytes of storage. NAS provides hierarchical storage subsystems (tape silos, disks, servers, network infrastructure, and system software) that securely store and swiftly retrieve very large data sets. NAS is evolving its storage platforms using customized and commercial (e.g., SGI DMF) software products to serve the NASA engineering and research user communities better.

The NASA's research users are deeply involved in the world wide Earth science community,

which has evolved its own mechanisms for sharing (not only the products, but in some cases the actual models, analyses, and data).

The NAS engages in information sharing of various kinds. These include conference calls with users of similar systems, participation and leadership at supercomputing, mass storage, security, and other relevant conferences and in vendor users groups, informal contacts of various kinds within the supercomputing data center community, report and paper writing and reading, Co-PI's on various research proposals, and across other channels.

The best matches to the Service Component Reference Model are in the area of COTS software. Software packages such as operating systems, editors, compilers, debuggers, dispatchers, schedulers, file system software, storage area network software, communications packages, math and physics libraries and the like are shared service components, with the sharing mediated by the software vendor. (This also includes freeware.)

Business Analytical Services	Analysis and Statistics	Yes
Business Analytical Services	Analysis and Statistics	Yes
Digital Asset	Knowledge Management	Yes

Services		
Digital Asset Services	Knowledge Management	Yes
Digital Asset Services	Knowledge Management	Yes
Back Office Services	Data Management	Yes
Back Office Services	Data Management	Yes
Back Office Services	Data Management	Yes
Back Office Services	Data Management	Yes

4.1.3.2 Relationship to Technology Component Model

Table 6

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access and Delivery	Access and Channels	Other Electronic Channels	System-to-System: Within the NAS, several hardware and software components must dialogue directly. This includes heartbeat monitoring to ensure high availability of critical storage and compute servers, Automated Cartridge System Library Software (ACSL) servers directing the storage silos and tape drives, and CTMS monitoring services.
Service Access and Delivery	Delivery Channels	Intranet	The following devices are used within the NAS: GigE, ATM, 10GB Ethernet, Infinaband, and 10/100 Ethernet.
Service Access and Delivery	Delivery Channels	Peer to Peer (P2P)	These include the hardware and software components discussed

Delivery

above relating to system-to-system access including heartbeat monitoring, ACSLS servers, and monitoring services.

Service Platform and Infrastructure

Supporting Platforms

Platform Dependent

Linux (Red Hat) are used on SGI Altix and Cray Opteron. IRIX is the operating system on the SGI Origin systems. Solaris is the operating system on the Sun systems. Linux (Red Hat and Debian) are used on several servers. UNICOS is used on Cray X1 System.

Service Platform and Infrastructure

Software Engineering

Integrated Development Environment (IDE)

Compilers - Fortran, C, C++, JAVA. Message Passing - Message Passing Interface (MPI), MLP, OpenMP, Shmem, Pthreads On many of the platforms at the NAS, proprietary debuggers, compilers, libraries, and more are used to assist application developers. TotalView is a commercial debugger that is used at the NAS on both the Cray and SGI machines.

Service Platform and Infrastructure

Software Engineering

Test Management

Proprietary performance profilers are also used on the High End Computers (HEC) at the NAS. Commercial codes such as Vampir and VampirTrace are used to analyze message passing applications. The NAS benchmark suite is used for functional and performance testing for new technologies.

Service Platform and Infrastructure

Database / Storage

Network Attached Storage (NAS). Storage Area Network (SAN). Data Migration Facility (DMF). Storage Resource Broker (SRB)/Metadata Catalog (MCAT) is used by the NAS to provide both the user community and the NAS with better tools to manage data. Users will be able to easily access and manage their mass storage archives remotely from SRB enabled platforms in a secure manner, regardless of the underlying physical devices on which the data is stored or

			underlying storage management software system.
Service Platform and Infrastructure	Hardware Infrastructure	Servers / Computers	Columbia: SGI Altix, Altix2: SGI Altix, Lomax: SGI Origin 3000, Turing: SGI Origin 3000, Mars: SGI Origin 3000, Venus: SGI Origin 3000, Lou: SGI Origin 3000, used for DMF, Susan: SGI Origin 3000, used for DMF, SGI Origin 300's are used as CXFS management servers.
Service Platform and Infrastructure	Hardware Infrastructure	Storage	StorageTek (STK) Silos, STK Tape Drives, 9840A Ultra SCSI, SGI Disk Arrays, Peripherals, Printers, Scanners,
Service Platform and Infrastructure	Hardware Infrastructure	Network Devices / Standards	Hubs, Switches, Routers, NICs, Firewall, GigE, ATM, 10/100 Ethernet.
Component Framework	Security	Peripherals	Secure Sockets Layer (SSL), Peripherals Supporting Security Services, Transport Layer Security (TLS), TCP/IP Wrappers, Secure Shell (SSH), Firewall, Secure ID, Access Control Lists (ACL) used on all systems and network devices, Log Hosts centralize logging of activities on the machines, Continuous scanning for vulnerabilities, Minimal network services are configured on all the machines, Private networks are used for all consoles and network infrastructure.
Component Framework	Business Logic	Platform Independent	C/C++, JavaScript
Component Framework	Data Interchange	Data Exchange	Hierarchical Data Format (HDF), IEEE binary data formats
Component Framework	Data Management	Database Connectivity	Remedy AR database is used for knowledge management and help desk activities. The various databases used for mass storage also include tools for obtaining information about and managing data. These include the internal, application specific databases for

			DMF; MCAT/SRB.
Service Interface and Integration	Integration	Middleware	Remote Procedure Call (RPC), UDP, MPI, OpenMP, Shmem, MCAT/SRB, MLP.
Service Interface and Integration	Interoperability	Data Format / Classification	MCAT/SRB.
Service Interface and Integration	Interoperability	Data Types / Validation	Database Schema.
Service Interface and Integration	Interface	Service Discovery	

4.1.3.3 Partnerships

There exists an international community of research scientists and engineers that share diverse components and applications, including both data and programs, across the Government and globally. This includes scientists that are users of NAS systems. (The scientists own the software components and applications, but use the NAS.) The Earth System Modeling Framework (ESMF) is a good example of a joint effort of NAS, JPL, NASA Goddard, and other agencies to leverage application components across the Government.

4.1.4 Security and Privacy

4.1.4.1 How is it provided and funded?

The CIO provides significant IT Security support for the ARC Aerospace Technology Support System through the IT Infrastructure, Office Automation and Telecommunications investment. This general IT Security support is funded by General and Administrative (G&A) and service pool funds, all of which are provided indirectly by the supported programs. In addition, the programs supported by the NAS directly provide IT Security support, primarily via system and network administration functions. This direct IT Security support is included in this investment.

4.1.4.2 How is security accomplished?

The Project complies with the NASA Procedures and Requirements (NPR) 2810.1. This NPR is NASA's IT Security Procedures Guide. This NPR employs standards requirements and guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPR 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge

and that NIST is revising their procedures; when NIST completes this process NASA will revisit its policy and procedures to conform to NIST new guidance.

This system is supported by the Agency and Center implementation of a defense-in-depth approach: IT Security policy, procedures and enforcement; IT Security training and awareness; use of IT Security technologies (e.g., firewalls, intrusion detection, scanning and monitoring); and reporting within the NASA Incident Reporting Database system. The incident response capability utilizes the skills of Certified System Administrators who coordinate responses and collaborate with the Center's IT Security Incident Response Team. All incidents are reported to Center Information Technology Security Manager, Center Counter Intelligence, Office of Inspector General, and other federal agencies as appropriate (e.g., FBI, DHS' Fed CIRC., etc.).

The system is operated by contractors. All contracts include specific security requirements required by law and policy. All contractors of the NAS program and of the programs and projects supported by the system are subject to the following: Contractors' IT Security Plans and Procedures are issued within the contractually specified time after contract award, are incorporated within the relevant program or project's IT Security Plan, and are required to be reviewed annually, tested, and updated every three years. These plans are required to be compliant with NPR 2810.1, NASA Procedures and Requirements for the Security of Information Technology, and are reviewed by the Ames Research Center IT Security Manager and the cognizant program or project manager. These plans are approved by the IT Security Manager, the Chief Information Officer, and Line Manager.

4.1.4.3 Effective use of security, controls and authentication tools

Most systems of the NAS do not permit public access. Those that allow public access do not contain or collect private information.

4.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

5 Goddard Space Flight Center (GSFC) – Earth Observing Sys Data Info Systems

Project Description

The Earth Observing System (EOS) Data and Information System (EOSDIS) is a comprehensive distributed system designed to support NASA's EOS. EOSDIS archives, manages, and distributes Earth science data from NASA missions and provides spacecraft control and science data processing for the EOS missions. EOSDIS has been archiving and distributing pre-EOS

data since 1994. Currently EOSDIS supports both the pre-EOS and EOS data. EOSDIS has been distributing Earth Science Enterprise (ESE) data to a broad user community, enabling research, applications, education and policy analysis. EOSDIS is now supporting Aura mission that was launched in July 2004. It is an essential component of NASA's Earth science program in order to ensure that the valuable data from its Earth observing satellites are captured, preserved and made available to the user community for scientific research and applications of national importance. A large community has now become accustomed to data and information products from EOSDIS as evidenced by the number of users of EOSDIS (over 2.3 million accessing and over 280,000 ordering data in FY 2003 and similar statistics expected in FY 2004). The users have been very satisfied with EOSDIS, according to a recent survey. The American Customer Satisfaction Index (ACSI) of the customers of EOSDIS was 75, compared to the federal government average of 71. EOSDIS has the following external dependencies. The data from EOSDIS will be transitioned to NOAA and USGS for permanent archiving. For its success, EOSDIS depends on the network infrastructure that exists in the US to provide the data to the users. These consist of both NASA's internal networks and networks funded and managed by other entities (E.g., NSF). International partners' contributions to the overall interoperable data system are also important to the success of EOSDIS.

The spacecraft and instrument operations, data capture, low-level telemetry processing, and the supporting networks have now been transitioned to mission operations personnel and will no longer be reported as a part of this investment.

It is not meaningful to provide Government FT E costs for PY-1 and prior, since we were not in full-cost accounting mode for those years. The Project is expected to go beyond the budget horizon of FY 2010. However, the outlays in FY 10 and beyond column reflect just the carryover of FY 10 funds into FY 11.

Most of EOSDIS is in its operational phase of the life cycle. EOSDIS is evaluated regularly on an annual basis as a part of all of the Earth Science Enterprise's programs by ESE's FACA committee – Earth System Science and Applications Advisory Committee (ESSAAC). These reviews result in advice to the Associate Administrator of ESE on continuation, modification and/or reprioritization of programs. Specifically, EOSDIS is reviewed by a subcommittee of ESSAAC – the Earth Science Information Systems Subcommittee. The last such review was held during February 17-18, 2004. It was determined that EOSDIS is meeting value and budget objectives and a decision to continue funding has been made, subject to the annual Program Operating Plan process that makes budget decisions.

The Earth Observing System Data and Information System (EOSDIS) is a comprehensive distributed data and information system designed to support NASA's Earth Observing System (EOS). It supports NASA's mission to "advance and communicate scientific knowledge and understanding of the Earth, the solar system, and the universe" as stated in NASA's Strategic Plan, 2000, by supporting the Earth Science Enterprise's (ESE) mission to "develop a scientific understanding of the Earth system and its response to natural and human-induced changes to enable improved prediction of climate, weather, and natural hazards for present and future generations." In order to accomplish this mission, the satellite data of the past, present and future need to be well organized, preserved, and made accessible to scientists who can derive information and knowledge from the data. The data and information need to be made available

to the applications community that adds further value for the benefit of the nation and the world. EOSDIS is the key system in the ESE that performs the end-to-end functions in ensuring that the value of ESE's missions is fully realized by the community.

The functions of EOSDIS that support the ESE's mission are: to archive, manage, and distribute Earth science data from NASA missions and provide spacecraft control and science data processing for the EOS missions. For EOS spacecraft and instruments, the EOSDIS provides the capabilities for mission operations for instrument and spacecraft control, acquisition, capture and processing of telemetry data, and processing of telemetry data into higher level science data products, archiving and distribution of standard science products. Landsat-7 has now been operating for over five years. Terra has been operating for over four years. Aqua has been operating for over two years. EOSDIS has been successfully supporting their operations. The mission operations capabilities (spacecraft and instrument control, data capture and low level telemetry processing and networks to support these), developed under this investment in prior years, have now been fully transitioned into operations and will no longer be reported here. The science data processing, archival and distribution will continue to be reported as a part of this investment.

The data holdings of EOSDIS are growing at a rate of over 3.5 terabytes per day. At the end of FY 2003, the archives of EOSDIS held over 2.3 petabytes of data and over 30 million data granules (smallest units of data kept track of by the databases). There are over 2100 distinct types of data products in the archives of EOSDIS. EOSDIS has been distributing ESE data to a broad user community, enabling research, applications, education and policy analysis. The community includes:

- Instrument teams for EOS spacecraft
- Research scientists
- Applications users
- Federal, state and local governments
- Education community
- Commercial remote sensing community
- General public

During FY03 over 2.3 million distinct users accessed the Distributed Active Archive Centers (DAACs) funded by the EOSDIS Program. Over 230,000 users obtained data. Over 25 million data products were provided by the DAACs to users.

A study of EOSDIS customers was performed by Claes Farnell International (CFI) Group and concluded in May 2004. This study is titled "American Customer Satisfaction Index (ACSI): NASA EOSDIS Customer Satisfaction Study". This study indicates that the Customer Satisfaction Index for EOSDIS is 75, which is four points higher than the 2003 ACSI for the Federal Government overall.

Architecture

5.1.1 Business

5.1.1.1 Process simplification/reengineering/design projects

As a multi-mission data and information system needed to support a series of Earth science satellite missions, EOSDIS has undergone a rigorous, multiphase development process typical of large NASA initiatives. It started with an in-house Phase A conceptual study, two parallel Phase B studies by Hughes and TRW, and a design and implementation phase. The system architecture and design has evolved over time. For example, during the Phase A study, the architecture was centralized, with two data centers managing all the data. During the Phase B studies, after trade studies and significant reviews and discussions with the user community, it was determined that the programmatic goals would be best served by using a more distributed implementation with eight Distributed Active Archive Centers (DAACs) that were discipline-focused.

Implementation methodology involved significant prototyping, including a multi-site interoperability prototype called Version 0 EOSDIS. Lessons learned from Version 0 were used in the subsequent versions of EOSDIS. In general, the historical and anticipated future evolution of EOSDIS, is simplifying the overall implementation by increasing the number of implementing partners and working with well-defined interfaces. This is evidenced by the number of DAACs, the Federation Experiment, distribution of standard data production responsibility to the Science Investigator-led Processing Systems (SIPs), and the recommendations from the study on Strategic Evolution of Earth Science Enterprise (ESE) Data Systems (SEEDS).

An example of simplification/reengineering is the use of an adaptive approach to processing for generating standard data products from EOS instruments. At the outset, the plans were to generate all the standard products at the DAACs using the EOSDIS Core System (ECS – a “core” common set of hardware and software capabilities developed under a large contract) by integrating algorithmic software provided by the scientists responsible for the respective instruments. It was recognized that this would lead to a complex system design and complicated interactions between the ECS and the instrument teams. Significant simplifications were achieved by providing the instrument teams an option to generate standard products using SIPs under their direct control, and defining a common interface with EOSDIS Core system (ECS) to deliver the data products to the DAACs where they are archived.

5.1.1.2 Major organization restructuring, training and change management projects

Organization restructuring: As a data and information system supporting the EOS series of satellite missions in the early 1990’s, EOSDIS went through several restructuring activities along with the restructuring of the overall EOS Program for the purposes of reducing costs. These were conducted through several reviews internal and external to NASA and with full participation and advice from the scientific user community. The EOS Program and, correspondingly, EOSDIS have had reorganizations to match the evolving programmatic needs.

Most of the overall funding appropriated for EOSDIS is managed by the Earth Science Data and Information System (ESDIS) Project at the Goddard Space Flight Center (GSFC) while the rest of the funding is managed directly by NASA HQ Earth Science Enterprise (Code Y). The ESDIS Project has been under different organizational structures at different times since its inception in 1990. Initially it was under the EOS Project (Code 420) at GSFC, and

programmatically reported to the EOSDIS Program Manger at HQ. The EOS Program management moved from NASA HQ to GSFC as a part of overall downsizing of HQ. A Mission to Planet Earth Office (Code 170) was established at GSFC, with the ESDIS Project reporting technically to this office. This office was later replaced by three Program offices at Goddard, JPL, and Langley Research Center. The ESDIS Project has remained at Goddard and reports to the Goddard EOS Program (Code 420).

As indicated above, the Phase B studies led to organizational assignments for processing, archiving and distributing scientific data products at eight DAACs. The budget and work assignments to these DAACs are given by the ESDIS Project and the Project manages their activities with regular communications and progress reporting.

Training from the point of view of keeping up with evolving technologies, prototyping has been an active part of the history of EOSDIS. The staff responsible for EOSDIS keeps up with technologies by participating in prototyping activities, leading and/or participating in technical conferences and interagency/international standards organizations. Examples of such activities are:

- Software Engineering Institute training courses
- Earth Science Mark-up Language Workshop
- Annual workshops on Hierarchical Data Format Earth Observing System (HDF-EOS)
- Annual meetings of the American Geophysical Union (present papers, posters, organize sessions)
- Hands-on workshops on EOS Data Gateway (EDG) and EOS Clearing House (ECHO)
- Annual meetings of the Society of Photo-optical Instrumentation Engineers (SPIE)
- Annual meetings of the IEEE Geosciences and Remote Sensing Society (IGARSS)
- Hardware vendors' Workshops
- NASA's in-house annual computer security training

On the average, each individual in the Project participates in such activities two to three times a year.

5.1.2 Data

5.1.2.1 Types of Data

EOSDIS is a multi-mission system dealing with scientific and engineering data from satellites. By their very nature, all the data originate electronically and are maintained electronically throughout the data life cycle. The data are geospatial. The raw data from the satellites are acquired as swaths along the satellite tracks. They include multi-spectral images of land and oceans, atmospheric soundings, etc. The raw data are converted using scientific algorithms into calibrated radiances, geophysical parameters, mapped onto spatial and temporal grids, and are used in models.

5.1.2.2 Existing Data Access

EOSDIS acquires data from NASA's Earth observing satellites, uses ancillary data from other federal agencies (NOAA and USGS) and scientific algorithms from NASA-funded Earth scientists to produce, archive and distribute scientific data products.

5.1.3 Application and Technology

5.1.3.1 Relationship to Service Component Model

Table 7

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Process Automation Services	Tracking and Workflow		No	The service domains, service types and components EOSDIS are not a natural fit to the Service Component Reference Model, since EOSDIS is a data and information system that processes, archives and distributes large quantities of global, satellite-acquired geophysical data. The discussion of the SRM tends to focus on business IT systems. However, service domains, service types and components EOSDIS can be mapped into the SRM with the following substitutions: Documents referenced in the SRM generally correspond to satellite acquired and processed digital data products. The "business cycle" of the SRM corresponds to satellite design life and data life cycle. Given this, EOSDIS is active in the Process Automation Services Domain, especially in the Tracking and Workflow service type

– most of the processes for handling the terabytes a day of data products are automated. Business Management Services in SRM corresponds to Project Management in EOSDIS. Automated and web-based processes exist in the ESDIS Project that map to the Management of Process service type of the SRM. Similarly, there are components in the ESDIS Project that map to Organizational Management service type. The web-based configuration management system used in the ESDIS Project, for example, is a Requirements Management component as well as a Workgroup/Groupware component. There are some aspects of Supply Chain Management service in EOSDIS as well. Treating the supply chain here as the chain starting with the satellite data acquisition and ending with the research scientist or an applications' user, there are several automated capabilities in EOSDIS at the head of the chain to cover: planning and scheduling acquisition of data and generation of derived data products; managing the catalog and inventory of the data products (Catalog Management); and facilitating users' searches and ordering (Ordering/Purchasing; Storefront/Shopping Cart).

The digital data products produced by EOSDIS are a result of many scientific Principal Investigators' research and peer-reviewed algorithms. As such they constitute significant investment by NASA and intellectual capital. With this definition, EOSDIS fits well in the Digital Asset Services Domain of the SRM. Relevant service types and components in this domain are: Content Management (Tagging and Aggregation), Document Management (recall "document" in SRM maps to "digital data products" in EOSDIS – Library/Storage, Document Review and Approval, Document Conversion, Indexing, Classification), Knowledge Management (Information Retrieval, Information Mapping/Taxonomy, Information Sharing, Knowledge Capture). In conducting its business, the EOSDIS Project uses most of the components listed under the Support Services Domain of the SRM in some form or the other. The Customer Services Domain is a direct mapping since EOSDIS does have a large customer community and provides components supporting Customer/Account Management, Customer Feedback, and several components under the Customer Initiated Assistance including On-

Line Help, On-line Tutorials,
Self-Service and
Assistance Request.

Business Management Services	Management of Process	No
Business Management Services	Management of Process	No
Business Management Services	Organizational Management	No
Business Management Services	Supply Chain Management	No
Business Management Services	Supply Chain Management	No
Digital Asset Services	Content Management	No
Digital Asset Services	Document Management	No
Digital Asset Services	Document Management	No
Customer Services	Customer Initiated Assistance	No

5.1.3.2 Relationship to Technology Component Model

Table 8

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access and Delivery	Access Channels	Collaboration Communication	EOSDIS has been developed through several versions starting with Version 0 to the Version 3 through extensive interaction with the users and definition of data, applications and hardware requirements.

EOSDIS Version 0 was developed during 1990 through 1994 as a collaborative effort between the ESDIS Project and eight geographically distributed active archive centers (DAACs). EOSDIS is a highly distributed system including the DAACs, Science Investigator-led Processing Systems (SIPs) and several other components as discussed below.

EOSDIS addresses in some form all the Service Areas in the Technical Reference Model, including Service Access and Delivery, Service Platform and Infrastructure, Component Framework, and Service Interface and Integration.

Service Access and Delivery: EOSDIS makes extensive use of Web Browser access, Electronic Mail, public and private networks, user authentication, and an extensive array of network protocols and standards including but not limited to IMAP/POP3, TCP/IP, HTTP, and HTTPS.

Service Platform and Infrastructure: EOSDIS provides Web delivery Servers, uses extensive Software Engineering practices including Software Configuration Management, Test Management, and UML based Modeling, and uses Sybase database technology. EOSDIS makes extensive use of robotically controlled tape storage silos (not itemized in the Technical Reference Model), as well as direct attached disk storage. The hardware infrastructure is server based,

uses RAID storage, and standard WAN and LAN protocols and components.

Service Access and Delivery	Access Channels	Other Electronic Channels	
Service Access and Delivery	Access Channels	Other Electronic Channels	
Service Access and Delivery	Access Channels	Other Electronic Channels	
Service Access and Delivery	Delivery Channels	Internet	
Service Access and Delivery	Delivery Channels	Intranet	
Service Access and Delivery	Delivery Channels		
Service Access and Delivery	Service Requirements	Legislative Compliance	/
Service Access and Delivery	Service Requirements	Legislative Compliance	/
Service Access and Delivery	Service Requirements	Legislative Compliance	/
Service Access and Delivery	Service Requirements	Hosting	
Service Access and Delivery	Service Transport	Supporting Network Services	
Service Access and Delivery	Service Transport	Supporting Network Services	
Service	Service	Service	

Access and Delivery	Transport	Transport
Service Access and Delivery	Service and Transport	Service Transport
Service Access and Delivery	Service and Transport	Service Transport
Service Platform and Infrastructure	Supporting Platforms	Platform Independent
Service Platform and Infrastructure	Supporting Platforms	Platform Dependent
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management

Infrastructure

Service Platform and Infrastructure Software Engineering Test Management

Service Platform and Infrastructure Software Engineering Modeling

Service Platform and Infrastructure Software Engineering Modeling

Service Platform and Infrastructure Database Storage / Database

Service Platform and Infrastructure Database Storage / Database

Service Platform and Infrastructure Database Storage / Storage

Service Platform and Infrastructure Hardware Infrastructure / Servers Computers /

Service Platform and Infrastructure	Hardware Infrastructure	/	Embedded Technology Devices
Service Platform and Infrastructure	Hardware Infrastructure	/	Wide Area Network (WAN)
Service Platform and Infrastructure	Hardware Infrastructure	/	Local Area Network (LAN)
Service Platform and Infrastructure	Hardware Infrastructure	/	Network Devices / Standards
Service Platform and Infrastructure	Hardware Infrastructure	/	Network Devices / Standards
Component Framework	Security		Certificates / Digital Signature
Component Framework	Security		Supporting Security Services
Component Framework	Presentation Interface	/	Static Display
Component Framework	Business Logic		Platform Independent
Component Framework	Business Logic		Platform Independent
Component Framework	Data Interchange		Data Exchange
Component Framework	Data Interchange		Data Exchange
Component Framework	Data Management		Database Connectivity
Service Interface and Integration	Integration		Middleware
Service Interface and Integration	Interoperability		Data Format / Classification

Service Interface and Integration	Interoperability	Data Types / Validation
Service Interface and Integration	Interoperability	Data Types / Validation
Service Interface and Integration	Interface	Service Discovery
Service Interface and Integration	Interface	Service Description / Interface
Service Interface and Integration	Interface	Service Description / Interface

5.1.3.3 Partnerships

For performing its infrastructure business functions, the ESDIS Project will utilize as appropriate the services provided by the Federal Geospatial One Stop initiative and other Federal E-Government initiatives.

5.1.4 Security and Privacy

5.1.4.1 How is it provided and funded?

The program office funds the Project for all of its activities including providing security. The Project has a Computer Security Official responsible for the following IT security activities:

1. Work with system and project managers to make sure IT security is implemented as a system life cycle process incorporating Center, Agency and Federal Requirements and Regulations.
2. Lead a contractor team that performs independent IT security assessment and provides reports and feedback to system and project managers. Independent assessments are performed twice a year to review that project IT resources have:
 - a. An assigned Security Point of Contact;
 - b. Up-to-date IT security documentation that adequately addresses:
 - c. Risk Assessment
 - d. Risk Management,
 - e. Risk Management,
 - f. Security Planning
 - g. Contingency Planning

- h. Up to date authorizations to process
- i. IT security banners on the systems
- j. Rules of Behavior provided to users requiring system accounts
- k. Users and system operators with the appropriate level of IT security training
- l. System operators who have undergone personnel screening
- m. Appropriate physical access controls.
- n. Appropriate limitations to access by foreign nationals.

In addition, the assessment team performs network based IT security vulnerability assessments, and works with system owners and operators to turn off unnecessary services, patch vulnerable necessary services or alternatively mitigate significant system vulnerabilities.

- 3. Monitor project information for sensitive unclassified information or EAR/ITAR and work with information owners to make sure such information is appropriately restricted.
- 4. Monitor project networks for configuration changes that could significantly weaken the project IT security posture (e.g. routing policy, access control list, firewall rule validation, verification & implementation).
- 5. Operate as project liaison between Center/Agency regarding changing IT security policy and procedures, including perimeter protection, personnel screening, foreign national & International Partner system access
- 6. Monitor project networks for malicious attacks and intrusion detection; and work with the Center and OIG regarding any project IT security incident.

5.1.4.2 How is security accomplished?

The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire life cycle of the project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures. When NIST completes this process NASA will revisit its policy and procedures to conform to NIST new guidance.

It is the responsibility of the Security Point of Contact/ System Administrators to regularly monitor logs for anomalous behavior and to report to the Project Computer Security Official, Center IT Manager and the NASA Automated Systems Incident Response Capability (NASIRC). All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. The Project uses an independent validation and verification (IV&V) contractor to assess the contractors' security posture and report to the contractor, ESDIS System Manager and ESDIS Project Manager for corrective action (if necessary).

5.1.4.3 Effective use of security, controls and authentication tools

One of the main purposes of EOSDIS is to disseminate NASA's Earth science data as widely as possible to a broad user community. There are parts of the system that are visible and accessible to the public to achieve this purpose. Thus, a member of the public can access, using a web address, information about EOSDIS' data holdings, browse through the data and order specific data products. However, mission critical elements of EOSDIS and the data archives themselves are separated from the publicly accessible servers by appropriate firewalls. The access to these parts of EOSDIS is limited to authorized personnel only with proper authentication.

5.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

6 Goddard Space Flight Center (GSFC) – Hubble Space Telescope Mission Ops IT

Project Description

The Hubble Space Telescope has been in an operations phase since launched on April 24, 1990. Four successful servicing missions have made dramatic improvements in the telescope. The planned investment is to keep the system functioning smoothly through the remainder of the Hubble Space Telescope mission. All funding for the Hubble Space Telescope comes from NASA, which is fully responsible for the maintenance of the satellite. The Hubble Space Telescope is unmatched by any ground based or space borne observatory. The demand for Hubble Space Telescope observing time by the worldwide science community is increasing. The Hubble Space Telescope Project is in the Operations phase of NASA IT Capital Planning and Investment Control (CPIC) process, and this IT investment is managed as a component of the NASA Project under NASA's NPG 7120 process.

The planned investment is for hardware and software maintenance and support, to keep the system functioning smoothly through the remainder of the Hubble Space Telescope mission, currently planned to end in 2010. The Hubble Space Telescope Operations Project will continue ground system development and maintenance of the highly distributed, commercial-off-the-shelf-based ground system. The investment supports core mission functions of the Space Science Enterprise. Continued funding is required because no alternative private sector or other government source can efficiently support the function.

The HST Program is re-assessing program plans due to the cancellation of Servicing Mission 4 on January 16, 2004. Development of the Cosmic Origins Spectrograph is complete. Wide Field Camera 3 (WFC3) development continues on the existing plan.

Based on HST spacecraft hardware reliability projections, the probability of continued HST science operation decreases to approximately 50% by the end of calendar year 2005. To extend the life of HST science operations beyond that time, the program is implementing methods to extend the operational life of HST, e.g., development of a 2-gyro control mode for science

operations and optimizing battery management.

A privacy impact statement is not required since the Hubble Space Telescope stores no personal data.

Architecture

6.1.1 Business

6.1.1.1 Process simplification/reengineering/design projects

Vision 2000

The Command and Control System (CCS) is a ground-based system that, among other things, sends commands to the Hubble Space telescope (HST). These commands control the spacecraft including its orientation and the activity of the scientific instruments on board. Another major function of CCS is to monitor the health and safety of the HST by continuously analyzing the incoming signals from the spacecraft. The goals of Vision 2000 include increased automation, and a more maintainable architecture.

The program is engaged in developing Life Extension capabilities for the spacecraft. If critical spacecraft hardware degrades or fails, such as batteries or the gyros of which a minimum of 3 are required to perform science operations, the HST mission may not complete all expected high priority science programs. Teams are working on extending the battery capacity and optimizing their use; and implementing a 2-gyro science capability.

6.1.1.2 Major organization restructuring, training and change management projects

Teams are being reorganized to work the HST Life Extension initiatives. They will be addressing the use of 2 gyros to complete science mission objectives and optimizing the use of the batteries onboard the spacecraft.

6.1.2 Data

6.1.2.1 Types of Data

The HST Project deals with scientific data from the satellite. All of this data originates electronically and is maintained by the Space Telescope Science Institute and Principle Investigator.

6.1.2.2 Existing Data Access

6.1.3 Application and Technology

6.1.3.1 Relationship to Service Component Model

Table 9

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
				<p>The Hubble Space Telescope program relates to the Support Services Domain of the Service Component Reference Model. Security management is a major focus for the program. Identification and authentication, access controls, encryption, intrusion detection, verification, user management, role/privilege management, and audit trail capture and analysis are managed in accordance with the NASA Procedure and Guideline 2810.1. User collaboration is through a variety of methods on HSTNet (email and document sharing) and the CNE (threaded discussions and shared calendaring). Communications between users is being developed in a way that assures data protection. We are looking at ways to provide chat and instant messaging to users for work purposes. Audio and Video conferencing is used in meetings to offset the need for travel. The HST Network is monitored by a system that will notify the appropriate administrators if a system were to go down or have a non-routine event. And System administrators use group management tools to effectively set up user accounts and manage access to data on the network. All system administrators follow procedures to maintain and track software licenses. We do some adhoc creations of forms and use electronic forms created and/or approved by the agency.</p>

- *Relationship to Technology Component Model*

Table 10

Service Area	Service Category	Service Standard	Relation to SRM of FEA
--------------	------------------	------------------	------------------------

The Hubble Space Telescope program relates to the Technical Reference Model section of the FEA in many ways. At this time, in the core area of Service Access and Delivery we support both the Internet Explorer and Netscape browsers, Wireless/PDA palm pilots, Electronic Mail, fax, web services and URL. We use Internet, Intranet and Virtual Private Networking as delivery channels. We comply with the legislative/compliance standards for Section 508, web content accessibility, and security. We support authentication and single sign-on (in appropriate areas) and host sites internally and externally. We use a variety of network services and service transport protocols - IMAP/POP3, MIME, SMTP, H323, SNMP, LDAP, DHCP, DNS, TCP, IP, HTTP, HTTPS, WAP, FTP, and IPSEC. Our service platform infrastructure is platform dependent on Windows 2000. Our delivery servers use either Apache or Internet Information Server to deliver web information. We do not support Real Audio or Windows Media Service media servers. We have internal to the program application and portal servers. Software engineering for the program covers all software configuration management and test management service specifications. Database storage is either on Oracle or SQL server. We do use Network Attached Storage. Our hardware infrastructure contains Enterprise Servers with RAM, Hard Disks, Microprocessors, RAID, printer, scanners, frame relay and ATM, using an Ethernet network with multiple VLANs. The network uses a variety of hubs, switches, routers, nic, transceivers, gateways and firewalls. We have a T1 connection to an offsite contractor. We use a Bridge and codec for our video conferencing over IP. We use Digital Certificate Authentication as well as FIPS 186 and SSL for security. We use TLS and SSH to support these. We use static html as a presentation interface. Visual basic and VB scripting tools are used.

6.1.3.2 *Partnerships*

None.

6.1.4 Security and Privacy

6.1.4.1 How is it provided and funded?

HST has an IT Security clause to all of its contracts. Each contractor is responsible for conducting risk assessments of their environments and the services they are responsible for providing. Also, any new services are required to adhere to this clause. HST has IT SECURITY GROUP who ensures and maintains the security of the HST network. They provide proactive network scans for vulnerabilities, work closely with system administrators assessing system requirements, work with the Center Information Technology Security Manager to address any security issues or incidents, review all configuration changes for impact on the overall security posture, and work with NISN to identify any unauthorized use. Based on the information level of the Data Processing Installation (DPI), this SMA exceeds NIST and NPR 2810 guidelines relative to authentication. Funding comes from the direct funds allocated to the HST Program and funded out the HST Program Office. Also, funding supports security.

6.1.4.2 How is security accomplished?

The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures. When NIST completes this process, NASA will revisit its policy and procedures to conform to NIST new guidance.

When a security incident takes place on the HST Network, HST IT Security team applies appropriate resources to eliminate risk to the government systems. Support to investigations by government agencies is primarily the responsibility of the HST IT Security team. The team expertly prepares, deploys, and maintains systems that greatly enhance intrusion detection capabilities on the HST network. The team also continues to improve the filters of the intrusion detection systems and therefore the efficiency of the systems and alerts to NASA, which interfaces with FedCIRC. The Organizational Computer Security Official tracks any incidents and provides status reports to project management. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. The Contractors' security procedures are monitored, verified, and validated by regulations set forth by the agency and administered by the HST Civil Servant management team and the Center Security Support Services.

6.1.4.3 Effective use of security, controls and authentication tools

This is not applicable. The Hubble Space Telescope investment does not handle personal information.

6.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

7 Goddard Space Flight Center (GSFC) – NASA Center for Computational Services (NCCS)

Project Description

The NASA Center for Computational Sciences (NCCS) supports primarily scientific modeling in the Earth sciences. The NCCS' high performance computer systems, mass data storage systems, and high performance networks serve about 1,000 users. NCCS is an ongoing operational data center, but most of NCCS funds are classified as DME (planning and acquisition) rather than Steady State. This is primarily because the purchase prices of new systems, which are replenished every few years, are much greater than system maintenance costs. Consequently, the NCCS investment is Mixed life cycle. The overall investment has been reviewed on August 13, 2004 by the Program Management Council (PMC) and the NASA headquarters OCIO as part of the NASA CPIC control processes. The investment is meeting its value objectives and a decision to continue funding has been made.

(Most hardware assets have an approximate three year lifecycle. NCCS constantly refreshes and updates its suite of hardware, software, mass storage, and network infrastructure, consistent with resource availability.)

NCCS supports scientific modeling research in the Earth, space, life, and microgravity sciences. The NCCS is a key resource in the effort to restore international leadership to the U.S. program in weather and climate prediction to increase understanding of Earth's climate system, natural and human influences on climate, and consequences for life on Earth. NCCS system applications will lead to greater understanding of the Earth system, the solar system, and the universe through computational use of space-borne observations and computer modeling. The three largest Earth Science projects that the NCCS supports are the Data Assimilation Office (DAO), the NASA Seasonal to Interannual Prediction Project (NSIPP) (Note: DAO and NSIPP merged as the GMAO - Global Modeling and Assimilation Office), and the Computational Technologies (CT) Project of the Earth Science Technology Office (ESTO). The Goddard Institute of Space Studies (GISS) is also a major NCCS user.

NOTE: The information in this submission is sensitive, including both information security and contract price-related data that should not be released to anyone without a need to know.

E-GOVERNMENT STRATEGY REVIEW

NCCS continuously updates its E-Government resources to promote accessibility and functionality for our using publics. The NCCS E-Government strategy includes the following primary initiatives:

- **Web Accessibility.** NCCS provides browser-, secure ftp-, and other similar access mechanisms for our electronic products of interest to both external and internal users including a) Assimilated data products; b) Research Earth science models, such as atmosphere, ocean, and coupled climate models, and including both model codes and output data sets; c) Research findings, such as journal articles; and d) Visualizations - graphic representation of model outputs.

Note 1: For security reasons, the NCCS distinguishes between internal NASA-only access and open access to the public at large, so web pages differ depending on audience. Note 2: All of Code 931/NCCS publicly available web sites are in compliance with 508 web accessibility standards.

- **Common Data Formats.** NCCS supports initiatives like the Earth System Modeling Framework to promote interoperability and compatibility across Earth science research models and data sharing among the Earth science research community and interested third parties.
- **Access Infrastructure.** NCCS provides, supports, or participates in initiatives that provide enhanced network infrastructure, with the purpose of enhancing accessibility and connectivity among using publics. Examples - NCCS' internal network connects with the nation-wide Abilene supercomputer network; NCCS' high performance systems are connected internally via the SEN (Scientific and Engineering Network), which has superior bandwidth and functional characteristics that promote internal and external data exchanges.
- **Performance.** NCCS works to provide enhanced network bandwidth; storage capacity and functionality; and processor performance to support better performance across all applications and users.
- **Security.** NCCS is constantly reviewing and frequently enhancing system and network security facilities, to protect the integrity and accessibility of data products, applications, and systems. The NCCS runs vulnerability scans and patches any and all identified weaknesses at least quarterly and often monthly or more frequently. The NCCS now uses dual authentication login to access systems.
- **Science research exchange.** NCCS promotes and participates in electronic exchange of a wide variety of scientific research artifacts by diverse means - electronic mail; visualizations; data products; models; publications; and so on.

[Note: the following material is an addendum to section I.H.1, methodology]

NCCS is an ongoing operational data center, but most of NCCS funds are classified as DME (Planning and Acquisition) rather than Steady State. This is primarily because the purchase prices of new systems, which are replenished every few years, are much greater than system maintenance costs. Nevertheless, OMB rules require EVM tracking because there are DME dollars. The following discussion is reproduced from the 2002 and 2003 OMB X 300

submissions for the NCCS.

Earned Value Management for NCCS

NCCS staff discussed the role of Earned Value Management for this project after reviewing relevant documents, including industry guidelines and the ANSI/EIA standard. Several issues were evident in this discussion that impact mapping of NCCS project tasks into the EVM model. Key issues included the following:

- EVM is most effective for projects with a complex set of discrete development tasks leading to a final end product, e.g., ship building or custom software development. The NCCS project provides ongoing support of high performance computer systems and related functions, not one-time development.
- EVM tracks costs and is oriented towards a cost-reimbursable project, with progress or periodic payments over time and management of cost and schedule over-runs. In a firm, fixed-price environment, there is little question of cost over-runs. (The Defense Department prescribes EVM only for cost-reimbursable projects, not fixed price.) The NCCS purchases high performance systems on a firm, fixed-price basis, so cost over-runs aren't really an issue. (There are cost-reimbursable support tasks, but these are small in comparison to system costs.)
- The NCCS can productively invest all budget resources allocated to the project. If more money is available, the NCCS can and will purchase additional computing power and use it productively. EVM assumes an end product, such as a software system, with fixed specifications and fixed requirements for a fixed budget. After initial planning, EVM manages cost and schedule against these fixed plans. This is not a direct map for the elastic requirements of the NCCS project.
- The kind of detailed work-breakdown structure that the EVM is based on is appropriate for custom development, e.g., a weapon system, done on a cost-reimbursable basis. But performance-based contracting, where the Government specifies the desired end-product and does not over-specify how the Contractor will develop it creates challenges for this type of advance planning. (Note: NCCS and its support contractor, CSC, are evolving their project management processes to match industry best practices, which will include a Word Breakdown Structure in the short term.)
- The NCCS uses competitive acquisition methods, as law and regulations require, for both integration services and high performance systems. The NCCS has learned that competition can result in dramatic cost savings. These savings are difficult to predict, particularly given the dynamism of the high performance computer marketplace. Supercomputers are not commodities like PCs or printers. The NCCS could not have planned for the dramatic discount received, for example, on the Phase 1 systems.
- The OMB questionnaire includes "EAC" or Estimate at Completion. "Completion" is less meaningful for a facility providing continuous, ongoing support to a community of end users. NCCS has provided a completion date in this submission, as OMB requests, but expects to continue operations beyond the completion date provided.

Architecture

7.1.1 Business

7.1.1.1 Process simplification/reengineering/design projects

The NCCS supports conversion, migration, and reengineering of application software and data sets; primary responsibility resides with the user community.

NCCS's strategic vision includes the development of a portal interface to its systems. When implemented, the portal will significantly simplify system use and user processes, including access to data sets and application codes.

The Data Management System is simplifying user access and interfaces with data and enabling management of the approximately 1 Petabyte data store.

Note to Question II.A.1.B: there are multiple parallel Enterprise Architecture initiatives NASA-wide and locally at this time. The NCCS is an active member of the Goddard SFC Enterprise Architecture Working Group and related projects.

7.1.1.2 Major organization restructuring, training and change management projects

There has been and will be training of end-users on code migration and optimization, use of system software and software tools, message passing, software reengineering, and similar topics. NCCS offers user training sessions in various sizes and formats. NCCS provides individual technical assistance to users daily. Formal classroom training is approximately quarterly.

NCCS migrated to automated operations ("lights out") during the last year and has reduced operations staffing.

NASA agency-wide is restructuring; impacts to NCCS are unknown at this time (Summer 2004).

NCCS is located within the Earth and Space Data Computing Division and the Division is restructuring due to several factors that include the Project Columbia initiative at NASA Ames. It is difficult to forecast the results at this time, but one likely outcome is an increased focus on application software support and software engineering and decreased focus on providing HPC hardware systems.

7.1.2 Data

7.1.2.1 Types of Data

The data is diverse and voluminous. The predominant data is matrices of numbers representing observations or models of the Earth's atmosphere, oceans, and other features. Most data are

mathematical representations of objects of inquiry of our community of researchers in the Earth, space, life, and microgravity sciences.

7.1.2.2 Existing Data Access

7.1.3 Application and Technology

7.1.3.1 Relationship to Service Component Model

Table 11

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Business Analytical Services	Analysis and Statistics	Modeling	No	The Service Domains, Service Types, and Service Categories in the reference model are familiar information technology management constructs, and applying them to NCCS service components was straightforward. (This discussion interprets service component categories that have an eGovernment, interactive, and web-based perspective in terms of the high performance platforms that NCCS provides.)The ease of implementation of these service components in systems software (hardware, software, infrastructure), services, and non-system business processes such that they can be shared across the Government or exploit components shared from elsewhere in the Government depends on the specific component. Where a service component uses, say, a

commercial software product that fits well with a defined Service Category or Categories, component-wise implementation may be simple. Where another component is, say, deeply imbedded in a complex custom application system, the job will be tougher. NCCS is primarily a provider of high performance computer (HPC) systems to researchers and similar users in the Goddard Earth science community. The services that NCCS provides are primarily processing, infrastructure, and data storage platforms. As part of its HPC system support, NCCS secondarily provides a suite of eGovernment services to various publics. This discussion addresses HPC. NCCS HPC support services are rolled into NASA-wide business cases for desktops, LANs, and web services and are not part of this X 300. Key Service Domain/Service Type/Components for NCCS HPC systems, and their potential for sharing, include the following:

- Business Analytical Services Domain/Analysis and Statistics Type/Components - Modeling; Predictive; Simulation; Mathematical.

NCCS users, but not the NCCS itself, are Earth scientists that use NCCS

platforms to run large numerical simulations of physical systems such as the Earth's atmosphere and oceans. The users, not NCCS, own the applications. NCCS provides hardware, software tools (development tools, debuggers, compilers, mathematical libraries, etc.) and technical assistance services that are a platform for very complex mathematical models. Large user applications, sometimes running on hundreds of processors for hundreds of hours, demand the large-scale platforms that NCCS provides. NCCS purchases and administers systems that are specifically tuned for efficient processing of these models.

**Business Analysis and Predictive
Analytical Statistics
Services** **No**

NCCS users, but not the NCCS itself, are Earth scientists that use NCCS platforms to run large numerical simulations of physical systems such as the Earth's atmosphere and oceans. The users, not NCCS, own the applications. NCCS provides hardware, software tools (development tools, debuggers, compilers, mathematical libraries, etc.) and technical assistance services that are a platform for very complex mathematical models. Large user applications, sometimes

and oceans. The users, not NCCS, own the applications. NCCS provides hardware, software tools (development tools, debuggers, compilers, mathematical libraries, etc.) and technical assistance services that are a platform for very complex mathematical models. Large user applications, sometimes running on hundreds of processors for hundreds of hours, demand the large-scale platforms that NCCS provides. NCCS purchases and administers systems that are specifically tuned for efficient processing of these models.

Digital Asset Services **Knowledge Management** **Information Retrieval** **No**

NCCS provides network infrastructure and related services that promote knowledge and information discovery, retrieval, and sharing. NCCS platforms and network services allow efficient (speedy) sharing of very large data sets across a suite of high performance network backbones and switches, web-accessibility to raw data (e.g., satellite observations), assimilated and modeled data sets (data product such as cyclical models of the global atmosphere and oceans), and intellectual capital (scientific research papers and the like). Although NCCS users own the data, the

Digital Asset Services	Knowledge Management	Information Sharing	No	<p>NCCS provides the infrastructure that allows the data to be stored, retrieved, and shared.</p> <p>NCCS provides network infrastructure and related services that promote knowledge and information discovery, retrieval, and sharing. NCCS platforms and network services allow efficient (speedy) sharing of very large data sets across a suite of high performance network backbones and switches, web-accessibility to raw data (e.g., satellite observations), assimilated and modeled data sets (data product such as cyclical models of the global atmosphere and oceans), and intellectual capital (scientific research papers and the like). Although NCCS users own the data, the NCCS provides the infrastructure that allows the data to be stored, retrieved, and shared.</p>
Digital Asset Services	Knowledge Management	Knowledge Discovery	No	<p>NCCS provides network infrastructure and related services that promote knowledge and information discovery, retrieval, and sharing. NCCS platforms and network services allow efficient (speedy) sharing of very large data sets across a suite of high performance network backbones and switches, web-accessibility to raw data (e.g., satellite</p>

observations), assimilated and modeled data sets (data product such as cyclical models of the global atmosphere and oceans), and intellectual capital (scientific research papers and the like). Although NCCS users own the data, the NCCS provides the infrastructure that allows the data to be stored, retrieved, and shared.

Back Office Services Data Management Data Exchange No

The NCCS mass storage subsystems are rapidly approaching 1 Petabyte of storage. NCCS provides hierarchical storage subsystems (tape silos, disks, servers, network infrastructure, and system software) that securely store and swiftly retrieve very large data sets. NCCS is evolving its storage platforms using customized (e.g., the Data Management System from Halcyon) and commercial (e.g., Legato Disk Extender/Unitree, Sun's SAM-QFS, Data Migration Facility) software products to serve the Goddard Earth and space science research user community better.

Back Office Services Data Management Data Warehouse No

The NCCS mass storage subsystems are rapidly approaching 1 Petabyte of storage. NCCS provides hierarchical storage subsystems (tape silos, disks, servers, network infrastructure, and system software) that securely store and swiftly

retrieve very large data sets. NCCS is evolving its storage platforms using customized (e.g., the Data Management System from Halcyon) and commercial (e.g., Legato Disk Extender/Unitree, Sun's SAM-QFS, Data Migration Facility) software products to serve the Goddard Earth and space science research user community better.

Back Office Services Data Management Extraction and Transformation No

The NCCS mass storage subsystems are rapidly approaching 1 Petabyte of storage. NCCS provides hierarchical storage subsystems (tape silos, disks, servers, network infrastructure, and system software) that securely store and swiftly retrieve very large data sets. NCCS is evolving its storage platforms using customized (e.g., the Data Management System from Halcyon) and commercial (e.g., Legato Disk Extender/Unitree, Sun's SAM-QFS, Data Migration Facility) software products to serve the Goddard Earth and space science research user community better.

Back Office Services Data Management Loading and Archiving No

The NCCS mass storage subsystems are rapidly approaching 1 Petabyte of storage. NCCS provides hierarchical storage subsystems (tape silos, disks, servers, network infrastructure, and system software) that securely store and swiftly

retrieve very large data sets. NCCS is evolving its storage platforms using customized (e.g., the Data Management System from Halcyon) and commercial (e.g., Legato Disk Extender/Unitree, Sun's SAM-QFS, Data Migration Facility) software products to serve the Goddard Earth and space science research user community better.

Back Office Services	Data Management	Data Classification	No	<p>The NCCS mass storage subsystems are rapidly approaching 1 Petabyte of storage. NCCS provides hierarchical storage subsystems (tape silos, disks, servers, network infrastructure, and system software) that securely store and swiftly retrieve very large data sets. NCCS is evolving its storage platforms using customized (e.g., the Data Management System from Halcyon) and commercial (e.g., Legato Disk Extender/Unitree, Sun's SAM-QFS, Data Migration Facility) software products to serve the Goddard Earth and space science research user community better.</p>
----------------------	-----------------	---------------------	----	--

7.1.3.2 Relationship to Technology Component Model

Table 12

Service Area	Service Category	Service Standard	Relation to SRM of FEA
			<p>The architecture features called out in the table in the next section date from the 2003 OMB submission</p>

(with a few changes). Recent NCCS analysis has yielded additional developmental To-Be architectural technical standards. These standards are generally not yet implemented at the NCCS, but describe the path that NCCS now intends to follow. These include the following:

- * **Data Centric.** (TRM Service Platform and Infrastructure Service Area; Database/Storage Service Category; Database Service Standard) NCCS will evolve to a configuration where processing engines are (topologically) arranged around a central data resource. Features: Not NASA center-centric; Common interfaces to resources enhance usability; Jobs are run on appropriate and available resources; Data can be retrieved or stored to a global address space; Data analysis and visualization environments are readily available and easily accessible.
- * **Consolidated Storage.** (TRM Service Platform and Infrastructure Service Area; Database/Storage Service Category; Storage Device Service Standard) In lieu of storage locally attached to and configured for individual processing engines, storage devices will be consolidated and accessible over a Storage Area Network (SAN) to all primary processing engines. Features: Storage area network provides shared, large, fast storage from all compute platforms; Data analysis and visualization environment can be tightly coupled to the SAN; Multi-tiered Hierarchical Storage Management (HSM) environment integrated into the SAN; Data Management System application package will support intelligent centralized access to

and management of large consolidated data store. · * Intel-Linux Clusters. (TRM Service Platform and Infrastructure Service Area; Hardware/Infrastructure Service Category; Servers/Computers Service Standard) Multiple HPC system manufacturers are producing machines based on the Intel family of microprocessors, the Linux operating system, and cluster interconnection fabrics. NCCS will structure future system acquisitions to permit these devices to demonstrate their utility. Features: Migration across vendor platforms with this commonality will be simple; Competitive forces will help control costs; Commodity and open source components will also help price/performance; Linux cluster software is maturing to the point of acceptable production use. · * Portal. (TRM Service Platform and Infrastructure Service Area; Delivery Servers Service Category; Portal Service Standard) Many computational science users are accustomed to low-level interaction with the system software and hardware using primitive tools like vi and command line shells. On the other hand, some GMAO data products are pre-packaged for downloading from the world wide web using a browser. Portal interface tools and technologies now in use in other arenas are susceptible to use at NCCS for access to applications, stored data, and outputs. Ease of use will lead to higher user productivity and better support. · * Common Interfaces and Services. (TRM Service Access and Delivery Service Area; Access Channels Service Category; Collaboration/Communication

Service Standard) Use of Intel-Linux clusters with common system software will facilitate evolution to user interfaces that are common across platforms. Unique system software infrastructure will recede or be masked behind common interfaces.

* **Multi-Tiered Platforms.** (TRM Service Platform and Infrastructure Service Area; Hardware/Infrastructure Service Category; Servers/Computers Service Standard) NCCS will mount computing devices with diverse capabilities, similar to the current assortment of processor engines, but with better interoperability. Features: Multi-tiered engines provide the appropriate platform for the application; initial steps towards a common center architecture (which see below); Portal or common job submission points coupled with scheduling resources on appropriate and available platforms; Multi-tiered HSM environment integrated into the SAN.

* **Common Center Architecture.** (Multiple TRM Service Areas; Service Categories; and Service Standards) Management of the high performance computer centers at Goddard (the NCCS) and at Ames Research Center has been more or less independent. GSFC supports Earth and space science primarily; ARC workloads include aircraft and spacecraft design, among others. Hardware platforms have historically been rather different. But GSFC and ARC are discussing migration to a common architecture. Features: increased computational workload sharing; increased data sharing; increased support service and technical

expertise sharing; reduced overhead; reduced budget and capacity bumps; facilitate other architecture initiatives shown here; shared research and development; increased reliability; more collaboration; "OneNASA"; and others. // These EA features are still in the development stage and are subject to further refinement and supporting analysis.

Key Service Areas/Service Categories/Service Standards/Service Specifications include the following: // Service Area: Service Access and Delivery // * Service Category: Access Channels // ** Service Standard: Other Electronic Channels // * Service Specification: System-to-System: Within the NCCS, several hardware and software components must dialogue directly. This includes heartbeat monitoring to ensure high availability of critical storage and compute servers, Automated Cartridge System Library Software (ACSL) servers directing the storage silos and tape drives, and Big Brother monitoring services. // Service Category: Service Transport // ** Service Standard: Transport // *** Service Specification: OpenSSH and Secure Shell access in use throughout the NCCS when accessing the compute engines and servers. // *** Service Specification: Secure File Transport Protocol (FTP) is used within the NCCS to access the hierarchical storage management system. // Service Area: Service Access and Delivery // ** Service Standard: Delivery Channels // *** Service**

Specification: Intranet The following devices are used within the NCCS: GigE, HIPi, ATM, and 10/100 Ethernet // ***** Service Specification: Peer to Peer (P2P)** These include the hardware and software components discussed above relating to system-to-system access including heartbeat monitoring, ACSLS servers, and monitoring services // **Service Area: Component Framework // * Service Category: Business Logic // ** Service Standard: Platform Independent // *** Service Specification: C/C++ // *** Service Specification: JavaScript // * Service Category: Data Interchange // ** Service Standard: Data Exchange // *** Service Specification: Hierarchical Data Format (HDF) // *** Service Specification: Network Common Data Format (net CDF) // *** Service Specification: IEEE binary data formats // Service Area: Service Access and Delivery // ** Service Standard: Delivery Channels // *** Service Specification: Intranet** The following devices are used within the NCCS: GigE, HIPi, ATM, and 10/100 Ethernet // ***** Service Specification: Peer to Peer (P2P)** These include the hardware and software components discussed above relating to system-to-system access including heartbeat monitoring, ACSLS servers, and monitoring services

Service Access and Delivery **Service Requirements** **Legislative Compliance** /

[Information Sharing; Data Exchange] The systems and services in the NCCS are in compliance with NASA's NPG 2810 and GPG 2810.1 security policies and guidelines and Section 508 for people with disabilities

Service Access and Delivery	Service Requirements	Legislative Compliance /	[Information Sharing; Data Exchange] Web pages follow GSFC General Policies defined at http://webmaster.gsfc.nasa.gov and the NASA logo policies defined at http://www.hq.nasa.gov/office/pao/insign-ia/text/Welcome.html
Service Access and Delivery	Service Requirements	Authentication / Single Sign-on (SSO)	[Information Sharing; Data Exchange] Authentication is performed via userid, secure token, and passwords on each system. Passwords change several times a minute via the secure tokens.
Service Platform and Infrastructure	Supporting Platforms	Platform Dependent	[Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] Tru64 is the operating system on the HP systems.
Service Interface and Integration	Supporting Platforms	Platform Dependent	[Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] IRIX is the operating system on the SGI systems
Service Platform and Infrastructure	Supporting Platforms	Platform Dependent	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Solaris is the operating system on the SUN systems
Service Platform and Infrastructure	Supporting Platforms	Platform Dependent	[Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] Linux (Red Hat and Debian) are used on several servers
Service Platform and Infrastructure	Delivery Servers	Application Servers	[Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] The NCCS is currently configuring and will be deploying a Web based source code repository, based on the Gforge software. Users and others will be able to use this on-line repository

Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)	to download applications given sufficient privileges, upload applications for others to use, and use it for version control.
Service Platform and Infrastructure	Software Engineering	Software Configuration Management	[Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] Compilers - Fortran, C, C++ // Message Passing - Message Passing Interface (MPI), OpenMP, shmem, Pthreads. On many of the platforms at the NCCS, proprietary debuggers, compilers, libraries, and more are used to assist application developers. TotalView is a commercial debugger that is used at the NCCS on both the HP and SGI machines.
Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Concurrent Version System (CVS) is used throughout the NCCS for application developers to maintain multiple versions of their code. As stated elsewhere, NCCS has deployed a web-based CVS based on the Gforge software product.
Service Platform and Infrastructure	Software Engineering	Test Management	Proprietary performance profilers are also used on the High End Computers (HEC) at the NCCS.
Service Platform and Infrastructure	Software Engineering	Test Management	Commercial codes such as Vampir and VampirTrace are used to analyze message passing applications.
Service Platform and Infrastructure	Software Engineering	Test Management	The NCCS benchmark suite is used for functional and performance testing for new technologies.
Service Platform and Infrastructure	Software Engineering	Test Management	Software Engineering Methodologies: GeckoLife (AMTI) is used for concept and requirements specification for applications.
Service Platform and Infrastructure	Software Engineering	Test Management	Software Engineering Methodologies: Validation and regression testing are performed by the users as the applications or

Service Platform and Infrastructure	Database Storage	/	Storage	systems change [Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Network Attached Storage (NAS)
Service Platform and Infrastructure	Database Storage	/	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Storage Area Network (SAN)
Service Platform and Infrastructure	Database Storage	/	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Legato Disk Extender/Unitree
Service Platform and Infrastructure	Database Storage	/	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Data Migration Facility (DMF)
Service Platform and Infrastructure	Database Storage	/	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Sun SAM-QFS
Service Platform and Infrastructure	Database Storage	/	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Veritas Cluster Software (VCS) provides the NCCS with agents that monitor the mass storage cluster and failover the servers when appropriate. This provides the users with a highly available system with a minimum of downtime where the users cannot access their mass storage holdings
Service Platform and Infrastructure	Database Storage	/	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Storage Request Broker (SRB)/Data Management System (DMS) is currently being developed by the NCCS to provide both the user community and the

NCCS with better tools to manage data. Users will be able to easily access and manage their mass storage archives remotely from DMS enable platforms in a secure manner, regardless of the underlying physical devices on which the data is stored or underlying storage management software system.

Service Platform and Infrastructure	Hardware Infrastructure	Servers Computers	/	[Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] Halem: HP Sierra Cluster (SC) 45
Service Platform and Infrastructure	Hardware Infrastructure	Servers Computers	/	[Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] Milton: HP Sierra Cluster (SC) 45
Service Platform and Infrastructure	Hardware Infrastructure	Servers Computers	/	[Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] Charney: HP Sierra Cluster (SC) 45
Service Platform and Infrastructure	Hardware Infrastructure	Servers Computers	/	[Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] Daley: SGI Origin 3000
Service Platform and Infrastructure	Hardware Infrastructure	Servers Computers	/	[Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] Courant: SGI Origin 3000
Service Platform and Infrastructure	Hardware Infrastructure	Servers Computers	/	[Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] Jimpf: SGI Origin 3000
Service Platform and Infrastructure	Hardware Infrastructure	Servers Computers	/	[Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] New Mintz: SGI Origin 3000

Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	/ [Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Sun E6500
Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	/ [Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Sun E10K (will removal after data migration is complete)
Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	/ [Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Sun Fire E15K
Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	/ [Modeling; Predictive; Simulation; Mathematical; Data Extraction and Transformation; Knowledge Discovery] Sun V880
Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	/ [Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] SGI Origin 300s are used as CXFS servers
Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	/ [Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Sun Ultra10 used as the ACSLS server for the storage silos
Service Platform and Infrastructure	Hardware / Infrastructure	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Storage Tek (STK) silos
Service Platform and Infrastructure	Hardware / Infrastructure	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] STK Tape Drives
Service Platform and Infrastructure	Hardware / Infrastructure	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] 9840A Ultra SCSI
Service Platform and Infrastructure	Hardware / Infrastructure	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving]

Infrastructure			Archiving] 9840A Fiber
Service Platform and Infrastructure	Hardware / Infrastructure	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] 9840C Fiber
Service Platform and Infrastructure	Hardware / Infrastructure	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] 9804B Fiber
Service Platform and Infrastructure	Hardware / Infrastructure	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Hitachi Disk Array
Service Platform and Infrastructure	Hardware / Infrastructure	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] Data Direct Network (DDN) Disk Arrays
Service Platform and Infrastructure	Hardware / Infrastructure	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] SGI TP9400 Disk Array
Service Platform and Infrastructure	Hardware / Infrastructure	Storage	[Information Sharing; Information Retrieval; Data Exchange; Data Warehouse; Loading and Archiving] SGI TP9100 Disk Array
Service Platform and Infrastructure	Hardware / Infrastructure	Peripherals	Printers
Service Platform and Infrastructure	Hardware / Infrastructure	Peripherals	Scanners
Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices Standards	[Information Sharing; Data Exchange] Hubs, switches, routers, NICs, Firewall, GigE, HIPPI, ATM, 10/100 Ethernet
Component Framework	Security	Supporting Security Services	[Information Sharing; Data Exchange] Secure Sockets Layer (SSL)
Component Framework	Security	Supporting Security	[Information Sharing; Data Exchange] Transport Security

		Services	Layer (TLS)
Component Framework	Security	Supporting Security Services	[Information Exchange] Sharing; TCP/IP Wrappers Data
Component Framework	Security	Supporting Security Services	[Information Exchange] Sharing; Secure Shell Data
Component Framework	Security	Supporting Security Services	[Information Exchange] Sharing; Firewall Data
Component Framework	Security	Supporting Security Services	[Information Exchange] Sharing; Access Control Lists (ACL) used on all systems and network devices Data
Component Framework	Security	Supporting Security Services	[Information Exchange] Sharing; Log hosts centralize scanning for vulnerabilities Data
Component Framework	Security	Supporting Security Services	[Information Exchange] Sharing; Continuous scanning for vulnerabilities Data
Component Framework	Security	Supporting Security Services	[Information Exchange] Sharing; Minimal network services are configured on all machines Data

7.1.3.3 Partnerships

There exists an international community of Earth scientists that share diverse components and applications, including both data and programs, across the Government and globally. This includes Earth scientists that are users of NCCS systems. (The scientists own the software components and applications, but use the NCCS.) The Earth System Modeling Framework (ESMF) is a good example of a joint effort of NCCS, NASA Goddard, and other agencies to leverage application components across the Government.

7.1.4 Security and Privacy

7.1.4.1 How is it provided and funded?

Funding is provided by the same source for funding for the Code 931 NASA Center for Computational Sciences (NCCS), which is the Earth Science Enterprise (program office) at

NASA headquarters. A portion of the information technology budget by which the NCCS provides services and resources to the user community is dedicated to security. Security is provided largely by efforts contained within the Code 931/NCCS organization, although there are elements (NASA/Goddard firewall, NASA/Goddard email servers, and the services of the Goddard campus networking environment) that are provided by the NASA/Goddard Space Flight Center infrastructure.

7.1.4.2 How is security accomplished?

The investment meets the security requirements by following NASA policy. The NASA Policy Directive NPD 2810.1 meets FISMA, OMB, and NIST requirements. NASA Procedures and Requirements (NPR) 2810.1 are in an update cycle to bring it in line with NIST Special Publications and Federal Information Processing Standards. Interim policy has been promulgated via NASA Information Technology Requirement (NITR) that stipulates the immediate use of NIST Special Publication and FIPS guidance while NPR 2810.1 is being updated.

All systems in the NASA Center for Computational Sciences program are covered by one security plan, which is kept current. There exists a set of security-related documents that include the security plan proper, authorizations to process, technical configuration data, tests results, and related materials. These documents cover the primary high performance processors within the NCCS individually, and smaller support systems in functional groups. Moreover, the networked, interconnected configuration that the NCCS operates is functionally and technically a single distributed system – for example, with respect to firewalls.

With the May 2004 release of NIST's certification and accreditation guidance (SP 800-37), NASA has been updating its NASA Procedures and Requirements (NPR) 2810, to reflect the new C&A methodology. The existing document and its upcoming update (based on NIST's latest guidance) lay out the security requirements for all phases of the IT life cycle. Currently, the Project complies with NPR 2810.1 that preceded the current approved standards and guidance from NIST.

NASA is aggressively pursuing a bottom-up review of its existing IT security policy and updating it to comply with NIST's special publications and FIPS PUBs. This effort is well underway with an expected delivery in the 3rd quarter of FY 2005. To bridge the gap, NASA has recently published an interim policy, NASA Information Technology Requirement (NITR) that stipulates the immediate use of NIST and FIPS guidance.

NCCS has recently instituted two-factor authentication (the user must have a secure token in order to access any system), has enhanced access control to internal resources (e.g., file and directory access rights) much more than before, and has taken many other actions to increase the security of its systems. These steps have been tested extensively by NCCS systems staff and other parties prior to production operations. Our users have been very patient and supportive, in spite of disruptions plus inconveniences in system use that continue to the present and thru the foreseeable future.

Tests include:

- Quarterly vulnerability scanning
- Scans following system updates
- Scans at new system installation
- Annual testing and training of all system administrators

External reviews to include review of configuration and controls by directorate security staff

Note: The following field accommodates only one date, but the individual system test dates are as follows:

halem - June 16, 2004.
 milton - June 16, 2004.
 charney - June 16, 2004.
 daley - June 16, 2004.
 courant - June 16, 2004.
 jimpf - June 16, 2004.
 mass storage servers – June 16, 2004.
 support servers and desktops – June 16, 2004.

Incident detection, handling, and response are done according to NASA Agency policy. These policies and procedures are an integral part of the system management standards as applied.

These policies extend over the entire incident lifecycle from prevention through response. All systems at NASA are tied into the NASA Incident Response Center, which acts as a focal point for all IT security incidents by maintaining an authoritative data base. Reporting is done via the Center information technology security authorities and the Agency. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. The GSA Millennium contract cites several specific guidelines and states that, "All Contractor personnel must comply with Government-wide, NASA, and Goddard installation-specific security requirements." Security requirements appearing in the Millennium contract include a) Contractor contribution to information technology Security Plans, b) Contractor preparation of a Safety & Health Plan, c) Contractor incident notification/reporting to the Goddard Safety and Environmental Branch, d) Contractor notification of non-compliance with safety standards, e) various contract clauses related to data handling, f) tracking and badging of Contractor personnel using the Locator and Information Services Tracking System (LISTS), including procedures for departing personnel, g) contract clauses requiring compliance with Goddard security manuals, emergency plans, safety programs, and related documents, h) background checks of all contractor staff, i) required compliance with NASA information technology Security policy directives and guidelines, j) Government oversight and review of Contractor activities, k) compliance with information technology system use controls (user ids, passwords, access controls), and a variety of other controls.

7.1.4.3 Effective use of security, controls and authentication tools

Via the policies and guidelines in NASA's NPR2810 (reference: <http://nodis.hq.nasa.gov/Library/Directives/NASA-WIDE/Procedures/Legal Policies/N PG 2810.html>). NCCS's systems are in conformance with NPR2810 standards regarding privacy protection.

7.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000. The date of the most recent update to the agency GPEA plan, the 2003 progress update, is provided below.

8 Goddard Space Flight Center (GSFC) – Space and Ground Network IT Support

Project Description

The Space and Ground Network IT Support is in the operation phase of the NASA IT Capital Planning Investment Control Process. The National Aeronautics and Space Administration Space and Ground Networks, in operation since the 1980s, provide mission communications for multiple Space Network and Ground Network tracking stations. These existing communication facilities are operated and maintained for pre-launch checkout, launch and landing, and on-orbit tracking, telemetry data acquisition, and command services for crewed and robotic low-Earth orbiting spacecraft, and suborbital rockets and balloons. The Space Network includes nine geosynchronous satellites, and is currently supported through non-NASA reimbursable funding. The systems and staffing for Space and Ground Networks are described; the Space Network funding is not included.

Space Network - The Tracking and Data Relay Satellites (TDRS) in geosynchronous orbit are situated in Earth orbit such that they can provide continual, global coverage. There are currently nine spacecraft in orbit, five of which are being used daily to support the low Earth customer community. Of these five spacecraft, two are located just off the coast of South America over the Atlantic Ocean, two are over the middle of the Pacific Ocean, and one over the Indian Ocean. There is one satellite that is solely used to support National Science Foundation (NSF) operations at the South Pole and is not available for service to other customers. The other spacecraft are stored on-orbit as spares for the operational fleet.

There are several services provided by the Space Network to our customers. They include telecommunications, tracking and spacecraft clock calibration, testing, and analysis. The Space Network is operated 24x7, 365 days per year. This is driven by the need to control and operate the TDRS constellation and the fact that our customers request support at all hours. Included in this list of customers are the International Space Station and the Space Shuttle, both of whom schedule continuous coverage from the network.

Ground Network - The Ground Network (GN) is comprised of tracking stations in Poker Flat Research Range near Fairbanks Alaska, Merritt Island Launch Annex (MILA) in Florida, Svalbard Norway, McMurdo Ground Station in the Antarctic, and Wallops Island Virginia. The

Svalbard and Alaska stations include commercial assets and operators. The GN provides launch support, orbiting spacecraft support, and sounding rocket and atmospheric balloon mission support. The GN also supports critical Space Shuttle launch, emergency communications, and landing activities. The GN provides for the implementation, maintenance, and operation of the tracking and communications facilities necessary to fulfill program goals for flight projects in the NASA mission set. Missions supported also include NASA inter-agency collaborative programs, commercial enterprises, and other national, international, and commercial enterprises on a reimbursable basis. The Space Shuttle launches were successfully supported through dedicated facilities of the MILA station and the Ponce de Leon (PDL) inlet annex. The University of Chile is providing southern hemisphere coverage for missions such as RHESSI and TOMS-EP. Wallops Flight Facility (WFF) supported numerous sounding rockets, balloon and other orbital and sub-orbital campaigns. The Alaska and Svalbard stations continued to provide support to missions such as Aqua, Aura, EO-1, Landsat-7, QuikScat at S and X bands, while the Wallops station provided support to missions such as Gravity Probe-B, FAST, RHESSI, TOMS-EP, TRACE, SAMPEX, SORCE, SeaWiFS, and SWAS.

Architecture

8.1.1 Business

8.1.1.1 Process simplification/reengineering/design projects

None, project is currently in the mission operations phase. Near-Earth Networks Services (NENS) contract provides operations and maintenance of existing systems. Re-engineering of the customer planning and scheduling interface software is being considered. New missions and services may cause systems to change, which would be handled through the budget process.

8.1.1.2 Major organization restructuring, training and change management projects

Restructuring: The Mission Services Program (MSP), which manages the Space and Ground Network Systems, was established in August 1999, when the GSFC Flight Programs and Projects Directorate reorganization took effect. MSP was reorganized in September 2000 to focus specifically on Space Operations Management Office (SOMO) support and to realign its organization with elements of the SOMO program. In response to the elimination of SOMO, MSP reorganized in December 2002 with an organizational structure better aligned with the Space and Ground Networks and customer interface. A Systems Architecture Manager position and a Mars Laser Communication Demonstration Project were added in 2003. No further reorganizations are anticipated at this time.

8.1.2 Data

8.1.2.1 Types of Data

Spacecraft telemetry, command, and tracking data for multiple missions, including non-NASA satellites; Human spaceflight voice and video from International Space Station, Space Shuttle, and Soyuz vehicles.

8.1.2.2 Existing Data Access

8.1.3 Application and Technology

8.1.3.1 Relationship to Service Component Model

Table 13

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Support Services	Communication		Yes	This investment relates to the Support Services Domain of the Services Component Reference Model. Security is a primary focus within this system. Identification and authentication, access controls, encryption, intrusion detection, verification, user management, and audit trail capture and analysis are managed in accordance with the NASA Procedure Guideline 2810.1. This system provides Support Services of Communications and Systems Management, and Customer Relationship Management Partner Relationship Management in support of NASA missions, NASA cooperative missions with other foreign space agencies (Canada, Russia, Japan, Germany, France, ESA, Argentina, India), other U.S. agencies such as DoD, DoC/NOAA and DoI/USGS, universities (University of California, University of Colorado, Johns Hopkins University/Applied Physics

Laboratory, Stanford University, Bowie State University, Capitol College) and commercial Expendable Launch Vehicle companies (Boeing, Lockheed-Martin, Orbital Sciences Corp). The public benefits from the science results, images, and video returned from space. New service components need to be added to describe the Communications services for satellite communications. These components could include Satellite Telemetry, Tracking and Control (TT&C), Direct Satellite Downlink, and Satellite Data Relay.

Support Services	Systems Management	No
Customer Services	Customer Relationship Management	No
Customer Services	Customer Relationship Management	No
Customer Services	Customer Relationship Management	No

8.1.3.2 Relationship to Technology Component Model

Table 14

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access and Delivery	Service Transport	Service Transport	This existing system provides Service Transport. FEA TRM ver 1.0 does not cover satellite ground stations and satellite communication protocols, although it does cover the control system, network interface and scheduling components of a ground station. Add new specifications under Service Transport to include international Consultative Committee for Space Data Systems (CCSDS) and

International Telecommunication Union standards including ISO/DIS 13420 Space data and information transfer systems -- Advanced orbiting systems -- Networks and data links -- Architectural specification, CCSDS 401.0-B: Radio Frequency and Modulation Systems -- Part 1: Earth Stations and Spacecraft, DoD Range Commanders Council InterRange Instrumentation Group standards, Federal Communications Commission frequency specifications. At this time, in the core area of Service Access and Delivery we support both the Internet Explorer and Netscape browsers, Electronic Mail, fax, system to system, web services and URL. We use Internet, Intranet and Virtual Private Networking as delivery channels. We comply with the legislative/compliance standards for Section 508, web content accessibility, and security. We support authentication and single sign-on (in appropriate areas) and host sites internally. We use a variety of network services and service transport protocols - IMAP/POP3, MIME, VDP, NTP, SMTP, SNMP, LDAP, DHCP, DNS, TCP, IP, HTTP, HTTPS, FTP, FastCopy and IPSEC. Our service platform infrastructure includes platform independent (Java, Ada, C, C++) and platform dependent using VAX/VMS, HP/Unix, Sun/Solaris, Linux, Windows 2000, and Windows NT. Our delivery servers use Apache to deliver web information to authorized users. Software engineering for the program covers all software configuration management, modeling and test management service specifications. Database storage is on Oracle, CA/Ingres, rdb, FileMakerPro, Access and SQL server. We use Network Attached Storage. Our hardware infrastructure contains Enterprise Servers with RAM, Hard Disks, Microprocessors, RAID, printer, scanners, custom frame relay, using an Ethernet network. The network uses a variety of hubs, switches, routers, NIC, transceivers, gateways and firewalls. We use Digital Certificate Authentication as well as FIPS 186 and SSL for security. We use TLS and SSH to support these. We use SL/GMS, XML, and static html as a presentation interface. Integration middleware used includes rpc and Object Request Broker. Visual basic, Perl, VMS DCL, and TKL/TCL scripting tools are used.

Service Access and Delivery	Access Channels	Other Electronic Channels
--	----------------------------	--

8.1.3.3 Partnerships

None.

8.1.4 Security and Privacy

8.1.4.1 How is it provided and funded?

Funding for the Ground Network is provided through the Earth Science Enterprise, but the Space Network funding is a consumption type process where services are measured and paid for by the user. Approximately 5% of the Program budget is devoted to IT security. Program office prime contractor provides IT security through Program staff for policy and Operations and Engineering staff for system administration and security engineering. CSOC contract adheres to the IT policy and guidance provisions of the NPD 2810.1 Security of Information Technology, NPG 2810.1 NASA Procedures and Guidance for the Security of Information Technology, and other NASA requirements. IT planning provides determination of security objectives, review of project security, security planning, coordination of security budgets, and review of project security compliance. System security engineering performs life cycle protection tasks for CSOC systems and IT products. Protective measure baseline assurance defines, controls, maintains, and verifies facility and operational security compliance. Security administration and enforcement executes and enforces the security policy in CSOC facilities and IT systems. IT training and awareness explains the security program and individual responsibilities to CSOC personnel.

8.1.4.2 How is security accomplished?

The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures. When NIST completes this process, NASA will revisit its policy and procedures to conform to NIST's new guidance.

Review of audit logs and response to Wide Area Network communications monitoring is included in standard procedures. Weekly meetings are held to assess Information Technology security posture. Incidents are reported to the Center IT Security Manager, who forwards information to the NASA Incident Response Center and on to FedCIRC. NASA is an initial

member of Forum of Incident Response and Security Teams (FIRST). All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. Contractor presents IT security status at weekly meeting with civil servant Computer Security Official, and is subject to independent compliance audits performed by GSFC Center IT Security Manager, Goddard Security Office, and Network Security Official. NASA Office of Inspector General also performs independent surveys and audits.

8.1.4.3 Effective use of security, controls and authentication tools

Public access is not permitted to Space and Ground Network systems. Administrative systems are in conformance with NASA's NPG 2810.1 standards regarding privacy and personal information protection.

8.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. For reference only: the initial NASA Agency-wide GPEA Plan was delivered on 10/31/2000.

9 Johnson Space Center (JSC) – Flight Operations

Project Description

The Space Shuttle and Space Station programs play a vital role in enabling NASA's vision and mission. This includes advancing human exploration and providing safe access to space in support of human operations in low-earth orbit. FO, as the contractual arm of the JSC Mission Operations Directorate (MOD), directly supports NASA's goal of flying missions safely with mission objectives achieved by providing the products, services and facilities used to prepare and support such missions. The major functions for flight operations include management and integration, mission operations, vehicle operations, flight systems operations, flight control, flight crew and flight controller training functions, flight design & dynamic operations, preflight and flight control team functions, flight planning, payloads and assembly operations, crew procedures, and operational readiness for the Shuttle Program missions. Primary training facilities include the Shuttle Mission Training Facility, Flight Operations Trainers and the Space Station Training Facility. Shuttle onboard flight software is built and certified in the FO Software Production Facility. The JSC Flight Operations Investment is in the Control process of NASA Information Technology (IT) Capital Planning and Investment Control (CPIC) process, and this IT investment is managed as a component of the NASA project under NASA's NPG 7120 process.

Mission Operations Directorate (MOD) is the responsible organization for Mission Operations for both the Space Shuttle and Space Station Program. FO, as the contractual arm of MOD, perform with MOD the plan, train and fly tasks described in the Johnson Space Center Functional Statement for MOD.

Architecture

9.1.1 Business

9.1.1.1 Process simplification/reengineering/design projects

The Flight Operations Investment is currently in the operational phase. Several projects are nearing completion that will require cyclical replacements of hardware and software upgrades to stay current with marketplace technologies, add efficiencies, and improve maintenance costs.

9.1.1.2 Major organization restructuring, training and change management projects

None currently identified.

The Flight Operations Investment is currently in the mission operations phase. Organizational restructuring, training, and change management have been accomplished throughout the project's life cycle. As part of project management process, any needed improvements will be made using existing system engineering processes in place within the Agency.

9.1.2 Data

9.1.2.1 Types of Data

Data used in the sustaining operations of this project consists mostly of technical descriptions of mission preparation and execution, mission specific planning, technical training, flight control, payloads and assembly operations, crew procedures, and analyses.

9.1.2.2 Existing Data Access

9.1.3 Application and Technology

9.1.3.1 Relationship to Service Component Model

Table 15

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
-----------------------	---------------------	------------------	----------------------	--------------------------------

Process Automation Services		Tracking Workflow	and	Process Tracking
Business Management Services		Management Process	of	Change Management
Business Management Services		Management Process	of	Configuration Management
Business Management Services		Management Process	of	Requirements Management
Business Management Services		Management Process	of	Program / Project Management
Business Management Services		Management Process	of	Quality Management
Business Management Services		Management Process	of	Risk Management
Digital Services	Asset	Document Management		Document Imaging and OCR
Digital Services	Asset	Document Management		Document Referencing
Digital Services	Asset	Document Management		Document Revisions
Digital Services	Asset	Document Management		Library / Storage
Digital Services	Asset	Document Management		Document Review and Approval
Digital Services	Asset	Document Management		Document Conversion
Digital Services	Asset	Document Management		Indexing
Digital Services	Asset	Document Management		Classification
Digital Services	Asset	Knowledge		Information

Services		Management	Sharing	
Digital Services	Asset	Knowledge Management	Knowledge Capture	
Digital Services	Asset	Knowledge Management	Knowledge Distribution and Delivery	and
Business Analytical Services		Analysis Statistics	and Modeling	
Business Analytical Services		Analysis Statistics	and Predictive	
Business Analytical Services		Analysis Statistics	and Simulation	
Business Analytical Services		Analysis Statistics	and Mathematical	
Business Analytical Services		Analysis Statistics	and Structural Thermal	/
Business Analytical Services		Visualization	Graphing Charting	/
Business Analytical Services		Visualization	Imagery	
Business Analytical Services		Visualization	Multimedia	
Business Analytical Services		Visualization	CAD	
Business Analytical Services		Reporting	Ad-Hoc	
Business Analytical Services		Reporting	Standardization Canned	/

Back Services	Office	Data Management	Data Exchange
Back Services	Office	Data Management	Data Mart
Back Services	Office	Data Management	Data Warehouse
Back Services	Office	Data Management	Meta Data Management
Back Services	Office	Data Management	Data Cleansing
Back Services	Office	Data Management	Extraction and Transformation
Back Services	Office	Data Management	Loading and Archiving
Back Services	Office	Data Management	Data Recovery
Back Services	Office	Data Management	Data Classification
Back Services	Office	Assets / Materials Management	Facilities Management
Back Services	Office	Assets / Materials Management	Computers / Automation Management
Back Services	Office	Development and Integration	Legacy Integration
Back Services	Office	Development and Integration	Data Integration
Back Services	Office	Development and Integration	Instrumentation and Testing
Back Services	Office	Development and Integration	Software Development
Support Services		Security Management	Identification and Authentication
Support Services		Security Management	Access Control
Support Services		Security Management	Encryption

Support Services	Security Management	Intrusion Detection
Support Services	Security Management	Verification
Support Services	Security Management	Digital Signature
Support Services	Security Management	User Management
Support Services	Security Management	Role / Privilege Management
Support Services	Security Management	Audit Trail Capture and Analysis
Support Services	Communication	Audio Conferencing
Support Services	Communication	Video Conferencing
Support Services	Systems Management	License Management
Support Services	Systems Management	Remote Systems Control
Support Services	Systems Management	Systems Resource Monitoring
Support Services	Systems Management	Software Distribution

9.1.3.2 Relationship to Technology Component Model

Table 16

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access and Delivery	Access Channels	Web Browser	The Service Area, Service Category, Service Standard, and Service Specification that describe the technology supporting the Flight Operations are listed below. * Service Access and Delivery (Core Service Area) - Access Channels (Service) - Web

Browser (Standard) - Internet Explorer and Netscape Communicator (Specification)
*** Service Access and Delivery (Core Service Area) - Access Channels (Service) - Wireless / PDA (Standard) - Palm Pilot, Blackberry (Specification)**
*** Service Access and Delivery (Core Service Area) - Access Channels (Service) - Collaboration Communications (Standard) - Electronic Mail, Fax, Kiosk (Specification)**
*** Service Access and Delivery (Core Service Area) - Access Channels (Service) - Other Electronic Channels (Standard) - System to System, Web Service, URL (Specification)**
*** Service Access and Delivery (Core Service Area) - Delivery Channels (Service) - Internet, Intranet, Extranet, Virtual Private Network (VPN) (Standard)**
*** Service Access and Delivery (Core Service Area) - Service Requirements (Service) - Legislative / Compliance (Standard) - Section 508, Web Content Accessibility, Security, Privacy (Specification)**
*** Service Access and Delivery (Core Service Area) - Service Requirements (Service) - Authentication / Single Sign-on (Standard)**
*** Service Access and Delivery (Core Service Area) - Service Requirements (Service) - Hosting (Standard) - Internal (within Agency), External (ISP/ASP/FirstGov) (Specification)**
*** Service Access and Delivery (Core Service Area) - Service Transport (Service) - Supporting Network Services (Standard) - IMAP / POP3, MIME, SMTP,**

ESMTP, T.120, LDAP, Directory Services (Specification)
 * Service Access and Delivery (Core Service Area) - Service Transport (Service) - Service Transport (Standard) - TCP, IP, HTTP, HTTPS, WAP, FTP (Specification)

Service Access and Delivery	Access Channels	Web Browser
Service Access and Delivery		Wireless / PDA
Service Access and Delivery		Wireless / PDA
Service Access and Delivery		Collaboration Communication
Service Access and Delivery		Collaboration Communication
Service Access and Delivery		Collaboration Communication
Service Access and Delivery		Other Electronic Channels
Service Access and Delivery		Other Electronic Channels
Service Access and Delivery		Other Electronic Channels
Service Access and Delivery		Internet
Service Access and Delivery		Intranet

Service Access and Delivery		Extranet
Service Access and Delivery		Virtual Private Network (VPN)
Service Access and Delivery	Service Requirements	Legislative Compliance /
Service Access and Delivery	Service Requirements	Legislative Compliance /
Service Access and Delivery	Service Requirements	Legislative Compliance /
Service Access and Delivery	Service Requirements	Legislative Compliance /
Service Access and Delivery	Service Requirements	Authentication / Single Sign-on (SSO)
Service Access and Delivery	Service Requirements	Hosting
Service Access and Delivery	Service Requirements	Hosting
Service Access and Delivery	Service Transport	Supporting Network Services
Service Access and Delivery	Service Transport	Supporting Network Services
Service Access and Delivery	Service Transport	Supporting Network Services
Service Access and Delivery	Service Transport	Supporting Network Services
Service	Service	Supporting

Access Delivery	and	Transport	Network Services
Service Access Delivery	and	Service Transport	Supporting Network Services
Service Access Delivery	and	Service Transport	Supporting Network Services
Service Access Delivery	and	Service Transport	Service Transport
Service Access Delivery	and	Service Transport	Service Transport
Service Access Delivery	and	Service Transport	Service Transport
Service Access Delivery	and	Service Transport	Service Transport
Service Access Delivery	and	Service Transport	Service Transport
Service Platform Infrastructure	and	Supporting Platforms	Platform Independent
Service Platform Infrastructure	and	Supporting Platforms	Platform Dependent
Service Platform Infrastructure	and	Delivery Servers	Application Servers
Service Platform Infrastructure	and	Delivery Servers	Portal Servers
Service Platform Infrastructure	and	Delivery Servers	Media Servers
Service Platform Infrastructure	and	Delivery Servers	Media Servers

Infrastructure

Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management

Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Modeling
Service Platform and Infrastructure	Software Engineering	Modeling
Service Platform and Infrastructure	Database / Storage	Database

9.1.3.3 Partnerships

None.

9.1.4 Security and Privacy

9.1.4.1 How is it provided and funded?

The Flight Operations (FO) element of the United Space Alliance (USA) utilizes the security protocols and infrastructure set up to insure the integrity of the facilities and systems under FO control. USA maintains security control and administration in compliance with the NASA and JSC Information Technology (IT) Security Handbook. Access is limited to authorized personnel having a need to access any IT platform and is enforced utilizing multiple firewalls. The Station & Space Shuttle Program funds IT security.

9.1.4.2 How is security accomplished?

The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures, when NIST completes this process NASA will revisit its policy and procedures to conform to NIST new guidance.

Flight Operation IT Security incidents are handled and reported in accordance with Functional Policy & Procedure (FPP) D-03-06, IT Security Incident Reporting. Incidents involving NASA owned IT resources are reported to the appropriate NASA Office by United Space Alliance ITS. Processes have been established for the user role in incident handling. Annual security training ensures that users can recognize a security incident and respond properly. A priority list of contacts is established for communicating the incident and soliciting further response action. IT Security personnel review all incidents. Those with outside applicability are coordinated through established JSC incident response processes. Flight Operations (FO) IT Security personnel conduct intrusion detection monitoring. The FO IT Security personnel respond to alerts issued by the Center for vulnerabilities that are discovered in relevant security software or implementations. JSC administrators coordinate with external agencies regarding security incidents. Security relevant logs generated in the Flight Operations are reviewed at least monthly except where it can reasonably be accomplished and risk acceptance acknowledged. More frequent reviews are routinely done with narrower focus as interests dictate. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. United Space Alliance operates systems both on and off-site in support of NASA Programs. USA IT Security provides copies of all system security plans to NASA. USA IT Security provides system security posture presentations (obtained from the results of system IT security risk assessments) to the NASA SSP MIO Manager at JSC in order to obtain NASA's Authorization to Process (ATP) concurrence for each system.

9.1.4.3 Effective use of security, controls and authentication tools

Not applicable since the Flight Operations investment does not allow public access.

9.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. This investment does not support GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

10 Johnson Space Center (JSC) – Integrated Planning System

Project Description

The Mission Operations Directorate (MOD) plans, directs, manages, and implements overall mission operations including the Space Shuttle and Space Station programs; provides flight controller and flight crew training and simulations; and designs, upgrades, maintains, and operates the Mission Control Center (MCC), the mission simulators, and other major support facilities. The Directorate is responsible for:

- Developing integrated flight crew and flight control plans, procedures, and training.
- Establishing requirements for simulation and flight control ground instrumentation.
- Developing flight design.
- Configuring orbiter and International Space Station flight software.
- Contributing to the development and integration of spacecraft and payload support systems.
- Providing onboard portable computer hardware and software for the Space Shuttle and the International Space Station.
- Providing and directing real-time mission operations elements to support and control human space flight missions.
- Providing integrated concept development and requirements for ISS assembly, operations management, systems, training, and software analysis.
- Performing operations and training analysis of advanced space systems.

The Space Shuttle program plays a vital role in enabling NASA's vision and mission. This includes advancing human exploration and providing safe access to space in support of human operations in low-earth orbit. In order to maintain a viable human transportation capability that will operate and support NASA's launch requirements, specific program investments are required. NASA is revamping its approach to selecting and managing these investments to ensure Shuttle operability into the next decade and avoid future project overruns. These investments will be consistent with NASA's strategy of ensuring the Space Shuttle remains viable until a new transportation system is operational. These projects will provide revitalization of the infrastructure, and combat obsolescence of vehicle, ground systems, and facilities.

The International Space Station (ISS) is a complex of research laboratories in low Earth orbit in which American, Russian, Canadian, European, and Japanese astronauts are conducting unique scientific and technological investigations in a micro-gravity environment. The goal of the Station is to support scientific research and other activities requiring the unique attributes of humans in space and establish a permanent human presence in Earth orbit. The FY04 Budget request provides funding for continued development of the vehicle and for operations in support of continued assembly, logistics re-supply, crew exchange, research operations and other utilization. With fourteen U.S. assembly and logistic missions successfully completed, the budget includes funding to keep subsequent assembly missions on schedule through U.S. Core Complete (Flight 10A), currently planned for calendar year 2004, to support early research commensurate with the build-up of on-orbit utilization capabilities and resources.

(Source:FY04 IBPD)

The Integrated Planning Systems (IPS) provides the ground system computational capabilities which the Space Shuttle and the International Space Station (ISS) mission planners and flight controllers use for pre-mission planning, shuttle profile design and analysis including powered flight guidance and control software verification, post-mission analysis, and near real-time mission support. IPS is comprised of an Open Systems standards based data processing platform on which applications are hosted. IPS is a distributed system with Workstations (WS's) connected to computational and data servers. IPS provides a standard set of mission planning applications for producing the integrated mission activity timeline, and utilizes a central data management system to store and distribute products.

The JSC Integrated Planning System investment is in the Operations phase of NASA IT CPIC process, and this IT investment is managed as a component of the NASA project under NASA's NPG 7120 process.

Architecture

10.1.1 Business

10.1.1.1 Process simplification/reengineering/design projects

The Integrated Planning Systems (IPS) resulted from the incorporation of the Trajectory, Command, Analysis, and Timeline System (TCATS) from the Space Station Control Center (SSCC) into the successful Flight Analysis and Design System (FADS) project in the Summer of 1992. This combination of functions was done in the interest of providing more cost-effective mission support facilities for the Mission Operations Directorate (MOD). TCATS was intended to provide pre-mission and near real-time mission support tools for the Space Station Freedom Program. The FADS provided pre-mission trajectory design and post-mission analysis functions for the Space Shuttle Program. The IPS is planned to incorporate all mission planning/design functions for both the International Space Station (ISS) Program and the Space Shuttle Program in a common hardware and software system. These changes have been driven by new Program functional needs and by pressures to reduce costs. Strategic decisions were made in the early 90s to re-engineer the Mission Control Center (MCC) based on a Commercial Off The Shelf (COTS) based distributed system, based in large part on two key elements. The IPS is essentially complete and in a sustaining facility operations mode. As each of the IPS systems become classified as non-maintainable due to escalating sustaining cost or the system becomes non-maintainable by a commercial vendor, they will be replaced. As such, life cycle cost analysis is performed on each of the systems as part of the Non Maintainable Equipment (NME) action to ensure sustaining costs are brought back into line or reduced. A significant part of the IPS will undergo equipment replacement due to non-maintainability in the next 10 years.

10.1.1.2 Major organization restructuring, training and change management projects

None currently identified. As part of the project management process, any needed improvements will be made using existing system engineering processes in place within the Agency.

10.1.2 Data

10.1.2.1 *Types of Data*

Flight planning analysis trajectory, logistics, activity, and consumables information.

10.1.2.2 *Existing Data Access*

10.1.3 Application and Technology

10.1.3.1 *Relationship to Service Component Model*

Table 17

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Process Automation Services	Tracking Workflow	and Process Tracking		
Business Management Services	Management Process	of Change Management		
Business Management Services	Management Process	of Configuration Management		
Business Management Services	Management Process	of Requirements Management		
Business Management Services	Management Process	of Quality Management		
Business Management Services	Management Process	of Risk Management		

Digital Services	Asset	Document Management	Document Imaging and OCR
Digital Services	Asset	Document Management	Document Referencing
Digital Services	Asset	Document Management	Document Revisions
Digital Services	Asset	Document Management	Library / Storage
Digital Services	Asset	Document Management	Document Review and Approval
Digital Services	Asset	Document Management	Document Conversion
Digital Services	Asset	Document Management	Indexing
Digital Services	Asset	Document Management	Classification
Digital Services	Asset	Knowledge Management	Information Sharing
Digital Services	Asset	Knowledge Management	Knowledge Capture
Digital Services	Asset	Knowledge Management	Knowledge Distribution and Delivery
Business Analytical Services		Analysis Statistics	and Modeling
Business Analytical Services		Analysis Statistics	and Predictive
Business Analytical Services		Analysis Statistics	and Simulation
Business Analytical Services		Analysis Statistics	and Mathematical
Business Analytical Services		Analysis Statistics	and Structural Thermal /

Business Analytical Services		Visualization	Graphing / Charting
Business Analytical Services		Visualization	Imagery
Business Analytical Services		Visualization	Multimedia
Business Analytical Services		Visualization	CAD
Business Analytical Services		Reporting	Ad-Hoc
Business Analytical Services		Reporting	Standardization / Canned
Back Services	Office	Data Management	Data Exchange
Back Services	Office	Data Management	Data Mart
Back Services	Office	Data Management	Data Warehouse
Back Services	Office	Data Management	Meta Data Management
Back Services	Office	Data Management	Data Cleansing
Back Services	Office	Data Management	Extraction and Transformation
Back Services	Office	Data Management	Loading and Archiving
Back Services	Office	Data Management	Data Recovery
Back Services	Office	Data Management	Data Classification
Back Services	Office	Assets / Materials Management	Facilities Management

Back Services	Office	Assets / Materials Management	Computers Automation Management /
Back Services	Office	Development and Integration	Legacy Integration
Back Services	Office	Development and Integration	Data Integration
Back Services	Office	Development and Integration	Instrumentation and Testing
Back Services	Office	Development and Integration	Software Development
Support Services		Security Management	Identification and Authentication
Support Services		Security Management	Access Control
Support Services		Security Management	Encryption
Support Services		Security Management	Intrusion Detection
Support Services		Security Management	Verification
Support Services		Security Management	Digital Signature
Support Services		Security Management	User Management
Support Services		Security Management	Role / Privilege Management
Support Services		Security Management	Audit Trail Capture and Analysis
Support Services		Communication	Audio Conferencing
Support Services		Communication	Video Conferencing
Support Services		Systems Management	License Management
Support Services		Systems Management	Remote Systems Control

Support Services	Systems Management	Systems Resource Monitoring
Support Services	Systems Management	Software Distribution

10.1.3.2 Relationship to Technology Component Model

Table 18

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access and Delivery	Access Channels	Web Browser	
Service Access and Delivery	Access Channels	Web Browser	
Service Access and Delivery	Access Channels	Wireless / PDA	
Service Access and Delivery	Access Channels	Wireless / PDA	
Service Access and Delivery	Access Channels	Collaboration Communication	
Service Access and Delivery	Access Channels	Collaboration Communication	
Service Access and Delivery	Access Channels	Collaboration Communication	
Service Access and Delivery	Access Channels	Other Electronic Channels	
Service Access and Delivery	Access Channels	Other Electronic Channels	
Service Access and Delivery	Access Channels	Other Electronic Channels	
Service Access and Delivery	Service Requirements	Legislative / Compliance	
Service Access and Delivery	Service Requirements	Legislative / Compliance	
Service Access and Delivery	Service Requirements	Legislative / Compliance	
Service Access and Delivery	Service	Authentication / Single	

Delivery		Requirements	Sign-on (SSO)	
Service Access and Delivery		Service Requirements	Hosting	
Service Access and Delivery		Service Transport	Supporting Services	Network
Service Access and Delivery		Service Transport	Supporting Services	Network
Service Access and Delivery		Service Transport	Supporting Services	Network
Service Access and Delivery		Service Transport	Supporting Services	Network
Service Access and Delivery		Service Transport	Supporting Services	Network
Service Access and Delivery		Service Transport	Supporting Services	Network
Service Access and Delivery		Service Transport	Supporting Services	Network
Service Access and Delivery		Service Transport	Service Transport	
Service Access and Delivery		Service Transport	Service Transport	
Service Access and Delivery		Service Transport	Service Transport	
Service Access and Delivery		Service Transport	Service Transport	
Service Access and Delivery		Service Transport	Service Transport	
Service Platform and Infrastructure		Supporting Platforms	Platform Independent	
Service Platform and Infrastructure		Supporting Platforms	Platform Dependent	
Service Platform and Infrastructure		Delivery Servers	Application Servers	
Service Platform and Infrastructure		Delivery Servers	Portal Servers	
Service Platform and Infrastructure		Delivery Servers	Media Servers	

Infrastructure

Service Platform and Infrastructure	Delivery Servers	Media Servers
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software	Test Management

Infrastructure	Engineering	
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Modeling
Service Platform and Infrastructure	Software Engineering	Modeling
Service Platform and Infrastructure	Database Storage	/ Database
Service Platform and Infrastructure	Database Storage	/ Database
Service Platform and Infrastructure	Database Storage	/ Database
Service Platform and Infrastructure	Database Storage	/ Database
Service Platform and Infrastructure	Database Storage	/ Storage
Service Platform and Infrastructure	Database Storage	/ Storage

10.1.3.3 Partnerships

None.

10.1.4 Security and Privacy

10.1.4.1 How is it provided and funded?

Access to the Integrated Planning System (IPS) assets requires a User-ID and password. Passwords are changed on a regular and frequent basis. Acquisition and retention of an IPS account is contingent upon completion of annual security training. In addition, users requiring system privileges that bypass security controls must be investigated prior to receiving access. Security regulations, references, and incident response procedures are addressed in CIO security training.

Security control and administration in the IPS is compliant with the NASA and JSC Information Technology (I/T) Security Handbooks. These resources provide the basis for security policy and

assessment for the IPS. Proposed changes to the IPS architecture or operational procedures are reviewed for their influence on the security posture of the facility. Security controls are acquired, developed, or institutionalized to mitigate risk that is identified as unacceptable.

A Security Plan (SDPA-2100) is maintained and audited annually. The implemented security controls are evaluated annually against perceived threats. Actions are taken to strengthen the security posture if unacceptable weaknesses are identified. The resulting security posture is then reviewed with the Organizational Computer Security Manager (OCSM) for the Mission Operations Directorate (MOD).

A Contingency Plan is also maintained and audited annually. All IPS software and data are backed up on regular and frequent intervals. System restoration from backup is tested at least annually.

The security posture documented in the security and contingency plans is presented to MOD management on an annual basis. Emphasis is on the residual security risks inherent in the IPS given the implemented controls. MOD management decides whether to grant Authorization To Process (ATP) based on the acceptability of the residual risks.

Data pertaining to the security status of the IPS is recorded in the JSC Chief Information Officer's (CIO's) Information Technology (I/T) security database. This includes the most recent dates of the IPS Security and Contingency plans as well as the various security reviews. It also includes IPS points of contact for addressing security matters. This information supports security audits conducted by external organizations.

The SSP and ISS Programs fund IPS security. Security administration services are accounted for as a component of the overall IPS Program management. Implementation of security controls and routine sustaining and maintenance of security controls are accounted for under the overall IPS sustaining and maintenance. Security amounts to approximately 2% of the IPS I/T budget.

10.1.4.2 How is security accomplished?

The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures, when NIST completes this process NASA will revisit its policy and procedures to conform to NIST new guidance.

Processes have been established for the user role in incident handling. Annual security training ensures that users can recognize a security incident and respond properly. A priority list of contacts is established for communicating the incident and soliciting further response action. IT Security personnel review all incidents. Those with outside applicability are coordinated through established JSC incident response processes. IPS IT Security personnel conduct intrusion detection monitoring. The MCC IT Security personnel respond to alerts issued by the Center for

vulnerabilities that are discovered in relevant security software or implementations. JSC administrators coordinate with external agencies regarding security incidents. Security relevant logs generated in the Mission Control Center (MCC) are reviewed at least monthly except where it can reasonably be accomplished and risk acceptance acknowledged. More frequent reviews are routinely done with narrower focus as interests dictate. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. Security administration and management in accordance with JPG-2810.1 is contractually required. The IPS Project Manger and Mission Operations Directorate (MOD) management formally evaluate the Integrated Planning System (IPS) security posture on an annual basis. The IPS Project Manger and MOD management insight and influence on the IPS security administration is through regular participation in the bi-weekly Platform Change Assessment Group (PCAG) forums with the Contractor that serves to manage and control the IPS development, operations, and administration processes. Contractual mechanisms are also used to acquire security status and direct changes as necessary.

10.1.4.3 *Effective use of security, controls and authentication tools*

Public access to the IPS systems is not allowed. Layers of network protection and internal access controls ensure exclusion of public accessibility. Virtual Private Networks (VPN), Encrypted data distribution with access control, and dedicated lines are used to ensure access control to the IPS systems and data where entry or exit points are provided for internal use.

10.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. N/A. The JSC Integrated Planning System does not support electronic transactions or record keeping. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

11 Johnson Space Center (JSC) – Mission Control Center

Project Description

The Space Shuttle program plays a vital role in enabling NASA's vision and mission. This includes advancing human exploration and providing safe access to space in support of human operations in low-earth orbit. In order to maintain a viable human transportation capability that will operate and support NASA's launch requirements, specific program investments are required. NASA is revamping its approach to selecting and managing these investments to ensure Shuttle operability into the next decade and avoid future project overruns. These investments will be consistent with NASA's strategy of ensuring the Space Shuttle remains viable until a new transportation system is operational. These projects will provide revitalization

of the infrastructure, and combat obsolescence of vehicle, ground systems, and facilities.

The International Space Station (ISS) is a complex of research laboratories in low Earth orbit in which American, Russian, Canadian, European, and Japanese astronauts are conducting unique scientific and technological investigations in a micro-gravity environment. The goal of the Station is to support scientific research and other activities requiring the unique attributes of humans in space and establish a permanent human presence in Earth orbit. The FY04 Budget request provides funding for continued development of the vehicle and for operations in support of continued assembly, logistics re-supply, crew exchange, research operations and other utilization. With fourteen U.S. assembly and logistic missions successfully completed, the budget includes funding to keep subsequent assembly missions on schedule through U.S. Core Complete (Flight 10A), currently planned for calendar year 2004, to support early research commensurate with the build-up of on-orbit utilization capabilities and resources. (Source: FY04 IBPD)

The Mission Operations Directorate (MOD) plans, directs, manages, and implements overall mission operations including the Space Shuttle and Space Station programs; provides flight controller and flight crew training and simulations; and designs, upgrades, maintains, and operates the Mission Control Center (MCC), the mission simulators, and other major support facilities. The Directorate is responsible for:

- Developing integrated flight crew and flight control plans, procedures, and training.
- Establishing requirements for simulation and flight control ground instrumentation. Developing flight design.
- Configuring orbiter and International Space Station flight software.
- Contributing to the development and integration of spacecraft and payload support systems.
- Providing onboard portable computer hardware and software for the Space Shuttle and the International Space Station.
- Providing and directing real-time mission operations elements to support and control human space flight missions.
- Providing integrated concept development and requirements for ISS assembly, operations management, systems, training, and software analysis.
- Performing operations and training analysis of advanced space systems.

The JSC Mission Control Center (MCC) directly supports NASA's goals by providing command and control capabilities for safe mission operations of the International Space Station and Space Shuttle. The MCC provides common infrastructure architecture of distributed COTS, Unix workstations, servers, networks, voice systems, data storage and retrieval, and platform software to support multiple vehicles. The general-purpose software architecture provides a level of software infrastructure independent of program and vehicle. The support functions include flight reconfiguration product generation, mission planning, command and control flight operations, flight controller & crew training, & software development. Additional investments in Information Technology are necessary not only to maintain the existing equipment, but also to replace the equipment as it becomes non-maintainable due to escalating sustaining costs or due to the unavailability of commercial vendors.

The JSC Mission Control Center is in the Operations phase of NASA IT CPIC process, and this IT investment is managed as a component of the NASA project under NASA's NPG 7120 process.

Architecture

11.1.1 Business

11.1.1.1 Process simplification/reengineering/design projects

The JSC Mission Control Center (MCC) is an existing system for some 30 years. The MCC has undergone significant change in hardware, software, contracts and user management over the last 10 years. These changes have been driven by new Program functional needs and by pressures to reduce costs. Strategic decisions were made in the early 90s to re-engineer the MCC based on a Commercial Off The Shelf (COTS) based distributed system, based in large part on two key elements. The MCC is essentially complete and in a sustaining facility operations posture. As each of the MCC systems become classified as non-maintainable due to escalating sustaining cost or the system becomes non-maintainable by a commercial vendor, they will be replaced. As such, life cycle cost analysis is performed on each of the systems as part of the Non Maintainable Equipment (NME) action to ensure sustaining costs are brought back into line or reduced. A significant part of the MCC will undergo equipment replacement due to non-maintainability in the next 10 years, from front-end equipment, networks, voice systems, and user workstations.

11.1.1.2 Major organization restructuring, training and change management projects

None currently identified. As part of the project management process, any needed improvements will be made using existing system engineering processes in place within the Agency.

11.1.2 Data

11.1.2.1 Types of Data

The types of data used in this project are Science Engineering and Research (SER), Crew member health, International Space Station (ISS) and Space Shuttle Program (SSP) vehicle telemetry and commanding, and voice.

11.1.2.2 Existing Data Access

11.1.3 Application and Technology

11.1.3.1 Relationship to Service Component Model

Table 19

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
				<p>The MCC provides support through the following functions: flight reconfiguration, product generation, mission planning, command and control flight operations, flight controller and crew training, and software development. The MCC is providing a mission specific delivery of service that is very specialized and is difficult to leverage outside Space Operations. The SRM does not really lend itself to a complete, detailed analysis of the MCC application. MCC functions map into the SRM into the following Key Service Domain/Service Type/Components: Listing for SRM Service Domain/Service Type/Components</p> <ul style="list-style-type: none"> * Process Automation Services (Domain) - Tracking and Workflow (Type) - Process Tracking (Component) * Business Management Services (Domain) - Management of Process (Type) - Change Management, Configuration Management, Requirements Management, Quality Management, and Risk Management (Components) * Digital Asset Services (Domain) - Document Management (Type) - Document Imaging and OCR, Document Referencing, Document Revisions, Library / Storage, Document Review and Approval, Document Conversion, Indexing, and Classification (Components) * Digital Asset Services (Domain) - Knowledge Management (Type) - Information Sharing, Knowledge Capture, and Knowledge Distribution and Delivery (Components). * Business Analytical Services (Domain) - Analysis and Statistics (Type) -

Modeling, Predictive, Simulation, Mathematical, and Structural / Thermal (Components)

*** Business Analytical Services (Domain)
- Visualization (Type) - Graphing / Charting, Imagery, Multimedia, and CAD (Components)**

*** Business Analytical Services (Domain)
- Reporting (Type) - Ad Hoc and Standardized / Canned (Components)**

*** Back Office Services (Domain) - Data Management (Type) - Data Exchange, Data Mart, Data Warehouse, Meta Data Management, Data Cleansing, Extraction and Transformation, Loading and Archiving, Data Recovery, and Data Classification (Components)**

*** Back Office Services (Domain) - Assets / Materials Management (Type) - Facilities Management, and Computers / Automation Management (Components)**

*** Back Office Services (Domain) - Development and Integration (Type) - Legacy Integration, Data Integration, Instrumentation and Testing, and Software Development (Components)**

*** Support Services (Domain) - Security Management (Type) - Identification and Authentication, Access Control, Encryption, Intrusion Detection, Verification, Digital Signature, User Management, Role / Privilege Management, and Audit Trail Capture and Analysis (Components)**

*** Support Services (Domain) - Communication (Type) - Audio Conferencing and Video Conferencing (Components)**

*** Support Services (Domain) - Systems Management (Type) - License Management, Remote Systems Control, System Resource Monitoring, and Software Distribution (Components)**

11.1.3.2 Relationship to Technology Component Model

Table 20

Service Area	Service Category	Service Standard	Relation to SRM of FEA
			<p>The Service Area, Service Category, Service Standard, and Service Specification that describe the technology supporting the Mission Control Center are listed below.</p> <ul style="list-style-type: none"> * Service Access and Delivery (Core Service Area) <ul style="list-style-type: none"> - Access Channels (Service) - Web Browser (Standard) - Internet Explorer and Netscape Communicator (Specification) * Service Access and Delivery (Core Service Area) <ul style="list-style-type: none"> - Access Channels (Service) - Wireless / PDA (Standard) - Palm Pilot, Blackberry (Specification) * Service Access and Delivery (Core Service Area) <ul style="list-style-type: none"> - Access Channels (Service) - Collaboration Communications (Standard) - Electronic Mail, Fax, Kiosk (Specification) * Service Access and Delivery (Core Service Area) <ul style="list-style-type: none"> - Access Channels (Service) - Other Electronic Channels (Standard) - System to System, Web Service, URL (Specification) * Service Access and Delivery (Core Service Area) <ul style="list-style-type: none"> - Delivery Channels (Service) - Internet, Intranet, Extranet, VPN (Standard) * Service Access and Delivery (Core Service Area) <ul style="list-style-type: none"> - Service Requirements (Service) - Legislative / Compliance (Standard) - Section 508, Web Content Accessibility, Security, Privacy (Specification) * Service Access and Delivery (Core Service Area) <ul style="list-style-type: none"> - Service Requirements (Service) - Authentication / Single Sign-on (Standard) * Service Access and Delivery (Core Service Area) <ul style="list-style-type: none"> - Service Requirements (Service) - Hosting (Standard) - Internal (within Agency), External (ISP/ASP/FirstGov) (Specification) * Service Access and Delivery (Core Service Area) <ul style="list-style-type: none"> - Service Transport (Service) - Supporting Network Services (Standard) - IMAP / POP3, MIME, SMTP, ESMTP, T.120, LDAP, Directory Services (Specification) * Service Access and Delivery (Core Service Area) <ul style="list-style-type: none"> - Service Transport (Service) - Service Transport (Standard) - TCP, IP, HTTP, HTTPS, WAP, FTP (Specification)

11.1.3.3 Partnerships

None.

11.1.4 Security and Privacy

11.1.4.1 How is it provided and funded?

Access to JSC Mission Control Center (MCC) assets requires a User-ID and password. Passwords are changed on a regular and frequent basis. Acquisition and retention of an MCC account is contingent upon completion of annual security training. In addition, users requiring system privileges that bypass security controls must be investigated prior to receiving access. Security regulations, references, and incident response procedures are addressed in Center Information Office (CIO) security training. Security control and administration in the MCC is compliant with the NASA and JSC Information Technology (I/T) Security Handbooks. These resources provide the basis for security policy and assessment for the MCC.

Proposed changes to the MCC architecture or operational procedures are reviewed for their influence on the security posture of the facility. Security controls are acquired, developed, or institutionalized to mitigate risk that is identified as unacceptable.

A Security Plan (SDPA-3200) is maintained and audited annually. The implemented security controls are evaluated annually against perceived threats. Actions are taken to strengthen the security posture if unacceptable weaknesses are identified. The resulting security posture is then reviewed with the Organizational Computer Security Manager (OCSM) for the Mission Operations Directorate (MOD).

A Contingency Plan is also maintained and audited annually. All MCC software and data are backed up on regular and frequent intervals. System restoration from backup is tested at least annually.

The security posture documented in the security and contingency plans is presented to MOD management on an annual basis. Emphasis is on the residual security risks inherent in the MCC given the implemented controls. MOD management decides whether to grant Authorization To Process (ATP) based on the acceptability of the residual risks.

Data pertaining to the security status of the Mission Control Center (MCC) is recorded in the JSC Chief Information Officer's (CIO's) Information Technology (I/T) security database. This includes the most recent dates of the MCC Security and Contingency plans as well as the various security reviews. It also includes MCC points of contact for addressing security matters. This information supports security audits conducted by external organizations.

The Space Shuttle Program (SSP) and International Space Station (ISS) Programs fund the MCC

security. Security administration services are accounted for as a component of the overall MCC Program management. Implementation of security controls and routine sustaining and maintenance of security controls are accounted for under the overall MCC sustaining and maintenance. Security amounts to approximately 4% of the MCC I/T budget.

11.1.4.2 *How is security accomplished?*

The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures, when NIST completes this process NASA will revisit its policy and procedures to conform to NIST new guidance.

Dates of Last review are:

- MSOC - Mission Control Center June 10, 2003
- SFOC - Software Engineering Network (SWEN), March 31, 2004
- SFOC - Payload Operations Ground System (POGS), March 31, 2004
- SFOC - Remote Support System (RSS), March 31, 2004

Processes have been established for the user role in incident handling. Annual security training ensures that users can recognize a security incident and respond properly. A priority list of contacts is established for communicating the incident and soliciting further response action. IT Security personnel review all incidents. Those with outside applicability are coordinated through established JSC incident response processes. MCC IT Security personnel conduct intrusion detection monitoring. The MCC IT Security personnel respond to alerts issued by the Center for vulnerabilities that are discovered in relevant security software or implementations. JSC administrators coordinate with external agencies regarding security incidents. Security relevant logs generated in the MCC are reviewed at least monthly except where it can reasonably be accomplished and risk acceptance acknowledged. More frequent reviews are routinely done with narrower focus as interests dictate. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. A majority of the MCC is operated on site except for limited development activities conducted from the Contractor facility through a dedicated interface. Security administration and management in accordance with JPG-2810.1 is contractually required. The MCC Project Manger and Mission Operations Directorate (MOD) management formally evaluate the MCC security posture on an annual basis. The MCC Project Manger and MOD management insight and influence on the MCC security administration is through regular participation in forums with the Contractor that serves to manage and control the MCC development, operations, and administration processes. Contractual mechanisms are also used to acquire security status and direct changes as necessary.

11.1.4.3 *Effective use of security, controls and authentication tools*

Public access to the MCC systems is not allowed. Layers of network protection and internal access controls ensure exclusion of public accessibility. Virtual Private Networks (VPS), Encrypted data distribution with access control, and dedicated lines are used to ensure access control to the MCC systems and data where entry or exit points are provided for internal use.

11.1.5 Government Paperwork Elimination Act

N/A. This system does not support electronic transactions or record keeping covered by GPEA.

12 Johnson Space Center (JSC) – Software Development / Integration Laboratory

Project Description

The International Space Station (ISS) prime contract was awarded in 1993 to Boeing as a performance based contract for the total integrated design, development, manufacture, and integration of the U.S. On-Orbit Segment (USOS) of the ISS. As such, Boeing is responsible for integrating all ISS systems and subsystems such as the Command and Data Handling (C&DH) subsystem, including International Partner/Participant (IP/P) elements which interface with the USOS, government furnished equipment (GFE) developed by other contractors and provided to Boeing, providing ground support equipment (GSE), and providing technical support for ground and orbital operations.

The Software Development and Integration Laboratory (SDIL)/Avionics are the command and data handling (C&DH) subsystem utilizing the onboard computer and network capabilities of the ISS. It also includes the ground support and test functions for the associated ground operations and sustaining engineering. As such, this "project" supports the International Space Station. The C&DH functions executed using the onboard computer and network capabilities are an embedded technical subsystem of the ISS spacecraft vehicle. The C&DH subsystem is a critical subsystem of the ISS, providing the essential capabilities to perform guidance, navigation, and control commands to keep the ISS in orbit, and to handle critical on-orbit activities, such as power distribution, crew housekeeping activities, and research and science experiments in the laboratory module.

The ISS prime contract was awarded in 1993 to Boeing as a performance based contract for the total integrated design, development, manufacture, and integration of the U.S. On-Orbit Segment (USOS) of the ISS. As such, Boeing is responsible for integrating all ISS systems and subsystems such as the C&DH subsystem, including International Partner/Participant (IP/P) elements which interface with the USOS, government furnished equipment (GFE) developed by other contractors and provided to Boeing, providing ground support equipment (GSE), and providing technical support for ground and orbital operations.

The C&DH subsystem encompasses:

- 1.45 million lines of unique flight software code with 2.6 million additional lines of simulation code
- 47 Multiplexer - Demultiplexer computers
- 100 data bus networks
- The avionics activities that must be performed by the contractor to support the C&DH subsystem are:
- Hardware/Software Integration (HSI)
Perform ISS hardware/software integration, design integration, command and telemetry verification, and stage software verification; Provide flight support including C&DH MER console support and mission flight following; Provide flight software support at KSC and MOD personnel
- Guidance, Navigation & Control (GN&C)
- Perform engineering analysis, GN&C subsystem integration, and design of mission specific Pre-Position Loads (PPLs); Provide sustaining engineering support for the GN&C subsystem; Provide GN&C support to MEIT.
- Communications & Tracking (C&T)
- Perform C&T subsystem analysis and subsystem integration; Prepare CoFR packages;
- Perform Audio, Space to Space, Space to Ground Ku-Band, and S-Band evidence of requirements closure; Provide sustaining engineering support for the C&T subsystem;
- Provide C&T support to MEIT.
- C&DH Hardware
- Maintain and sustain C&DH hardware; Perform C&DH networks analysis; Provide sustaining engineering support for Avionics ORUs and cabling for PMA's, Node 1 and
- Truss Elements; Provide C&DH support to MEIT.
- Consolidated Laboratories

Provide and sustain the SVF, PSPF and SITE test rigs and expand the ISIL ITR; Perform SDIL systems engineering, maintenance and operation and perform test rig management; Provide computed systems security for all systems and ADPE.

ISIL Laboratory Improvements to Support Flight: Identify and implement laboratory fidelity improvements to support near-term flights

ASIL Implementation - Define requirements, design, implement and perform, operate and maintain an integrated test system to support long-term ISS program objectives for hardware/software integration and flight support.

The investment is in the Steady State portion of NASA's CPIC process.

Architecture

12.1.1 Business

12.1.1.1 *Process simplification/reengineering/design projects*

Improvements will be made using existing system engineering and ISO 9000 processes under the Vehicle Segment Sustaining Engineering (Contract F:), also the Software Processes were certified to Software Engineering Institute (SEI) Level 3 which is a continuing improvement process. The system has already successfully been augmented with enhanced capabilities. New commercial products have been added where stringent requirements can be achieved from Commercial Off The Shelf (COTS). New missions and services may require systems to change, which would be handled through the annual budget process.

12.1.1.2 *Major organization restructuring, training and change management projects*

Since the International Space Station (ISS) is a mature program that has been in place since 1993, the current organization and processes will continue to be utilized. The ISS Program continually examines where program management and organizational improvements can be made based on program goals, progress, and evolution.

12.1.2 Data

12.1.2.1 *Types of Data*

SER (Science, Engineering, and Research) -- Spacecraft telemetry, including science data and video, Earth Observing System data and video, Science Payload data and video as well as Human research data collected from Astronaut subjects.

12.1.2.2 *Existing Data Access*

12.1.3 Application and Technology

12.1.3.1 *Relationship to Service Component Model*

Table 21

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Business Management	Management of Process	Change Management		The IT Support for JSC Software

Services

Utilization/Integration

Laboratory supports C&DH functions executed using the onboard computer and network capabilities that are an embedded technical subsystem of the ISS spacecraft vehicle. The C&DH subsystem is a critical subsystem of the ISS, providing the essential capabilities to perform guidance, navigation, and control commands to keep the ISS in orbit, and to handle critical on-orbit activities, such as power distribution, crew housekeeping activities, and research and science experiments in the laboratory module. The IT Support for JSC Software

Utilization/Integration

Laboratory is providing a mission specific delivery of service that is very specialized and is difficult to leverage outside Space Transportation. The SRM does not really lend itself to a complete, detailed analysis of the IT Support for JSC Software

Utilization/Integration

Laboratory application. IT Support for JSC Software Development /Integration Laboratory functions map into the SRM into the following Key Service Domain/Service

**Type/Components:
Listing for SRM Service
Domain/Service
Type/Components
* Business Management
Services (Domain) -
Management of Process
(Type) - Change
Management,
Configuration
Management,
Requirements
Management, Quality
Management, and Risk
Management
(Components)
* Digital Asset Services
(Domain) - Document
Management (Type) -
Document Imaging and
OCR, Document
Referencing, Document
Revisions, Library /
Storage, Document
Review and Approval,
Document Conversion,
Indexing, and
Classification
(Components)
* Back Office Services
(Domain) - Data
Management (Type) -
Data Exchange, Data
Mart, Data Warehouse,
Meta Data Management,
Data Cleansing,
Extraction and
Transformation, Loading
and Archiving, Data
Recovery, and Data
Classification
(Components)
* Back Office Services
(Domain) - Assets /
Materials Management
(Type) -Facilities
Management, and
Computers / Automation
Management**

(Components)

*** Back Office Services (Domain) - Development and Integration (Type) - Legacy Integration, Data Integration, Instrumentation and Testing, and Software Development (Components)**

*** Support Services (Domain) - Security Management (Type) - Identification and Authentication, Access Control, Encryption, Intrusion Detection, Verification, Digital Signature, User Management, Role / Privilege Management, and Audit Trail Capture and Analysis (Components)**

*** Support Services (Domain) - Systems Management (Type) - License Management, Remote Systems Control, System Resource Monitoring, and Software Distribution (Components)**

Business Management Services	Management of Process	Configuration Management
Business Management Services	Management of Process	Requirements Management
Business Management Services	Management of Process	Quality Management
Business Management Services	Management of Process	Risk Management

Digital Asset Services	Document Management	Document Imaging and OCR
Digital Asset Services	Document Management	Document Referencing
Digital Asset Services	Document Management	Document Revisions
Digital Asset Services	Document Management	Library / Storage
Digital Asset Services	Document Management	Document Review and Approval
Digital Asset Services	Document Management	Document Conversion
Digital Asset Services	Document Management	Indexing
Digital Asset Services	Document Management	Classification
Back Office Services	Data Management	Data Exchange
Back Office Services	Data Management	Data Mart
Back Office Services	Data Management	Data Warehouse
Back Office Services	Data Management	Meta Data Management
Back Office Services	Data Management	Data Cleansing
Back Office Services	Data Management	Extraction and Transformation
Back Office Services	Data Management	Loading and Archiving
Back Office Services	Data Management	Data Recovery
Back Office Services	Data Management	Data Classification
Back Office	Assets /	Facilities

Services	Materials Management	Management
Back Office Services	Assets / Materials Management	Computers / Automation Management
Back Office Services	Development and Integration	Legacy Integration
Back Office Services	Development and Integration	Data Integration
Back Office Services	Development and Integration	Instrumentation and Testing
Back Office Services	Development and Integration	Software Development
Support Services	Security Management	Identification and Authentication
Support Services	Security Management	Access Control
Support Services	Security Management	Encryption
Support Services	Security Management	Intrusion Detection
Support Services	Security Management	Verification
Support Services	Security Management	Digital Signature
Support Services	Security Management	User Management
Support Services	Security Management	Role / Privilege Management
Support Services	Security Management	Audit Trail Capture and Analysis
Support Services	Systems Management	License Management

Support Services	Systems Management	Remote Systems Control
Support Services	Systems Management	Systems Resource Monitoring
Support Services	Systems Management	Software Distribution

12.1.3.2 Relationship to Technology Component Mode

Table 221

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Platform and Infrastructure	Supporting Platforms	Platform Independent	<p>The Service Area, Service Category, Service Standard, and Service Specification that describe the technology supporting the IT Support for ISS Boeing Prime is</p> <ul style="list-style-type: none"> * Service Platform and Infrastructure (Core Service Area) - Support Platforms (Service) - Platform Independent (J2EE) (Standard) - Java 2 Enterprise Edition (Specification) * Service Platform and Infrastructure (Core Service Area) - Support Platforms (Service) - Platform Dependent (MS) (Standard) - Windows 2000(Specification) * Service Platform and Infrastructure (Core Service Area) - Delivery Servers (Service) - Application Servers (Standard) * Service Platform and Infrastructure (Core Service Area) - Delivery Servers (Service) - Portal Servers (Standard) * Service Platform and Infrastructure (Core Service Area) - Delivery Servers (Service) - Media Servers (Standard) - Real Audio, Windows Media Services (Specification) * Service Platform and

**Infrastructure (Core Service Area) -
 Software Engineering (Service) -
 Integrated Development
 Environment (Standard) - IBM
 WebSphere Studio, Visual Studio,
 Visual Studio .NET (Specification)
 * Service Platform and
 Infrastructure (Core Service Area) -
 Software Engineering (Service) -
 Software Configuration
 Management (Standard) - Version
 Management, Defect Tracking,
 Issue Management, Task
 Management, Change
 Management, Deployment
 Management, Requirements
 Management (Specification)
 * Service Platform and
 Infrastructure (Core Service Area) -
 Software Engineering (Service) -
 Test Management (Standard) -
 Functional testing, Business Cycle
 Testing, Usability Testing,
 Performance Profiling,
 Load/Stress/Volume Testing,
 Security and Access Control
 Testing, Reliability Testing,
 Configuration Testing, Installation
 Testing (Specification)
 * Service Platform and
 Infrastructure (Core Service Area) -
 Software Engineering (Service) -
 Modeling (Standard) - UML, Case
 Management (Specification)
 * Service Platform and
 Infrastructure (Core Service Area) -
 Database / Storage (Service) -
 Database (Standard) - DB2, Oracle,
 SQL Server, Sybase (Specification)
 * Service Platform and
 Infrastructure (Core Service Area) -
 Database / Storage (Service) -
 Storage (Standard) - NAS, SAN
 (Specification)
 * Service Platform and
 Infrastructure (Core Service Area) -
 Hardware / Infrastructure (Service)
 - Servers / Computers (Standard) -
 Enterprise Server, Mainframe**

(Specification)
 * Service Platform and Infrastructure (Core Service Area) - Hardware / Infrastructure (Service)
 - Embedded Technology Devices (Standard) - RAM, Hard Disk Drive, Microprocessor, RAID (Specification)
 * Service Platform and Infrastructure (Core Service Area) - Hardware / Infrastructure (Service)
 - Peripherals (Standard) - Printer, Scanner (Specification)
 * Service Platform and Infrastructure (Core Service Area) - Hardware / Infrastructure (Service)
 - WAN (Standard) - Frame Relay, ATM (Specification)
 * Service Platform and Infrastructure (Core Service Area) - Hardware / Infrastructure (Service)
 - LAN (Standard) - Ethernet, Token Ring, VLAN (Specification)
 * Service Platform and Infrastructure (Core Service Area) - Hardware / Infrastructure (Service)
 - Network Devices / Standards (Standard) - Hub, Switch, Router, NIC, Transceivers, Gateway, ISDN, T1 / T3, DSL, Firewall (Specification)
 * Service Platform and Infrastructure (Core Service Area) - Hardware / Infrastructure (Service)
 - Video Conferencing (Standard) - Bridge, CODEC, Receiver (Specification)

Service Platform and Infrastructure	Supporting Platforms	Platform Dependent
Service Platform and Infrastructure	Delivery Servers	Application Servers
Service Platform and Infrastructure	Delivery Servers	Portal Servers
Service Platform and	Delivery	Media Servers

Infrastructure	Servers	
Service Platform and Infrastructure	Delivery Servers	Media Servers
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Test Management

Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Modeling
Service Platform and Infrastructure	Software Engineering	Modeling
Service Platform and Infrastructure	Database Storage	/ Database
Service Platform and Infrastructure	Database Storage	/ Database
Service Platform and Infrastructure	Database Storage	/ Database
Service	Database	/ Database

Platform and Infrastructure	Storage		
Service Platform and Infrastructure	Database Storage	/	Storage
Service Platform and Infrastructure	Database Storage	/	Storage
Service Platform and Infrastructure	Hardware Infrastructure	/	Servers Computers /
Service Platform and Infrastructure	Hardware Infrastructure	/	Servers Computers /
Service Platform and Infrastructure	Hardware Infrastructure	/	Embedded Technology Devices
Service Platform and Infrastructure	Hardware Infrastructure	/	Embedded Technology Devices
Service Platform and Infrastructure	Hardware Infrastructure	/	Embedded Technology Devices
Service Platform and Infrastructure	Hardware Infrastructure	/	Embedded Technology Devices
Service Platform and Infrastructure	Hardware Infrastructure	/	Peripherals
Service Platform and Infrastructure	Hardware Infrastructure	/	Peripherals
Service Platform and Infrastructure	Hardware Infrastructure	/	Wide Area Network (WAN)
Service Platform and Infrastructure	Hardware Infrastructure	/	Wide Area Network (WAN)
Service Platform and Infrastructure	Hardware Infrastructure	/	Local Area Network (LAN)

Infrastructure

Service Platform and Infrastructure **Hardware / Infrastructure** **Local Area Network (LAN)**

Service Platform and Infrastructure **Hardware / Infrastructure** **Local Area Network (LAN)**

Service Platform and Infrastructure **Hardware / Infrastructure** **Network Devices / Standards**

Service Platform and Infrastructure **Hardware / Infrastructure** **Network Devices / Standards**

Service Platform and Infrastructure **Hardware / Infrastructure** **Network Devices / Standards**

Service Platform and Infrastructure **Hardware / Infrastructure** **Network Devices / Standards**

Service Platform and Infrastructure **Hardware / Infrastructure** **Network Devices / Standards**

Service Platform and Infrastructure **Hardware / Infrastructure** **Network Devices / Standards**

Service Platform and Infrastructure **Hardware / Infrastructure** **Network Devices / Standards**

Service Platform and Infrastructure **Hardware / Infrastructure** **Network Devices / Standards**

Service Platform and Infrastructure **Hardware / Infrastructure** **Network Devices / Standards**

Service Interface and Integration **Hardware / Infrastructure** **Network Devices / Standards**

Service Platform and Infrastructure **Hardware / Infrastructure** **Video Conferencing**

Service Platform and Infrastructure Hardware / Infrastructure Video Conferencing

Service Platform and Infrastructure Hardware / Infrastructure Video Conferencing

12.1.3.3 *Partnerships*

None.

12.1.4 Security and Privacy

12.1.4.1 *How is it provided and funded?*

Security for the JSC Software Development/Integration Laboratory is funded by the International Space Station Program (ISSP).

The International Space Station Program (ISSP) configuration presently consists of only U.S. and Russian ground and onboard elements. Other ISSP partners and participants are providing documentation that their contributions and infrastructures have been designed with IT security controls included.

The operational functions necessary to command and control the ISS are possible only from Mission Control Centers (MCCs) in both the U.S. and Russia. The MCCs have the ability to send commands, receive/monitor telemetry, compute ballistics/trajjectory, and plan daily events. Interconnecting networks and uplink/downlink capability are utilized to communicate between the MCC and the ISS.

The ISS vehicle systems described in this document do not have traditional IT activities. Where traditional IT systems are thought of as systems for storing, sharing, and printing electronic files. In other words, there are only command and control activities with inherent IT aspects imbedded in the planned command and control procedures executed by trained flight controllers through the MCCs.

The details of the system architecture are contained in the MCC Security Plan, Consolidated Space Operations Contract (CSOC)-JSC-Plan_00238 and in the System Specification for the International Space Station, SSP-41000. Communication links for data transfers are performed via secure links established and maintained in accordance with guidelines set out in the Space to Ground Increment Control Documents SSP-41154 and SSP-42108. Additional security documentation is also available in MOD's MCC Distributed Security Plan, SPDA0008. Critical processing times are 24 hours a day, 7 days a week. The systems onboard the vehicle serves the

occupants of the vehicle.

The general public is not allowed access to this system. Furthermore, encryption is used on the RF link between the MCC and the vehicle. Additionally, there is a physical control due to the general public not having access to space vehicles.

The ISS Program Management conducts security control reviews annually.

12.1.4.2 How is security accomplished?

The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures, when NIST completes this process NASA will revisit its policy and procedures to conform to NIST new guidance.

The incident handling and reporting capability is incorporated in the SDIL security plan. Intrusion monitoring and detection is handled by systems incorporated in the firewall structures protecting the SDIL systems. Audit logs are reviewed on regular basis at least if not every few days. For all ground based systems supporting the ISS, intruder detection tools, Symantec's Intruder Alert, have been deployed on identified critical systems. Changes to critical files on those systems result in alerts being sent to system administration personnel. Passive security monitors, Symantec's Enterprise Security Manager, have been deployed on identified critical systems as well a number of other servers. Incorrect settings are detected in a timely manner and reported to System personnel and appropriate action taken. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. The ISS is controlled by the Mission Control Center which is a Joint NASA and Contractor team. A majority of the MCC is operated on site except for limited development activities conducted from the Contractor facility through a dedicated interface. Security administration and management in accordance with JPG-2810.1 is contractually required. The MCC Project Manger and MOD management formally evaluate the MCC security posture on an annual basis. The MCC Project Manger and MOD management insight and influence on the MCC security administration is through regular participation in forums with the Contractor that serves to manage and control the MCC development, operations, and administration processes. Contractual mechanisms are also used to acquire security status and direct changes as necessary. The ISS Organizational Security Computer Manager (OSCM) reviews specific security documents and procedures annually and evaluates the overall risk. For all identified risk a risk analysis and mitigation is conducted and reported to the ISS Program Manager for agreement on any residual risk(s).

12.1.4.3 *Effective use of security, controls and authentication tools*

Public access is not permitted to the JSC Software Development/Integration Laboratory.

12.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. This JSC Software Development/Integration Laboratory does not support electronic transactions or recordkeeping that is covered by GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

13 Johnson Space Center (JSC) – Space Shuttle Program Cockpit Avionics Upgrade

Project Description

The CAU will implement new Orbiter cockpit avionic hardware and software to meet the man-machine interface requirements identified by the Space Shuttle Cockpit Council to enhance overall crew safety. Orbiter cockpit displays and crew interface capabilities will be significantly improved by replacing the existing Integrated Display Processors (IDPs) with higher performance Command and Display Processors (CDPs). These units will provide expanded processing performance to enable dramatic improvements in information access and display capability as well as the implementation of the new Abort Flight Management software function.

As part of the Space Shuttle project approval process, the CAU Project has been fully reviewed and approved previously by the capital planning and investment committee. In addition the project has been approved each year since its inception in FY2000 by both the Program Operating Plan reviews and numerous independent audits and reviews. Space Shuttle Program Management as well as NASA Enterprise management is updated on a periodic (monthly and quarterly respectively) basis as to the status of technical objectives, risk monitoring and amelioration, and resource/schedule management status and projections through earned value reporting.

Architecture

13.1.1 Business

13.1.1.1 *Process simplification/reengineering/design projects*

Orbiter cockpit displays and crew interface capabilities will be significantly improved by replacing the existing Integrated Display Processors (IDPs) with higher performance and more

reliable Command and Display Processors (CDPs). The Cockpit Avionics Upgrade (CAU) Project will improve crew safety by providing better information in a more timely fashion which will result in improved decision making and a reduction in astronaut workload during critical mission phases.

13.1.1.2 Major organization restructuring, training and change management projects

This project was undertaken as part of an overall safety upgrades effort associated with the Space Shuttle Program and therefore will not have a significant impact on these areas. However, crew training will be reduced as data is presented in a more comprehensive and intuitive fashion during missions as opposed to the current system which requires the performance of additional analytical steps by the crew in a high workload environment.

13.1.2 Data

13.1.2.1 Types of Data

The Space Shuttle Cockpit Avionics Upgrade investment will format primary avionics software system data, backup flight software data, operational instrumentation data, and payload information data onto displays utilized by the flight crew during missions to low Earth orbit. The Project also enables the execution of commands from any display format or multi-function display unit.

13.1.2.2 Existing Data Access

13.1.3 Application and Technology

13.1.3.1 Relationship to Service Component Model

Table 23

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Business Management Services	Management of Process	Change Management		The Space Shuttle Program Cockpit Avionics Upgrade will support implementation of a new Orbiter avionics hardware and software to meet the man-machine interface requirements The Space Shuttle Program Cockpit Avionics Upgrade is

providing a mission specific delivery of service that is very specialized and is difficult to leverage outside Space Transportation. The SRM does not really lend itself to a complete, detailed analysis of the Space Shuttle Program Cockpit Avionics Upgrade application. A very small portion (< 2%) of the flight software CAU project functions providing support to project managers, engineers, and support personnel can be mapped into the SRM. Space Shuttle Program Cockpit Avionics Upgrade functions map into the SRM into the following Key Service Domain/Service

Type/Components:

Listing for SRM Service Domain/Service

Type/Components

* Business Management Services (Domain) -

Management of Process (Type)

- Change Management,

Configuration Management,

Requirements Management,

Quality Management, and Risk

Management (Components)

* Digital Asset Services

(Domain) - Document

Management (Type) -

Document Imaging and OCR,

Document Referencing,

Document Revisions, Library /

Storage, Document Review and

Approval, Document

Conversion, Indexing, and

Classification (Components)

* Back Office Services

(Domain) - Data Management

(Type) - Data Exchange,

Extraction and Transformation, Loading and Archiving, Data Recovery, and Data Classification (Components)

* Back Office Services (Domain) - Assets / Materials Management (Type) -Facilities Management, and Computers / Automation Management (Components)

* Back Office Services (Domain) - Development and Integration (Type) - Legacy Integration, Data Integration, Instrumentation and Testing, and Software Development (Components)

* Support Services (Domain) - Security Management (Type) - Identification and Authentication, Access Control, Intrusion Detection, Verification, User Management, Role / Privilege Management, and Audit Trail Capture and Analysis (Components)

* Support Services (Domain) - Systems Management (Type) - License Management, Remote Systems Control, System Resource Monitoring, and Software Distribution (Components)

Business Management Services	Management of Process	Configuration Management
Business Management Services	Management of Process	Requirements Management
Business Management Services	Management of Process	Quality Management
Business Management Services	Management of Process	Risk Management

Digital Asset Services	Document Management	Document Imaging and OCR
Digital Asset Services	Document Management	Document Referencing
Digital Asset Services	Document Management	Document Revisions
Digital Asset Services	Document Management	Library / Storage
Digital Asset Services	Document Management	Document Review and Approval
Digital Asset Services	Document Management	Document Conversion
Digital Asset Services	Document Management	Indexing
Digital Asset Services	Document Management	Classification
Back Office Services	Data Management	Data Exchange
Back Office Services	Data Management	Extraction and Transformation
Back Office Services	Data Management	Loading and Archiving
Back Office Services	Data Management	Data Recovery
Back Office Services	Data Management	Data Classification
Back Office Services	Assets / Materials Management	Facilities Management
Back Office Services	Assets / Materials Management	Computers / Automation Management
Back Office Services	Development and Integration	Legacy Integration
Back Office Services	Development and Integration	Data Integration
Back Office Services	Development and Integration	Instrumentation and Testing
Back Office Services	Development and Integration	Software Development

Support Services	Security Management	Identification and Authentication
Support Services	Security Management	Access Control
Support Services	Security Management	Intrusion Detection
Support Services	Security Management	Verification
Support Services	Security Management	User Management
Support Services	Security Management	Role / Privilege Management
Support Services	Security Management	Audit Trail Capture and Analysis

13.1.3.2 Relationship to Technology Component Model

Table 24

Service Area	Service Category	Service Standard	Relation to SRM of FEA
			<p>The Space Shuttle Program Cockpit Avionics Upgrade will support implementation of a new Orbiter avionics hardware and software to meet the man-machine interface requirements. The Space Shuttle Program Cockpit Avionics Upgrade is providing a mission specific delivery of service that is very specialized and is difficult to leverage outside Space Transportation. The TRM does not really lend itself to a complete, detailed analysis of the Space Shuttle Program Cockpit Avionics Upgrade application. A very small portion (< 2%) of the flight software CAU project functions providing support to project managers, engineers, and support personnel can be mapped into the TRM. The Service Area, Service Category, Service Standard, and Service Specification that describe the technology supporting the Space Shuttle Cockpit Avionics Upgrade is listed below.* Service Access and Delivery (Core Service Area) - Access Channels (Service) - Web Browser (Standard) - Internet Explorer and Netscape Communicator (Specification)* Service Access and Delivery (Core Service Area) - Access Channels (Service) - Wireless / PDA (Standard) - Palm Pilot, Blackberry</p>

(Specification)* Service Access and Delivery (Core Service Area) - Access Channels (Service) - Collaboration Communications (Standard) - Electronic Mail, Fax, Kiosk (Specification)* Service Access and Delivery (Core Service Area) - Access Channels (Service) - Other Electronic Channels (Standard) - System to System, Web Service, URL (Specification)* Service Access and Delivery (Core Service Area) - Delivery Channels (Service) - Internet, Intranet, Extranet, VPN (Standard)* Service Access and Delivery (Core Service Area) - Service Requirements (Service) - Legislative / Compliance (Standard) - Section 508, Web Content Accessibility, Security, Privacy (Specification)* Service Access and Delivery (Core Service Area) - Service Requirements (Service) - Authentication / Single Sign-on (Standard)* Service Access and Delivery (Core Service Area) - Service Requirements (Service) - Hosting (Standard) - Internal (within Agency), External (ISP/ASP/FirstGov) (Specification)* Service Access and Delivery (Core Service Area) - Service Transport (Service) - Supporting Network Services (Standard) - IMAP / POP3, MIME, SMTP, ESMT, T.120, LDAP, Directory Services (Specification)* Service Access and Delivery (Core Service Area) - Service Transport (Service) - Service Transport (Standard) - TCP, IP, HTTP, HTTPS, WAP, FTP (Specification)* Service Platform and Infrastructure (Core Service Area) - Support Platforms (Service) - Platform Independent (J2EE) (Standard) - Java 2 Enterprise Edition (Specification)* Service Platform and Infrastructure (Core Service Area) - Support Platforms (Service) - Platform Dependent (MS) (Standard) - Windows 2000(Specification)* Service Platform and Infrastructure (Core Service Area) - Delivery Servers (Service) - Application Servers (Standard)* Service Platform and Infrastructure (Core Service Area) - Delivery Servers (Service) - Portal Servers (Standard)* Service Platform and Infrastructure (Core Service Area) - Delivery Servers (Service) - Media Servers (Standard) - Real Audio, Windows Media Services (Specification)* Service Platform and Infrastructure (Core Service Area) - Software Engineering (Service) - Integrated Development Environment (Standard) - IBM WebSphere Studio, Visual Studio, Visual Studio .NET (Specification)

13.1.3.3 Partnerships

None.

13.1.4 Security and Privacy

13.1.4.1 How is it provided and funded?

The Space Shuttle Program Systems Engineering and Integration Office in conjunction with the Johnson Space Center 's Mission Operations Directorate and Engineering Directorate provide security and funding associated with this project. The Johnson Space Center IT Security provides some aspects of security via center network and firewall for some parts of this project. United Space Alliance corporate IT Security networks, firewalls, etc. also provide security for aspects of this investment.

13.1.4.2 How is security accomplished?

The investment meets the security requirements by following NASA policy and guidance documents NPD and NPG 2810, adhering to updates from NIST guidelines and incorporating OMB polices as issued. The Product Development Plan for Information Technology Security (USA003018) is the overarching IT Security Plan. Per that plan, facility level plans are created and maintained (FSW/PASS Security Plan (USA007141, dated: 03/31/2003) and Software Production Facility (SPF) Security Plan (USA008008, dated: 10/31/2003)). These plans are in compliance with NPG 1620.1, NASA Security Procedures and Guidelines.

The Product Development Plan for Information Technology Security (USA003018) is the overarching IT Security Plan. Per that plan, facility level plans are created and maintained (FSW/PASS Security Plan (SFOC-FL2210) and Software Production Facility (SPF) Security Plan (SFOC-FL036)). These plans are in compliance with NPG 1620.1, NASA Security Procedures and Guidelines.

Certification and accreditation is achieved through accreditation of supporting facilities. Flight Software has been approved by a C&A process described in the USA FPPs D-03-01, IT Security Accreditation, D-03-08, IT Security Evaluation Process. This process meets the Office of Management and Budget (OMB) requirements for government facility IT accreditation.

The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures, when NIST completes this process NASA will revisit its policy and procedures to conform to NIST new guidance.

Processes have been established for the user role in incident handling. Annual security training ensures that users can recognize a security incident and respond properly. A priority list of contacts is established for communicating the incident and soliciting further response action. IT Security personnel review all incidents. Those with outside applicability are coordinated through established JSC incident response processes. Mission Control Center (MCC) IT Security personnel conduct intrusion detection monitoring. The MCC IT Security personnel respond to alerts issued by the Center for vulnerabilities that are discovered in relevant security software or implementations. JSC administrators coordinate with external agencies regarding security incidents. Security relevant logs generated in the MCC are reviewed at least monthly except where it can reasonably be accomplished and risk acceptance acknowledged. More frequent reviews are routinely done with narrower focus as interests dictate. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. Contractors operate the system both on-site and off-site. NPG 1620.1, NASA Security Procedures and Guidelines, and NPG 2810 Security of Information Technology are levied as requirements on the contractor. The Product Development Plan for Information Technology Security (USA003018) is a contractor deliverable to NASA. The contractor provides monthly incident reports to the NASA monitor. Those reports are reviewed by the organizational security manager for each functional area.

13.1.4.3 *Effective use of security, controls and authentication tools*

Not applicable, no public access is provided to the JSC Space Shuttle Program Cockpit Avionics Upgrade which is within the Space Shuttle Program.

13.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. The JSC Space Shuttle Program Cockpit Avionics Upgrade program does not include transactions or record keeping that is covered by GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

14 Johnson Space Center (JSC) – Space Shuttle Program Flight Software

Project Description

The Space Shuttle program plays a vital role in enabling NASA's vision and mission. This includes advancing human exploration and providing safe access to space in support of human operations in low-earth orbit. In order to maintain a viable human transportation capability that will operate and support NASA's launch requirements, specific program investments are required. NASA is revamping its approach to selecting and managing these investments to

ensure Shuttle operability into the next decade and avoid future project overruns. These investments will be consistent with NASA's strategy of ensuring the Space Shuttle remains viable until a new transportation system is operational. These projects will provide revitalization of the infrastructure, and combat obsolescence of vehicle, ground systems, and facilities.

The Flight Software Element (FSW) is responsible for the maintenance, testing, reconfiguration and configuration management of the Onboard Shuttle Software. Execution of these responsibilities is accomplished by several teams within FSW: the Shuttle Avionics Integration Lab (SAIL), the Primary Avionics Software System (PASS), the Backup Flight System (BFS), the Multifunction Electronic Display System (MEDS), the secure client/server computing environment (ASDEP), and Cockpit Avionics Upgrade (CAU). All IT resources identified for FSW are dedicated to these responsibilities. The JSC Space Shuttle Program Flight Software Investment is in the Operations phase of NASA Information Technology (IT) Capital Planning and Investment Control (CPIC) process, and this IT investment is managed as a component of the NASA project under NASA's NPG 7120 process.

The FY04 information technology annual review/approval (Capital Planning and Investment Control process) for this investment was held September 26, 2003.

The Flight Software (FSW) Information Technology (IT) plan is a part of the Space Flight Operations Contract (SFOC) overall annual Level A (5 year) and Level B (annual Fiscal Year) Information Technology Plan deliverables to the Space Shuttle Program (SSP) Chief Information Officer (CIO). FY04 Plans reviewed and approved in September 2004 by the SSP CIO with concurrence from the Johnson Space Center (JSC) CIO, Kennedy Space Center CIO and Marshall Space Flight Center CIO. The FSW portion of the SFOC IT Plan focused on the essential needs to maintain the resources necessary to continue to provide the unique IT support required by the FSW organization. The organization and their supporting contractors have a requirement to develop, verify and maintain Shuttle Flight Software in a JSC designated "critical" "mission" client server environment using TCP/IP protocols, in support of the SFOC contract. A secure LAN infrastructure and development environment is required to support this requirement. The ASDEP and FSW/PASS systems are designed to provide the secure client/server environments. FSW has its own firewalls setup which was necessary to gain NASA security approval to use client/server technology to access NASA mainframes.

The Flight Software (FSW) investment is in its operational phase of the NASA Information Capital Planning and Investment Control process. The FSW is a system that is responsible for the development, verification, and implementation of the onboard Space Shuttle software. Major responsibilities of the FSW Element include the Primary Avionics Flight Software System (PASS), the Backup Flight Software (BFS), the Multifunctional Electronic Display System (MEDS), the Shuttle Avionics Integration Laboratory (SAIL), the secure client/server computing environment (ASDEP), and the Cockpit Avionics Upgrade (CAU). Currently, the FSW is supporting the Operational Increments (OI's)-28, -29, and -30. OI-41, which provides the CAU with safety enhancements, is scheduled for release in August 2004. OI-42, also a CAU release, is currently under development and scheduled for release in 2006. Both OI's will support safety, reliability, and affordability.

FSW supports NASA's Space Flight capabilities by releasing software upgrades that have enhanced Space Shuttle safety and improved system reliability and performance during Space Shuttle flights. OI-41/42 will provide safety and reliability enhancements for the Cockpit Avionics Upgrade. FSW has released software upgrades that have contributed to an increased availability of the Shuttle to perform on-orbit experimentation as well as having increased mission duration to support Space Station research. For example, FSW is currently upgrading to support an ISS-SSP (Space Station-Shuttle) power converter that will increase SSP mission duration at the ISS in support of Contingency Shuttle Crew Support.

Project Management tools and processes have been implemented to control and identify cost-saving opportunities.

Architecture

14.1.1 Business

14.1.1.1 Process simplification/reengineering/design projects

None currently identified. The Project is currently in the mission operations phase. Organizational simplification/reengineering/design projects have been accomplished throughout the project's life cycle.

14.1.1.2 Major organization restructuring, training and change management projects

None currently identified. The Project is currently in the mission operations phase. Organizational restructuring, training, and change management have been accomplished throughout the project's life cycle.

14.1.2 Data

14.1.2.1 Types of Data

Science Engineering and Research (SER) -- Flight data generated for and during the flights of the Space Shuttle missions.

14.1.2.2 Existing Data Access

14.1.3 Application and Technology

14.1.3.1 Relationship to Service Component Model

Table 25

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Business Management Services	Management Process	of Change Management		
Business Management Services	Management Process	of Configuration Management		
Business Management Services	Management Process	of Requirements Management		
Business Management Services	Management Process	of Quality Management		
Business Management Services	Management Process	of Risk Management		
Digital Services	Asset	Document Management	Document Imaging and OCR	
Digital Services	Asset	Document Management	Document Referencing	
Digital Services	Asset	Document Management	Document Revisions	
Digital Services	Asset	Document Management	Library / Storage	
Digital Services	Asset	Document Management	Document Review and Approval	
Digital Services	Asset	Document Management	Document Conversion	
Digital Services	Asset	Document Management	Indexing	
Digital	Asset	Document	Classification	

Services	Management		
Back Services	Office	Data Management	Data Exchange
Back Services	Office	Data Management	Data Mart
Back Services	Office	Data Management	Data Warehouse
Back Services	Office	Data Management	Meta Data Management
Back Services	Office	Data Management	Data Cleansing
Back Services	Office	Data Management	Extraction and Transformation
Back Services	Office	Data Management	Loading and Archiving
Back Services	Office	Data Management	Data Recovery
Back Services	Office	Data Management	Data Classification
Back Services	Office	Assets Materials Management	/ Facilities Management
Back Services	Office	Assets Materials Management	/ Computers Automation Management
Back Services	Office	Development and Integration	Legacy Integration
Back Services	Office	Development and Integration	Data Integration
Back Services	Office	Development and Integration	Instrumentation and Testing
Back Services	Office	Development and Integration	Software Development
Support Services		Security Management	Identification and Authentication
Support Services		Security Management	Access Control

Support Services	Security Management	Intrusion Detection
Support Services	Security Management	Verification
Support Services	Security Management	User Management
Support Services	Security Management	Role / Privilege Management
Support Services	Security Management	Audit Trail Capture and Analysis
Support Services	Systems Management	License Management
Support Services	Systems Management	Remote Systems Control
Support Services	Systems Management	Systems Resource Monitoring
Support Services	Systems Management	Software Distribution

14.1.3.2 Relationship to Technology Component Model

Table 26

Service Area			Service Category	Service Standard	Relation to SRM of FEA
Service Delivery	Access	and	Access Channels	Web Browser	
Service Delivery	Access	and	Access Channels		
Service Delivery	Access	and			
Service Delivery	Access	and			
Service Delivery	Access	and			
Service Delivery	Access	and			

Service Access and Delivery

Service Access and Delivery

Service Access and Delivery

Service Access and Delivery

14.1.3.3 Partnerships

None.

14.1.4 Security and Privacy

14.1.4.1 How is it provided and funded?

The Space Shuttle Program provides all funding for security of the JSC Space Shuttle Program Flight Software.

This project utilizes the security protocols and infrastructure set up to insure the integrity of the Onboard Shuttle Software. Access is limited to authorized personnel having a need to access the software and is enforced utilizing multiple firewalls, secured workstations and Smart card authentication. The software itself is kept in tight configuration control. All controls are commensurate with the required data classification.

14.1.4.2 How is security accomplished?

The investment meets the security requirements by following NASA policy and guidance documents NASA Program Direction and NASA Procedures and Guidelines 2810, adhering to updates from National Institute of Standards and Testing guidelines and incorporating OMB polices as issued.

The following systems in the JSC Space Shuttle Program Flight Software program have up to date security plans as of :

- Software Production Facility (SPF) – 10/31/03
- Software Engineering Network (SWEN) – 3/31/04
- Flight Software Primary Avionics Software Sys (FSW/PASS) - 3/31/03
- Avionics Software Development Environment Pathfinder (ASDEP) – 2/29/04
- Shuttle Avionics Integration Lab (SAIL) – 9/30/03

The Project complies with the NASA Procedures and Guidelines (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures, when NIST completes this process NASA will revisit its policy and procedures to conform to NIST new guidance. Each of the above systems was last reviewed and received certification and accreditation as of the stated security plan approval dates.

Avionics Software Development Environment Pathfinder (ASDEP) and FSW/PASS systems have appropriate logging enabled, firewalls have "alert" intrusion detection enabled. Reviews are done by FSW/PASS security on a daily basis and incidents are reported to United Space Alliance (USA) ITS security, where applicable. Shuttle Avionics Integration Laboratory (SAIL) is in a secured location on NASA JSC premises. Access is controlled, monitored, and incidents handled by NASA JSC security. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. The Flight Software element is operated by contractors both onsite and at the contractor facility. Specific security requirements are documented in the Product Development Plan (PDP) for IT Security for the SFOC contract. The monitoring procedures, reportable metrics, etc. are agreed to and monitored through the standard PDP review process. The contractor provides monthly incident reports that are reviewed by the appropriate functional organizational security manager.

14.1.4.3 *Effective use of security, controls and authentication tools*

Not applicable, the JSC Space Shuttle Program Flight Software does not allow public access. Security control is via user assigned accounts and userids. Currently using authentication control software by Safeword and Blockade.

14.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. Not applicable, the JSC Space Shuttle Program Flight Software does not support GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

15 Johnson Space Center (JSC) – Space Shuttle Program / Program Integration

Project Description

The Space Shuttle program plays a vital role in enabling NASA's vision and mission. This includes advancing human exploration and providing safe access to space in support of human operations in low-earth orbit. In order to maintain a viable human transportation capability that will operate and support NASA's launch requirements. NASA is revamping its approach to selecting and managing these investments to ensure Shuttle operability into the next decade and avoid future project overruns. These investments will be consistent with NASA's strategy of ensuring the Space Shuttle remains viable until a new transportation system is operational. These projects will provide revitalization of the infrastructure, and combat obsolescence of vehicle, ground systems, and facilities.

Space Shuttle Program Program Integration (SSP PI) includes elements managed by the Space Shuttle Program Office at the Johnson Space Center (JSC) and conducted primarily by United Space Alliance, including payload integration into the Space Shuttle, systems integration of the flight hardware elements through all phases of flight, and configuration management of program hardware, software, and requirements.

The information technology parts of SSP PI include such applications as Baseline Accounting and Reporting System, Mission Requirements control System, Automated Scheduling and Planning, Automated Mission & Payload Tracking System, Shuttle Drawing System, Program Compliance Assurance and Status System, Shuttle Integration Accounting Status System, Verification Information System, Work Authorizing Documentation System, Waivers/Exceptions, Operations and Maintenance Requirements and Specifications Change Processing, Document Configuration Management System, Technical Document Management System 2, Shuttle Payload Integration and Cargo Evaluation System, Critical Math Model Database, Launch Management System. The major expenses are either sustaining or migrating mainframe projects to a web-based, client-server environment. This also includes the cost allocations for the office automation services supporting the employees of this function. The FY04 information technology annual review/approval (Capital Planning and Investment Control process) for this investment was held September 26, 2003.

The SSP Program Integration (PI) Information Technology (IT) plan is a part of the Space Flight Operations Contract (SFOC) overall annual Level A (5 year) and Level B (annual Fiscal Year) Information Technology Plan deliverables to the Space Shuttle Program (SSP) Chief Information Officer (CIO). FY04 Plans reviewed and approved in September 2004 by the SSP CIO with concurrence from the Johnson Space Center (JSC) CIO, Kennedy Space Center CIO and Marshall Space Flight Center CIO. The major IT expenses deal with either sustaining the above systems or migrating mainframe projects to a web-based, client-server environment using state of the art technology for data access, availability and transfer.

Architecture

15.1.1 Business

15.1.1.1 *Process simplification/reengineering/design projects*

The Project is currently in the mission operations phase. Organizational simplification/reengineering/design projects have been accomplished throughout the project's life cycle. Migration from mainframe-based to web/client-server based applications are evaluated and implemented as business cases are viewed and approved in the annual budget review processes and in joint weekly and quarterly NASA technical management representative and contractor management meetings.

15.1.1.2 *Major organization restructuring, training and change management projects*

The Project is currently in the mission operations phase. Organizational restructuring, training, and change management have been accomplished throughout the project's life cycle.

15.1.2 Data

15.1.2.1 *Types of Data*

SER (Science, Engineering and Research)

The data is unique internal SSP schedule, engineering, and configuration management data. Official data is approved and documented via formal control board processes.

15.1.2.2 *Existing Data Access*

15.1.3 Application and Technology

15.1.3.1 *Relationship to Service Component Model*

Table 27

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Business Management Services	Management of Process	Change Management		The Space Shuttle Program Program Integration provides support through the following functions: Payload/Cargo Engineering, System Integration, Management Integration,

Technical Information Systems, and ISS Program Integration.

The Space Shuttle Program Program Integration is providing a mission specific delivery of service that is very specialized and is difficult to leverage outside Space Transportation. The SRM does not really lend itself to a complete, detailed analysis of the Space Shuttle Program Program Integration

application. Space Shuttle Program Program Integration functions map into the SRM into the following Key Service

Domain/Service Type/Components: Listing for SRM Service

Domain/Service Type/Components

*** Business**

Management Services (Domain) - Management of Process (Type) - Change

Management, Configuration Management, Requirements Management, Quality

Management, and Risk Management (Components)

*** Digital Asset Services (Domain) - Document Management (Type) - Document Imaging and OCR, Document Referencing, Document Revisions, Library / Storage, Document Review and Approval, Document Conversion, Indexing, and Classification (Components)**

*** Back Office Services (Domain) - Data Management (Type) - Data Exchange, Data Mart, Data Warehouse, Meta Data Management, Data Cleansing, Extraction and Transformation, Loading and Archiving, Data Recovery, and Data Classification (Components)**

*** Back Office Services (Domain) - Assets / Materials Management (Type) -Facilities Management, and Computers / Automation Management (Components)**

*** Back Office Services (Domain) - Development and Integration (Type) - Legacy Integration, Data Integration, Instrumentation and**

Testing, and Software Development (Components)
 * Support Services (Domain) - Security Management (Type)
 - Identification and Authentication, Access Control, Intrusion Detection, Verification, User Management, Role / Privilege Management, and Audit Trail Capture and Analysis (Components)
 * Support Services (Domain) - Communication (Type) - Audio Conferencing and Video Conferencing (Components)
 * Support Services (Domain) - Systems Management (Type)
 - License Management, Remote Systems Control, System Resource Monitoring, and Software Distribution (Components)

Business Management Services **Management of Process** **Configuration Management**

Business Management Services **Management of Process** **Requirements Management**

Business Management Services **Management of Process** **Quality Management**

Business Management **Management of** **Risk**

Services	Process	Management
Business Management Services	Management of Process	Change Management
Digital Asset Services	Document Management	Document Imaging and OCR
Digital Asset Services	Document Management	Document Referencing
Digital Asset Services	Document Management	Document Revisions
Digital Asset Services	Document Management	Library / Storage
Digital Asset Services	Document Management	Document Review and Approval
Digital Asset Services	Document Management	Document Conversion
Digital Asset Services	Document Management	Indexing
Digital Asset Services	Document Management	Classification
Back Office Services	Assets / Materials Management	Facilities Management
Back Office Services	Assets / Materials Management	Computers / Automation Management
Back Office Services	Development and Integration	Legacy Integration
Back Office Services	Development and Integration	Data Integration
Back Office Services	Development and Integration	Instrumentation and Testing
Back Office Services	Development and Integration	Software Development
Support Services	Security Management	Identification and

		Authentication
Support Services	Security Management	Access Control
Support Services	Security Management	Intrusion Detection
Support Services	Security Management	Verification
Support Services	Security Management	User Management
Support Services	Security Management	Role / Privilege Management
Support Services	Security Management	Audit Trail Capture and Analysis
Support Services	Communication	Audio Conferencing
Support Services	Communication	Video Conferencing
Support Services	Systems Management	License Management
Support Services	Systems Management	Remote Systems Control
Support Services	Systems Management	Systems Resource Monitoring
Support Services	Systems Management	Software Distribution

15.1.3.2 Relationship to Technology Component Model

Table 28

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access and Delivery	Access Channels	Web Browser	The Service Area, Service Category, Service Standard, and Service Specification that describe the technology

supporting the Space Shuttle Program - Program Integration is listed below.

* Service Access and Delivery (Core Service Area) - Access Channels (Service) - Web Browser (Standard) - Internet Explorer and Netscape Communicator (Specification)

* Service Access and Delivery (Core Service Area) - Access Channels (Service) - Wireless / PDA (Standard) - Palm Pilot, Blackberry (Specification)

* Service Access and Delivery (Core Service Area) - Access Channels (Service) - Collaboration Communications (Standard) - Electronic Mail, Fax, Kiosk (Specification)

* Service Access and Delivery (Core Service Area) - Access Channels (Service) - Other Electronic Channels (Standard) - System to System, Web Service, URL (Specification)

* Service Access and Delivery (Core Service Area) - Delivery Channels (Service) - Internet, Intranet, Extranet, VPN (Standard)

* Service Access and Delivery (Core Service Area) - Service Requirements (Service) - Legislative / Compliance (Standard) - Section 508, Web Content Accessibility, Security, Privacy (Specification)

* Service Access and Delivery (Core Service Area) - Service Requirements (Service) - Authentication / Single Sign-on (Standard)

* Service Access and Delivery (Core Service Area) - Service Requirements (Service) - Hosting (Standard) - Internal (within Agency), External (ISP/ASP/FirstGov) (Specification)

* Service Access and Delivery

(Core Service Area) - Service Transport (Service) - Supporting Network Services (Standard) - IMAP / POP3, MIME, SMTP, ESMTP, T.120, LDAP, Directory Services (Specification)

*** Service Access and Delivery (Core Service Area) - Service Transport (Service) - Service Transport (Standard) - TCP, IP, HTTP, HTTPS, WAP, FTP (Specification)**

*** Service Platform and Infrastructure (Core Service Area) - Support Platforms (Service) - Platform Independent (J2EE) (Standard) - Java 2 Enterprise Edition (Specification)**

*** Service Platform and Infrastructure (Core Service Area) - Support Platforms (Service) - Platform Dependent (MS) (Standard) - Windows 2000(Specification)**

*** Service Platform and Infrastructure (Core Service Area) - Delivery Servers (Service) - Application Servers (Standard)**

*** Service Platform and Infrastructure (Core Service Area) - Delivery Servers (Service) - Portal Servers (Standard)**

*** Service Platform and Infrastructure (Core Service Area) - Delivery Servers (Service) - Media Servers (Standard) - Real Audio, Windows Media Services (Specification)**

*** Service Platform and Infrastructure (Core Service Area) - Software Engineering (Service) - Integrated Development Environment (Standard) - IBM WebSphere Studio, Visual Studio, Visual Studio .NET (Specification)**

*** Service Platform and Infrastructure (Core Service Area) - Software Engineering (Service) - Software Configuration**

Management (Standard) -
 Version Management, Defect
 Tracking, Issue Management,
 Task Management, Change
 Management, Deployments
 Management, Requirements
 Management (Specification)

Service Access Delivery	and Access Channels	Web Browser
Service Access Delivery	and Access Channels	Wireless / PDA
Service Access Delivery	and Access Channels	Wireless / PDA
Service Access Delivery	and Access Channels	Collaboration Communication
Service Access Delivery	and Access Channels	Collaboration Communication
Service Access Delivery	and Access Channels	Collaboration Communication
Service Access Delivery	and Access Channels	Other Electronic Channels
Service Access Delivery	and Access Channels	Other Electronic Channels
Service Access Delivery	and Access Channels	Other Electronic Channels
Service Access Delivery	and Delivery Channels	Internet
Service Access Delivery	and Delivery Channels	Intranet
Service	Delivery	Extranet

Access Delivery	and	Channels	
Service Access Delivery	and	Delivery Channels	Virtual Private Network (VPN)
Service Access Delivery	and	Service Requirements	Legislative Compliance /
Service Access Delivery	and	Service Requirements	Legislative Compliance /
Service Access Delivery	and	Service Requirements	Legislative Compliance /
Service Access Delivery	and	Service Requirements	Legislative Compliance /
Service Access Delivery	and	Service Requirements	Authentication / Single Sign-on (SSO)
Service Access Delivery	and	Service Requirements	Hosting
Service Access Delivery	and	Service Requirements	Hosting
Service Access Delivery	and	Service Transport	Supporting Network Services
Service Access Delivery	and	Service Transport	Supporting Network Services
Service Access Delivery	and	Service Transport	Supporting Network Services
Service Access Delivery	and	Service Transport	Supporting Network Services
Service Access Delivery	and	Service Transport	Supporting Network

Delivery		Services
Service Access and Delivery	Service and Transport	Supporting Network Services
Service Access and Delivery	Service and Transport	Supporting Network Services
Service Access and Delivery	Service and Transport	Service Transport
Service Access and Delivery	Service and Transport	Service Transport
Service Access and Delivery	Service and Transport	Service Transport
Service Access and Delivery	Service and Transport	Service Transport
Service Access and Delivery	Service and Transport	Service Transport
Service Access and Delivery	Service and Transport	Service Transport
Service Platform and Infrastructure	Supporting Platforms	Platform Independent
Service Platform and Infrastructure	Supporting Platforms	Platform Dependent
Service Platform and Infrastructure	Delivery Servers	Application Servers
Service Platform and Infrastructure	Delivery Servers	Portal Servers
Service Platform and Infrastructure	Delivery Servers	Media Servers

Service Platform and Infrastructure	Delivery Servers	Media Servers
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Software Configuration Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and	Software	Test

Infrastructure	Engineering	Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Software Engineering	Test Management

15.1.3.3 Partnerships

None.

15.1.4 Security and Privacy

15.1.4.1 How is it provided and funded?

Program Integration (PI) Information Technology Security (ITS) support is provided by United Space Alliance (USA) ITS, Boeing ITS and NASA. Each major system is documented in a Product Development Plan (PDP) with NASA. USA maintains Security Plans for each group of applications. PI allocates funding for USA ITS via the PC pool; Boeing ITS is also funded by allocations from Programs. NASA ADP Consolidated Center (NACC) funding is funded directly by the SSP NASA Management Integration Office (MIO).

15.1.4.2 *How is security accomplished?*

The investment meets the security requirements by following NASA policy and guidance documents NASA Program Direction (NPD) and NASA Procedures and Guidelines 2810, adhering to updates from National Institute of Standards and Testing guidelines and incorporating OMB polices as issued.

The Project complies with the NASA Procedures and Guidelines (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures, when NIST completes this process NASA will revisit it's policy and procedures to conform with NIST new guidance.

Program Integration Support Applications (PISA)

Plan #: SPMA0016

Last ATP: March 2004

System: Program Integration-NASA ADP Consolidation Center (PI-NACC)

Plan #: SPMA0005

Last ATP: May 2004

System: Shuttle Drawing System

Plan #: SPMA0007

Last ATP: November 2003

System: Regents Park III Office Automation System

Plan #: SPMA0011

Last ATP: March 03

Processes have been established for the user role in incident handling. Annual security training ensures that users can recognize a security incident and respond properly. A priority list of contacts is established for communicating the incident and soliciting further response action. IT Security personnel review all incidents. Those with outside applicability are coordinated through established JSC incident response processes. Mission Control Center (MCC) IT Security personnel conduct intrusion detection monitoring. The MCC IT Security personnel respond to alerts issued by the Center for vulnerabilities that are discovered in relevant security software or implementations. JSC administrators coordinate with external agencies regarding security incidents. Security relevant logs generated in the MCC are reviewed at least monthly except where it can reasonably be accomplished and risk acceptance acknowledged. More frequent reviews are routinely done with narrower focus as interests dictate. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. United Space Alliance (USA) operates systems both on and off-site in support of NASA Programs. USA IT Security provides copies of all system security plans to NASA. USA IT Security provides system security posture presentations (obtained from the results of system IT security risk assessments) to the NASA Space Shuttle Program (SSP)

Management Integration Office (MIO) Manager at JSC in order to obtain NASA 's Authorization to Process (ATP) concurrence for each system. The contractor provides monthly incident reports that are reviewed by the appropriate functional organizational security manager.

15.1.4.3 *Effective use of security, controls and authentication tools*

Not applicable, this investment does not allow public access.

15.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA.

16 Johnson Space Center (JSC) – Space Station Production Facility

Project Description

This facility, separated into Development, Integration, and Production environments, provides tools for engineering analysis for International Space Station Program (ISSP) development and sustaining; for management of program manifests and on-orbit inventory, etc.; for access to and maintenance of critical Program data (including Station physical properties, drawings, etc.) required for NASA, Boeing and other Program Participants to meet their Program commitments. These tools are a combination of COTS and internally developed applications specifically to provide support to the ISSP.

The JSC Space Station Production Facility Investment is in the Operations phase of NASA IT Capital Planning & Investment Control (CPIC) process, and this IT investment is managed as a component of the NASA project under NASA's NPG 7120 process.

Architecture

16.1.1 Business

16.1.1.1 *Process simplification/reengineering/design projects*

Improvements will be made using existing system engineering and ISO 9000 processes. The Software Processes will be certified to Software Engineering Institute (SEI) Level 3 which is a continuing improvement process. The system has already successfully been augmented with enhanced capabilities. New commercial products have been added where stringent requirements can be achieved from Commercial Off the Shelf (COTS). New missions and services may require systems to change, which would be handled through the annual budget process.

16.1.1.2 Major organization restructuring, training and change management projects

Since the International Space Station (ISS) is a mature program that has been in place since 1993, the current organization and processes will continue to be utilized. The ISS Program continually examines where program management and organizational improvements can be made based on program goals, progress, and evolution.

16.1.2 Data

16.1.2.1 Types of Data

SER (Science, Engineering, and Research) -- Technical data regarding International Space Station (ISS) systems physical and functional properties, risk analysis and problem reporting information, data for use in management of the manifest information on-orbit.

16.1.2.2 Existing Data Access

16.1.3 Application and Technology

16.1.3.1 Relationship to Service Component Model

Table 29

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Business Management Services	Management of Process	Change Management		The ISS Production Facility supports the ISS software development, integration, and production environment and provides access to and maintains critical Program data. The ISS Production Facility is providing a mission specific delivery of service that is very specialized and is difficult to leverage

outside Space
 Transportation. The
 SRM does not really
 lend itself to a
 complete, detailed
 analysis of the ISS
 Production Facility
 application. ISS
 Production Facility
 functions map into the
 SRM into the following
 Key Service
 Domain/Service
 Type/Components:
 Listing for SRM Service
 Domain/Service
 Type/Components
 * Business
 Management Services
 (Domain) -
 Management of
 Process (Type) -
 Change Management,
 Configuration
 Management,
 Requirements
 Management, Quality
 Management, and Risk
 Management
 (Components)
 * Digital Asset Services
 (Domain) - Document
 Management (Type) -
 Document Imaging
 and OCR, Document
 Referencing,
 Document Revisions,
 Library / Storage,
 Document Review and
 Approval, Document
 Conversion, Indexing,
 and Classification
 (Components)
 * Back Office Services
 (Domain) - Data
 Management (Type) -
 Data Exchange, Data
 Mart, Data Warehouse,
 Meta Data

Management, Data
Cleansing, Extraction
and Transformation,
Loading and
Archiving, Data
Recovery, and Data
Classification
(Components)

* Back Office Services
(Domain) - Assets /
Materials Management
(Type) -Facilities
Management, and
Computers /
Automation
Management
(Components)

* Back Office Services
(Domain) -
Development and
Integration (Type) -
Legacy Integration,
Data Integration,
Instrumentation and
Testing, and Software
Development
(Components)

* Support Services
(Domain) - Security
Management (Type) -
Identification and
Authentication,
Access Control,
Encryption, Intrusion
Detection, Verification,
Digital Signature, User
Management, Role /
Privilege
Management, and
Audit Trail Capture and
Analysis (Components)

* Support Services
(Domain) - Systems
Management (Type) -
License Management,
Remote Systems
Control, System
Resource Monitoring,
and Software

**Distribution
(Components)**

Business Management Services	Management of Process	Configuration Management
Business Management Services	Management of Process	Requirements Management
Business Management Services	Management of Process	Quality Management
Business Management Services	Management of Process	Risk Management
Digital Asset Services	Document Management	Document Imaging and OCR
Digital Asset Services	Document Management	Document Referencing
Digital Asset Services	Document Management	Document Revisions
Digital Asset Services	Document Management	Library / Storage
Digital Asset Services	Document Management	Document Review and Approval
Digital Asset Services	Document Management	Document Conversion
Digital Asset Services	Document Management	Indexing
Digital Asset Services	Document Management	Classification
Back Office Services	Data Management	Data Exchange
Back Office Services	Data Management	Data Mart
Back Office Services	Data Management	Data Warehouse

Back Office Services	Data Management	Meta Data Management
Back Office Services	Data Management	Data Cleansing
Back Office Services	Data Management	Extraction and Transformation
Back Office Services	Data Management	Loading and Archiving
Back Office Services	Data Management	Data Recovery
Back Office Services	Data Management	Data Classification
Back Office Services	Assets / Materials Management	Facilities Management
Back Office Services	Assets / Materials Management	Computers / Automation Management
Back Office Services	Development and Integration	Facilities Management
Back Office Services	Development and Integration	Computers / Automation Management
Support Services	Security Management	Identification and Authentication
Support Services	Security Management	Access Control
Support Services	Security Management	Encryption
Support Services	Security Management	Intrusion Detection
Support Services	Security Management	Verification
Support Services	Security Management	Digital Signature
Support	Security	User

Services	Management	Management
Support Services	Security Management	Role Privilege Management /
Support Services	Security Management	Audit Trail Capture and Analysis
Support Services	Systems Management	License Management
Support Services	Systems Management	Remote Systems Control
Support Services	Systems Management	Systems Resource Monitoring
Support Services	Systems Management	Software Distribution

16.1.3.2 Relationship to Technology Component Model

Table 30

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access and Delivery	Access Channels	Web Browser	<p>The Service Area, Service Category, Service Standard, and Service Specification that describe the technology supporting the ISS Production Facility are listed below.</p> <p>* Service Access and Delivery (Core Service Area) - Access Channels (Service) - Web Browser (Standard) - Internet Explorer and Netscape Communicator (Specification)</p> <p>* Service Access and Delivery (Core Service Area) - Access Channels (Service) - Wireless / PDA (Standard) - Palm Pilot, Blackberry (Specification)</p> <p>* Service Access and Delivery (Core Service Area) - Access Channels (Service) -</p>

Collaboration Communications (Standard) - Electronic Mail, Fax, Kiosk (Specification)
*** Service Access and Delivery (Core Service Area) - Access Channels (Service) - Other Electronic Channels (Standard)**
- System to System, Web Service, URL (Specification)
*** Service Access and Delivery (Core Service Area) - Delivery Channels (Service) - Internet, Intranet, Extranet, VPN (Standard)**
*** Service Access and Delivery (Core Service Area) - Service Requirements (Service) - Legislative / Compliance (Standard) - Section 508, Web Content Accessibility, Security, Privacy (Specification)**
*** Service Access and Delivery (Core Service Area) - Service Requirements (Service) - Authentication / Single Sign-on (Standard)**
*** Service Access and Delivery (Core Service Area) - Service Requirements (Service) - Hosting (Standard) - Internal (within Agency), External (ISP/ASP/FirstGov) (Specification)**
*** Service Access and Delivery (Core Service Area) - Service Transport (Service) - Supporting Network Services (Standard) - IMAP / POP3, MIME, SMTP, ESMTP, T.120, LDAP, Directory Services (Specification)**
*** Service Access and Delivery (Core Service Area) - Service Transport (Service) - Service Transport (Standard) - TCP, IP, HTTP, HTTPS, WAP, FTP (Specification)**
*** Service Platform and Infrastructure (Core Service Area) - Support Platforms**

(Service) - Platform Independent (J2EE) (Standard) - Java 2 Enterprise Edition (Specification)
 * Service Platform and Infrastructure (Core Service Area) - Support Platforms (Service) - Platform Dependent (MS) (Standard) - Windows 2000(Specification)
 * Service Platform and Infrastructure (Core Service Area) - Delivery Servers (Service) - Application Servers (Standard)
 * Service Platform and Infrastructure (Core Service Area) - Delivery Servers (Service) - Portal Servers (Standard)
 * Service Platform and Infrastructure (Core Service Area) - Delivery Servers (Service) - Media Servers (Standard) - Real Audio, Windows Media Services (Specification)

Service Access and Delivery	Access Channels	Web Browser
Service Access and Delivery	Access Channels	Wireless / PDA
Service Access and Delivery	Access Channels	Wireless / PDA
Service Access and Delivery	Access Channels	Collaboration Communication
Service Access and Delivery	Access Channels	Collaboration Communication
Service Access and Delivery	Access Channels	Collaboration Communication

Service Access Delivery	and	Access Channels	Other Electronic Channels
Service Access Delivery	and	Access Channels	Other Electronic Channels
Service Access Delivery	and	Access Channels	Other Electronic Channels
Service Access Delivery	and	Delivery Channels	Internet
Service Access Delivery	and	Delivery Channels	Intranet
Service Access Delivery	and	Delivery Channels	Extranet
Service Access Delivery	and	Delivery Channels	Virtual Private Network (VPN)
Service Access Delivery	and	Service Requirements	Legislative Compliance /
Service Access Delivery	and	Service Requirements	Legislative Compliance /
Service Access Delivery	and	Service Requirements	Legislative Compliance /
Service Access Delivery	and	Service Requirements	Legislative Compliance /
Service Access Delivery	and	Service Requirements	Authentication / Single Sign-on (SSO)
Service Access Delivery	and	Service Requirements	Hosting
Service		Service	Supporting

Access Delivery	and	Transport	Network Services
Service Access Delivery	and	Service Transport	Supporting Network Services
Service Access Delivery	and	Service Transport	Supporting Network Services
Service Access Delivery	and	Service Transport	Supporting Network Services
Service Access Delivery	and	Service Transport	Supporting Network Services
Service Access Delivery	and	Service Transport	Supporting Network Services
Service Access Delivery	and	Service Transport	Supporting Network Services
Service Access Delivery	and	Service Transport	Service Transport
Service Access Delivery	and	Service Transport	Service Transport
Service Access Delivery	and	Service Transport	Service Transport
Service Access Delivery	and	Service Transport	Service Transport
Service Access Delivery	and	Service Transport	Service Transport
Service Platform	and	Supporting Platforms	Platform Independent

Infrastructure

Service Platform and Infrastructure	Supporting Platforms	Platform Dependent
Service Platform and Infrastructure	Delivery Servers	Application Servers
Service Platform and Infrastructure	Delivery Servers	Portal Servers
Service Platform and Infrastructure	Delivery Servers	Media Servers
Service Platform and Infrastructure	Delivery Servers	Media Servers
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Service Transport	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Service Transport	Software Configuration Management
Service Platform and Infrastructure	Service Transport	Software Configuration Management
Service Platform and Infrastructure	Service Transport	Software Configuration Management
Service Platform and Infrastructure	Service Transport	Software Configuration Management
Service Platform and Infrastructure	Service Transport	Software Configuration Management

Service Platform and Infrastructure	Service Transport	Software Configuration Management
Service Platform and Infrastructure	Service Transport	Software Configuration Management
Service Platform and Infrastructure	Service Transport	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Service Transport	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Service Transport	Integrated Development Environment (IDE)
Service Platform and Infrastructure	Service Transport	Test Management
Service Platform and Infrastructure	Service Transport	Test Management
Service Platform and Infrastructure	Service Transport	Test Management
Service Platform and Infrastructure	Service Transport	Test Management
Service Platform and Infrastructure	Service Transport	Test Management
Service Platform and Infrastructure	Service Transport	Test Management
Service Platform and Infrastructure	Service Transport	Test Management
Service Platform and Infrastructure	Service Transport	Test Management

16.1.3.3 Partnerships

None.

16.1.4 Security and Privacy

16.1.4.1 How is it provided and funded?

The security for the JSC Space Station Production Facility is funded by the International Space Station Program (ISSP).

A combination of security provided by the center IT security infrastructure (firewalls, intrusion detection, etc) and program procured and developed security systems and access control.

16.1.4.2 How is security accomplished?

The investment meets the security requirements by following NASA policy and guidance documents NPD and NPG 2810, adhering to updates from NIST guidelines and incorporating OMB polices as issued.

The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures. When NIST completes this process NASA will revisit its policy and procedures to conform to NIST new guidance, with certification and accreditation will be based on the NIST standards put out by the JSC I/T Security Office. All past certification and accreditation has been based on the JPG2810.1b requirements.

The incident handling and reporting capability is incorporated in the IPF and documented by its security plan. Intrusion monitoring and detection is handled by firewall servers protecting the IPF systems. Audit logs are produced and reviewed by the contractor and the Organizational Computer Security Manager on a weekly basis, if not every few days. All incidents are reported to DHS' Fed CIRC.

All contracts include specific security requirements required by law and policy. Program and center security personnel regularly review and validate procedures used by the contractor. This includes quarterly scans of all systems and annual review of all processes and procedures.

16.1.4.3 Effective use of security, controls and authentication tools

The investment is not available to the public.

16.1.5 Government Paperwork Elimination Act

The investment does not support electronic transactions or recordkeeping that is covered by GPEA

17 Johnson Space Center (JSC) – Space Station Training Facility

Project Description

Description.

The following paragraphs describe the "Line Of Sight" for this investment using the methodology prescribed in the Performance Reference Model, (version 1.0):

The overarching mission is for NASA to operate the International Space Station (ISS) for the benefit of the American public, (i.e. ISS theme of NASA goal #8). Benefits include discoveries through research on the ISS that are matured and infused into technologies resulting in products and services that improve the quality of life for the public. Another benefit is the experience gained on operating spacecraft in low Earth orbit. Knowledge acquired is integrated into the principles, policies, procedures, tools, and technologies supporting spacecraft operations. The benefits inherent in ISS operations are possible only by ensuring that the operators have the necessary knowledge and skills. The operators are the ISS crew and the flight controllers in the ground control centers. Assurance of prerequisite knowledge and skills prior to ISS mission operations is made possible by extensive training. ISS training is mandatory before and during flight.

This investment is the Space Station Training Facility (SSTF). It consists of a set of simulators that provide application services in support of ISS training needs. Each simulator is designed to focus on specific types of training. The primary customers are the instructors, crew, and flight controllers. Other customers include the Mission Control Center test team and ISS procedure developers. The ISS Program Manager is the key stakeholder.

The SSTF has three main simulators: Full Task Trainer (FTT), Part Task Trainer (PTT), and American Segment Trainer (AST). A detailed and hierarchal set of requirements defines the specific application services specified for the types of training provided by each of these simulators. The requirements are defined by the organization responsible for conducting the training. The customer for the requirements is the SSTF development organization.

Implementation of the requirements results in a cohesive set of hardware and software assets that deliver the application services to the customers. Custom built and Commercial Off The Shelf (COTS) products are integrated to yield the Information Technology (I/T) solution. The custom components consist of products produced by the SSTF development organization as well as products provided by the ISS Program via collaborative arrangements.

The objective of the I/T solution for the FTT is effective crew and flight controller team training. The crew and flight controllers interact via an infrastructure that supports data, audio, and video generation and distribution. The focus of their interaction involves data provided by high fidelity simulations of ISS systems integrated together yielding realistic cause and effect signatures. These simulations are the SSTF application services. Crew access to the simulations is via flight equivalent laptops and display and control panels located in mockups of the ISS modules. Flight controllers access the simulations via their actual flight support console in the ground control center. The type of training provided by the FTT includes ISS assembly, routine operations, payload operations, and multi-segment emergency scenarios. The FTT also supports procedure verification and testing of the Mission Control Center (MCC) at Johnson Space Center (JSC).

The objective of the I/T solution for the PTT is transference of knowledge on individual ISS systems. PTT provides ISS crew and flight controller proficiency training geared toward individual ISS systems. The PTT infrastructure is narrower than the FTT consisting of a student station, instructor station, and simulation computer.

The AST is functionally based on the PTT, however it has unique requirements for supporting training at International Partner locations. NASA provides AST platforms to the Russian Space Agency (RSA), Japanese Aerospace Exploration Agency (JAXA), and the European Space Agency (ESA).

The primary SSTF deliverables are called training loads. They consist of software and data integrated together to provide the simulated signatures representing the behavior of the ISS. These signatures are sent to appropriate hardware assets that provide the student (i.e. user) with a realistic interface to respond to the simulated behavior. Instructors manipulate the simulation by inserting simulated malfunctions of ISS systems thereby creating scenarios for the crew and flight controllers to operationally manage. Instructors evaluate student responses and provide feedback to enhance the student's operational knowledge and skills. Instructor assessment is also used to establish compliance with certification criteria for the ISS operations personnel. In addition to evaluating the students, the Instructors also evaluate each training session with respect to how well the simulator met the training objectives for that session. This is a direct measure of the performance of the SSTF I/T solution relative to programmatic objectives.

The FTT has a significantly larger I/T footprint than the PTT or AST due to the larger set of requirements inherent in its purpose. Specifically, team oriented training introduces requirements for external network interfaces to other trainers and ground control centers. In addition, the FTT is required to support much higher fidelity training on the ISS avionics systems than the PTT or AST. The FTT is built to process the real ISS flight software, whereas the PTT and AST provide functional simulations of the ISS flight software. These differences result in notably higher I/T costs for the FTT than the PTT or AST. The steady state processes and management of the FTT are therefore correspondingly more complicated than those of the PTT and AST.

SSTF is managed in accordance with Johnson Space Center (JSC) Policy Directive (JPD) 7120.1 using processes tailored from NASA Procedures and Guidelines (NPG) 7120.5. Formal

management processes are in place to address baseline control, change assessment, Trouble Reports, risks, I/T administration, process improvement, and status reporting.
SSTF Contract Transition:

The SSTF has two overall lifecycle phases: Development and Operations. The Development lifecycle phase is implemented under the Training Systems Contract (TSC), NAS9-18191. The Operations phase is supported under the Space Flight Operations Contract (SFOC), NAS9-20000.

The methodology for transitioning the SSTF from development to operations (i.e. TSC to SFOC) consists of a preparatory phase, classroom training phase, and two On-The-Job Training (OJT) phases. The first OJT phase is when TSC personnel lead an applicable I/T task with SFOC personnel monitoring and supporting to the degree possible. The roles swap in the second OJT phase so that SFOC personnel are primary with limited ("help desk") support from TSC personnel. The length of the preparatory and classroom training activities are a function of the specific area being transitioned. Each OJT phase is planned to take three months. Handover of responsibility from TSC to SFOC for a given task is planned to occur after successful completion of the first OJT phase. The objective of these transition activities is to ensure transference of skills from TSC to SFOC personnel so that steady state operations can be maintained during the operational lifecycle phase under SFOC. Consequently, effort on these transition activities is assigned to the Steady State (SS) category in the NASA Capital Planning and Investment Control (CPIC) process.

A detailed responsibility matrix identifies the items of responsibility to be transferred from TSC to SFOC. Each item of responsibility has a set of criteria that specifies prerequisites that must be accomplished before responsibility handover can be authorized. A detailed schedule provides the phasing of the transition activities for each area within the SSTF. A management structure consisting of a Control Board and several working groups was established to manage the transition effort. Transition Readiness Reviews are conducted to assess compliance of each responsibility handover prerequisite prior to authorizing the handover.

Status:

The development phase of the SSTF lifecycle is currently in the final stages of completion. Remaining TSC deliverables consist of training loads that support Shuttle Return To Flight (RTF), primary functionality for subsequent ISS flights, and residual platform enhancements.

There are three remaining RTF deliverables under TSC. One is generic in nature and the other two are specific to the next two flights to the ISS. These deliverables will be used for ISS training upon delivery. Development of these loads is in the Development/Modernization/Enhancement (DME) category of the NASA Capital Planning and Investment Control (CPIC) process. The operations effort to support ISS training with these deliverables is in the Steady State (SS) category of the CPIC process.

Status:

The development phase of the SSTF lifecycle is currently in the final stages of completion. Remaining TSC deliverables consist of training loads that support Shuttle Return To Flight

(RTF), primary functionality for subsequent ISS flights, and residual platform enhancements. There are three remaining RTF deliverables under TSC. One is generic in nature and the other two are specific to the next two flights to the ISS. These deliverables will be used for ISS training upon delivery. Development of these loads is in the Development/Modernization/Enhancement (DME) category of the NASA Capital Planning and Investment Control (CPIC) process. The operations effort to support ISS training with these deliverables is in the Steady State (SS) category of the CPIC process.

Four deliverables remain in the development lifecycle phase under TSC to support flights subsequent to the RTF missions. These flight loads are being managed so that all simulation functionality is completed during the development lifecycle phase under TSC. These deliverables will be updated with the latest revisions of software and data necessary to correctly simulate the ISS behavior for the applicable flight during the operational lifecycle phase under SFOC. This work is tagged to the DME category of the CPIC process since it yields new capabilities despite occurring during the operational phase of the lifecycle. The work done by the operations contractor to refresh the configuration of these loads with the latest versions of software and data is consistent with steady state processes required during the operational phase. Consequently, this relatively small DME cost occurring during the operational lifecycle phase is not assessed using Earned Value measurement methodology. Instead, performance of this DME effort is assessed via operational measurement indicators including planned versus actual cost variance, customer satisfaction, and level of service.

The remaining platform enhancements consist of modernization efforts to re-host software from a Silicon Graphics Incorporated (SGI) platform to a Personal Computer (PC) platform. These include a Status and Control subsystem, a Camera Support System, and a backup storage system. In addition, remaining TSC work includes a re-architecture of the SSTF Robotics system. This is a streamlining initiative that will result in performance enhancements. This work is primarily DME; however, some steady state support is applicable by way of routine maintenance tasks necessary to enable the platform enhancements.

The process of transitioning the SSTF from TSC to SFOC is currently underway. Transition activities are planned to occur during FY04 and FY05.

Handover of responsibility for SSTF Maintenance and Operations (M&O) of the FTT, PTT, and AST is scheduled for July 1, 2004. Limited support for these functions will be provided under TSC until October 1, 2004. These are the first areas to transfer from the development to operations lifecycle phases. A series of five additional handovers is planned from October 2004 through April 2005. These subsequent events include hardware engineering, systems engineering, technical baseline products, I/T security, data integration, flight software integration, load build, test and verification, delivery management, reconfiguration, and sustaining.

Architecture

17.1.1 Business

17.1.1.1 Process simplification/reengineering/design projects

The re-host of the SSTF from an architecture based on Silicon Graphics Incorporated (SGI) computers to one based on Personal Computers (PCs) is complete. This is expected to be the last major re-engineering task in the SSTF. Future architecture changes will leverage off of the PC based architecture. Systems engineering principles will continue to be enforced and process definition and execution will continue in accordance with ISO9000 and Johnson Space Center (JSC) Quality Management System (QMS) practices.

Existing processes used to develop and manage the SSTF under the Training Systems Contract (TSC) will be transferred to the Space Flight Operations Contract (SFOC) for use as is. Once the SFOC contractor becomes comfortable with the SSTF processes, effort will be made to integrate as much of the SSTF processes into those used with the other facilities managed under SFOC. This will result in cost savings through resource and process synergy. This is expected to occur during FY07.

17.1.1.2 Major organization restructuring, training and change management projects

The transition of the Space Station Training Facility (SSTF) from the Training Systems Contract (TSC) to the Space Flight Operations Contract (SFOC) is a forthcoming major organizational change. Specifically, the development phase of the SSTF lifecycle implemented by Raytheon Technical Services Company (RTSC) under TSC will be complete and the operational phase will commence with support provided by United Space Alliance (USA) under SFOC. Handover of responsibilities from RTSC to USA will occur at six pre-defined points from July 2004 through April 2005. The TSC contract period of performance ends on April 30, 2005.

Future significant organizational changes will depend on SFOC contracting decisions. The SFOC period of performance is scheduled to end on September 30, 2005, unless it is extended via an option. If not extended, then a competitive procurement would occur. SSTF support would be included in the Statement Of Work for any re-competition of SFOC.

17.1.2 Data

17.1.2.1 Types of Data

The Space Station Training Facility (SSTF) accepts commands and generates data from an integrated set of International Space Station (ISS) simulation models. Commands are either operating system specific, application specific, or identical to ISS formats. Simulation data includes simulated internal system health and status, ISS telemetry, operating system responses, and application responses. The SSTF does not process any type of sensitive data.

17.1.2.2 Existing Data Access

NA. The data processed in the Space Station Training Facility (SSTF) is unique to the International Space Station (ISS) Program.

17.1.3 Application and Technology

17.1.3.1 Relationship to Service Component Model

Table 31

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Customer Services	Customer Relationship Management	Product Management		
Customer Services	Customer Relationship Management	Customer Feedback		
Customer Services	Customer Relationship Management	Surveys		
Customer Services	Customer Assistance	Initiated Online Help		
Customer Services	Customer Assistance	Initiated Assistance Request		
Customer Services	Customer Assistance	Initiated Scheduling		
Process Automation Services	Tracking Workflow	and Case / Issue Management		
Business Management Services	Management Process	of Change Management		
Business Management Services	Management Process	of Configuration Management		
Business Management Services	Management Process	of Requirements Management		
Business Management	Management	of Program / Project		

Services		Process	Management	
Business Management Services		Management Process	of	Quality Management
Business Management Services		Management Process	of	Risk Management
Business Management Services		Organizational Management		Network Management
Business Management Services		Investment Management		Strategic Planning and Mgmt
Business Management Services		Investment Management		Performance Management
Business Management Services		Supply Management	Chain	Procurement
Business Management Services		Supply Management	Chain	Ordering / Purchasing
Digital Services	Asset	Document Management		Library / Storage
Digital Services	Asset	Knowledge Management		Information Sharing
Digital Services	Asset	Knowledge Management		Knowledge Capture
Digital Services	Asset	Knowledge Management		Knowledge Distribution and Delivery
Digital Services	Asset	Records Management		Record Linking / Association
Business Analytical Services		Analysis Statistics	and	Modeling
Business Analytical Services		Analysis Statistics	and	Simulation

Business Analytical Services		Visualization	Imagery
Business Analytical Services		Reporting	Standardization / Canned
Back Office Services		Human Resources	Education / Training
Back Office Services		Human Resources	Health and Safety
Back Office Services		Assets / Materials Management	Property / Asset Management
Back Office Services		Assets / Materials Management	Facilities Management
Back Office Services		Development and Integration	Data Integration
Back Office Services		Development and Integration	Software Development
Back Office Services		Human Capital / Workforce Management	Resource Planning and Allocation
Back Office Services		Human Capital / Workforce Management	Skills Management
Support Services		Security Management	Identification and Authentication
Support Services		Security Management	Access Control
Support Services		Security Management	Encryption
Support Services		Security Management	Intrusion Detection
Support Services		Security Management	User Management
Support Services		Security Management	Role / Privilege Management
Support Services		Security Management	Audit Trail Capture and Analysis

Support Services	Collaboration	Email
Support Services	Collaboration	Document Library
Support Services	Communication	Audio Conferencing
Support Services	Systems Management	License Management
Support Services	Systems Management	Systems Resource Monitoring
Support Services	Forms Management	Forms Creation
Support Services	Forms Management	Forms Modification

17.1.3.2 *Relationship to Technology Component Model*

Table 32

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access and Delivery	Access Channels	Web Browser	The Space Station Training Facility (SSTF) supports the Technical Reference Model in the following ways: Access Channels Personal Computers (PCs) are provided at the SSTF Instructor Station consoles to support Instructor access to the Johnson Space Center (JSC) Intranet as well as Email services. SSTF also has connectivity to other systems. These include the Mission Control Center (MCC) at JSC, the Payload Operations and Integration Center (POIC) at Marshall Space Flight Center (MSFC), and the Shuttle Mission Training Facility (SMTF) located on the opposite side of JSC building 5 from the SSTF. In addition, the SSTF user interfaces, (i.e. Instructor Station, Portable Computer System laptop, and Station Support Computer) are remotely accessible from the Space Vehicle Mockup

Facility (SVMF) in JSC building 9.

Delivery Channels The SSTF supports information retrieval via the JSC intranet. In addition, The interface between the SSTF and the POIC at MSFC is via a Virtual Private Network (VPN) tunnel through the NASA Institutional Services Network (NISN).

Service Requirements SSTF supports Section 508 and NASA Information Technology (I/T) security requirements to the greatest extent possible. Annual audits are conducted to assess the level of compliance. Access controls to SSTF assets are enforced through initial user identification and then through authentication mechanisms. Authentication involves user-ID and password controls.

Service Transport SSTF deliverables, (i.e. training loads) are thoroughly tested prior to delivery. Standard testing involves installation testing, configuration verification, usability, and functional testing. Other types of testing are used as needs dictate. These include performance profiling, stress testing, and reliability testing. I/T security testing is also conducted, including access control.

Database and Storage SSTF uses Oracle for management of requirements and the list of external dependencies. The Russian Segment Trainer (RST) in the SSTF also uses Oracle. It has a file server that arbitrates data exchange between the Personal Computer (PC) cluster and the chassis containing Single Board Computers (SBCs) that process the Russian flight software.

Hardware / Infrastructure SSTF incorporates standard computer technology, (RAM, Hard disk drives, printers, and Ethernet network with supporting hubs, switches, and routers). SSTF also has microprocessors embedded on Single Board Computers (SBCs)

that execute the real International Space Station (ISS) flight software. Transceivers are used in the SSTF to support wireless connectivity within the SSTF emulation of the ISS onboard Local Area Network (LAN). Access to the Johnson Space Center (JSC) institutional network is through a firewall. A T1 line connects the SSTF development environment in the contractor's facility to the SSTF general purpose LAN. Storage of data within the SSTF is through a Redundant Array of Independent Disks (RAID) device. SecuritySSTF uses Secure Shell (SSH) for remote access to certain computers. These types of access are restricted to system administrators. Presentation / InterfaceThe SSTF web site uses Active Server Pages. IntegrationSSTF has a variety of middleware applications. Mode-to-model communication in the simulation is through a messaging infrastructure unique to the SSTF. This Simulation Virtual Machine (SVM) software manages data flow between the operating system and the real-time application layer. Database access is used within the SSTF to manage the process of looking up data needed for certain processing services. An object request broker is used to manage the state of simulated International Space Station (ISS) components in a database.

Service Access and Delivery	Access and Channels	Collaboration Communication
Service Access and Delivery	Access and Channels	Other Electronic Channels
Service Access and Delivery	Delivery and Channels	Intranet

Service Access and Delivery	Delivery Channels	Virtual Private Network (VPN)
Service Access and Delivery	Service Requirements	Legislative Compliance /
Service Access and Delivery	Service Requirements	Legislative Compliance /
Service Access and Delivery	Service Requirements	Authentication / Single Sign-on (SSO)
Service Access and Delivery	Service Transport	Test Management
Service Access and Delivery	Service Transport	Test Management
Service Access and Delivery	Service Transport	Test Management
Service Access and Delivery	Service Transport	Test Management
Service Access and Delivery	Service Transport	Test Management
Service Access and Delivery	Service Transport	Test Management
Service Access and Delivery	Service Transport	Test Management
Service Access and Delivery	Service Transport	Test Management
Service Access and Delivery	Database Storage	/ Database
Service	Hardware	/ Embedded

Access and Delivery	Infrastructure	Technology Devices
Service Access and Delivery	Hardware / Infrastructure	Embedded Technology Devices
Service Access and Delivery	Hardware / Infrastructure	Embedded Technology Devices
Service Access and Delivery	Hardware / Infrastructure	Embedded Technology Devices
Service Access and Delivery	Hardware / Infrastructure	Peripherals
Service Access and Delivery	Hardware / Infrastructure	Local Area Network (LAN)
Service Access and Delivery	Hardware / Infrastructure	Network Devices / Standards
Service Access and Delivery	Hardware / Infrastructure	Network Devices / Standards
Service Access and Delivery	Hardware / Infrastructure	Network Devices / Standards
Service Access and Delivery	Hardware / Infrastructure	Network Devices / Standards
Service Access and Delivery	Hardware / Infrastructure	Network Devices / Standards
Service Access and Delivery	Hardware / Infrastructure	Network Devices / Standards
Component Framework	Security	Supporting Security Services
Component Framework	Presentation / Interface	Dynamic / Server-Side Display

Service Interface and Integration **Integration** **Middleware**

Service Interface and Integration **Integration** **Middleware**

Service Interface and Integration **Integration** **Middleware**

17.1.3.3 Partnerships

Space Station Training Facility (SSTF) applications are unique to the International Space Station (ISS) Program.

17.1.4 Security and Privacy

17.1.4.1 How is it provided and funded?

The International Space Station (ISS) Program funds the Space Station Training Facility (SSTF) for all of its activities, including Information Technology (I/T) security.

17.1.4.2 How is security accomplished?

The JSC I/T Security Handbook (JPG-2810.1) prescribes the C&A process. It is derived from the parent NASA handbook (NPG-2810.1). The NASA/JSC Space Station Training Facility (SSTF) Project Office and the SSTF Contractor conduct a review of the implemented security controls and inherent risk. This is done at least annually. The agreed risk posture is coordinated with the Mission Operations Directorate (MOD) Organization Computer Security Manager (OCSM) in an annual review. These reviews consider guidance on risk posture and mitigation measures from the I/T Security Handbooks. The resulting security posture is presented to MOD management in an annual Authorization To Process (ATP) review. Focus is on acceptability of the residual risks. Authorization to process is granted if the risks are deemed acceptable.

SSTF operational and technical security controls are tested in conjunction with system changes or vulnerability assessments. The scope of these tests is generally focused on a particular aspect of the system, but the frequency of the tests is routine, (one every four to six weeks on average). Issues that surface relative to the effectiveness of the controls are resolved in conjunction with

the associated change. SSTF managerial controls are typically evaluated during the course of the annual security controls review prior to updating the Security Plan. The policies, procedures, and directives that the managerial controls are based upon are re-assessed through this process.

Annual Information Technology (I/T) security training addresses identification of security incidents and the user role in responding to an identified incident. The incident response process is a formal process governed by ISO9000 compliant work instructions. A priority list identifying points of contact is established for communicating the incident and soliciting further response action. System Analysts who support daily operations are key initial points of contact. The Space Station Training Facility (SSTF) security administrators respond and resolve all incidents. The level of response is dependent upon the potential impact of the incident. Response considerations are coordinated with NASA. Incidents having applicability outside the SSTF are coordinated with the affected facilities through established JSC incident response processes.

Intrusion detection in the SSTF is supported primarily through review of audit logs. The system administrators execute special scripts on a daily basis that capture key information from the system audit logs. The scripts are designed to flag violations or unusual activity, like frequent, repeated unsuccessful access attempts. The logs are also manually reviewed for less obvious signatures of potentially harmful activity at least monthly. Any identified issues are addressed through follow-up actions.

Johnson Space Center (JSC) network administrators routinely conduct intrusion detection monitoring. The SSTF often supports analysis of observed events in network traffic data as requested by the Center. In addition, SSTF responds to alerts issued by the Center for vulnerabilities that are discovered in relevant security software or implementations. JSC administrators coordinate with external agencies regarding security incidents.

Information Technology (I/T) security incidents that are identified in the SSTF are handled in accordance with Mission Operations Directorate (MOD) and Johnson Space Center (JSC) processes. Incidents identified by the SSTF that have applicability external to the SSTF are reported to the MOD Organizational Computer Security Manager (OCSM). The OCSM coordinates the incident with JSC IT security teams. These teams elevate security incidents as necessary to external IT security organizations within the Government. Security threats identified by other Governmental organizations are reported through the JSC IT security teams and the MOD OCSM. Also, the JSC security teams conduct routine vulnerability scans. The SSTF security and system administrators respond as necessary to externally identified security threats or vulnerabilities.

17.1.4.3 *Effective use of security, controls and authentication tools*

Public access to the Space Station Training Facility (SSTF) is prohibited. Layers of network protection and internal access controls ensure exclusion of public accessibility. Encryption is used on the link with the Payload Operations and Integration Center (POIC). Additionally, the surrounding Johnson Space Center (JSC) firewalls and the SSTF firewall provide a solid barrier between the SSTF and public access.

17.1.5 Government Paperwork Elimination Act

N/A. The Space Station Training Facility (SSTF) does not support electronic transactions or record keeping that is covered by GPEA.

18 Kennedy Space Center (KSC) – Ground Operations

Project Description

Ground Operations is in the Operational phase of the NASA Capital Planning and Investment Control Process. Ground Operations are networks, tasks, and functions that are not covered in the Launch Control Systems and directly support Shuttle Processing at the Kennedy Space Center. This covers all platforms and LAN operational functions and associated maintenance and support of ADP hardware and software. This category also covers the O&M of the various Instrumentation systems such as the Ground Measurement System, Permanent Measuring System, Catenary Wire Lightning Instrumentation System, Lightning Induced Voltage Instrumentation System, the Shuttle Modal Inspection System, and others.

The FY04 information technology annual review/approval (Capital Planning and Investment Control process) for this investment was held September 26, 2003 by the Shuttle Program IT CPIC Review Board. The SSP Program Integration (PI) Information Technology (IT) plan is a part of the Space Flight Operations Contract (SFOC) overall annual Level A (5 year) and Level B (annual Fiscal Year) Information Technology Plan deliverables to the Space Shuttle Program (SSP) Chief Information Officer (CIO). FY04 Plans reviewed and approved in September 2004 by the SSP CIO with concurrence from the Johnson Space Center (JSC) CIO, Kennedy Space Center CIO and Marshall Space Flight Center CIO. The major IT expenses deal with either sustaining the above systems or migrating mainframe projects to a web-based, client-server environment using state of the art technology for data access, availability and transfer.

This investment is closely coupled with shuttle processing. The loss of this investment would require us to revert to manual based systems. This would increase our headcount and impact our processing schedule.

Architecture

18.1.1 Business

18.1.1.1 Process simplification/reengineering/design projects

None. The Project is currently in the mission operations phase. Organizational restructuring, training, and change management have been accomplished throughout the project’s life cycle.

18.1.1.2 Major organization restructuring, training and change management projects

None. The Project is currently in the mission operations phase. Organizational restructuring, training, and change management have been accomplished throughout the project’s life cycle.

18.1.2 Data

18.1.2.1 Types of Data

In addition to Shuttle telemetry data there is various types of planning, processing, maintenance and other data related to the different Ground Operations managed systems, networks and processes.

18.1.2.2 Existing Data Access

18.1.3 Application and Technology

18.1.3.1 Relationship to Service Component Model

Table 33

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Process Automation Services	Tracking and Workflow	Process Tracking	No	
Process Automation Services	Tracking and Workflow	Case / Management	Issue No	
Process Automation Services	Tracking and Workflow	Conflict Resolution	No	
Process Automation Services	Routing and Scheduling	Inbound Correspondence Management	No	
Process	Routing and	Outbound	No	

Automation Services	Scheduling	Correspondence Management		
Process Automation Services	Management of Process	Change Management		No
Process Automation Services	Management of Process	Configuration Management		No
Process Automation Services	Management of Process	Requirements Management		No
Process Automation Services	Management of Process	Program / Management	Project	No
Process Automation Services	Management of Process	Governance / Management	Policy	No
Process Automation Services	Management of Process	Business Management	Rule	No
Process Automation Services	Management of Process	Quality Management		No
Process Automation Services	Management of Process	Risk Management		No
Process Automation Services	Organizational Management	Workgroup/Groupware		No
Process Automation Services	Organizational Management	Network Management		No
Process Automation Services	Investment Management	Strategic Planning and Mgmt		No
Process Automation Services	Investment Management	Portfolio Management		No
Process Automation	Investment Management	Performance Management		No

Services

Process Automation Services	Supply Chain Management	Procurement	No
Process Automation Services	Supply Chain Management	Sourcing Management	No
Process Automation Services	Supply Chain Management	Catalog Management	No
Process Automation Services	Supply Chain Management	Ordering / Purchasing	No
Process Automation Services	Supply Chain Management	Invoice / Requisition Tracking and Approval	No
Digital Asset Services	Content Management	Content Authoring	No
Digital Asset Services	Content Management	Content Review and Approval	No
Digital Asset Services	Content Management	Tagging and Aggregation	No
Digital Asset Services	Content Management	Content Publishing and Delivery	No
Digital Asset Services	Content Management	Syndication Management	No
Digital Asset Services	Document Management	Document Imaging and OCR	No
Digital Asset Services	Document Management	Document Referencing	No
Digital Asset Services	Document Management	Document Revisions	No
Digital Asset Services	Document Management	Library / Storage	No
Digital Asset Services	Document Management	Document Review and Approval	No
Digital Asset Services	Document Management	Document Conversion	No

Digital Asset Services	Document Management		Indexing	No
Digital Asset Services	Document Management		Classification	No
Digital Asset Services	Knowledge Management		Knowledge Discovery	No
Digital Asset Services	Knowledge Management		Knowledge Capture	No
Digital Asset Services	Knowledge Management		Knowledge Engineering	No
Digital Asset Services	Knowledge Management		Information Retrieval	No
Digital Asset Services	Knowledge Management		Information Mapping / Taxonomy	No
Digital Asset Services	Knowledge Management		Information Sharing	No
Digital Asset Services	Knowledge Management		Categorization	No
Digital Asset Services	Knowledge Management		Knowledge Engineering	No
Digital Asset Services	Records Management		Record Linking / Association	No
Digital Asset Services	Records Management		Document Classification	No
Digital Asset Services	Records Management		Document Retirement	No
Digital Asset Services	Records Management	Digital Management	Rights	No
Business Analytical Services	Analysis Statistics	and	Modeling	No
Business Analytical Services	Analysis Statistics	and	Predictive	No
Business Analytical Services	Analysis Statistics	and	Simulation	No

Business Analytical Services	Analysis and Statistics	Mathematical	No
Business Analytical Services	Analysis and Statistics	Structural / Thermal	No
Business Analytical Services	Visualization	Graphing / Charting	No
Business Analytical Services	Visualization	Imagery	No
Business Analytical Services	Visualization	Multimedia	No
Business Analytical Services	Visualization	CAD	No
Business Analytical Services	Business Intelligence	Demand Forecasting / Mgmt	No
Business Analytical Services	Business Intelligence	Balanced Scorecard	No
Business Analytical Services	Business Intelligence	Decision Support and Planning	No

18.1.3.2 Relationship to Technology Component Model

Table 34

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access and Delivery	Access Channels	Web Browser	
Service Access and Delivery	Access Channels	Wireless / PDA	
Service Access and Delivery	Access Channels	Collaboration Communication	

Service Delivery	Access and	Access Channels	Other Channels	Electronic
Service Delivery	Access and	Delivery Channels	Internet	
Service Delivery	Access and	Delivery Channels	Intranet	
Service Delivery	Access and	Delivery Channels	Extranet	
Service Delivery	Access and	Delivery Channels	Peer to Peer (P2P)	
Service Delivery	Access and	Delivery Channels	Virtual Private Network (VPN)	
Service Delivery	Access and	Delivery Channels	Legislative / Compliance	
Service Delivery	Access and	Delivery Channels	Authentication / Single Sign-on (SSO)	
Service Delivery	Access and	Delivery Channels	Hosting	
Service Delivery	Access and	Service Transport	Supporting Services	Network
Service Delivery	Access and	Service Transport	Test Management	
Service Delivery	Access and	Service Transport	Modeling	
Service Infrastructure	Platform and	Database / Storage	Database	
Service Infrastructure	Platform and	Database / Storage	Storage	
Service Infrastructure	Platform and	Hardware Infrastructure	/ Servers / Computers	
Service Infrastructure	Platform and	Hardware Infrastructure	/ Embedded Technology Devices	
Service Infrastructure	Platform and	Hardware Infrastructure	/ Peripherals	
Service Infrastructure	Platform and	Hardware Infrastructure	/ Wide Area Network (WAN)	

Service Platform and Infrastructure	Hardware Infrastructure	/ Local Area Network (LAN)
Service Platform and Infrastructure	Hardware Infrastructure	/ Network Devices / Standards
Service Platform and Infrastructure	Hardware Infrastructure	/ Video Conferencing
Component Framework	Security	Certificates / Digital Signature
Component Framework	Security	Supporting Security Services
Component Framework	Presentation Interface	/ Static Display
Component Framework	Presentation Interface	/ Dynamic / Server-Side Display
Component Framework	Presentation Interface	/ Content Rendering
Component Framework	Presentation Interface	/ Wireless / Mobile / Voice
Component Framework	Data Interchange	Data Transformation
Service Interface and Integration	Integration	Middleware
Service Interface and Integration	Integration	Enterprise Application Integration
Service Interface and Integration	Interoperability	Data Format / Classification
Service Interface and Integration	Interoperability	Data Types / Validation
Service Interface and Integration	Interoperability	Data Transformation
Service Interface and Integration	Interface	Service Discovery
Service Interface and Integration	Interface	Service Description / Interface

18.1.3.3 Partnerships

18.1.4 Security and Privacy

18.1.4.1 How is it provided and funded?

In FY2006 four percent of the Ground Operations budget supports the IT security investment. The Shuttle Program funds the Project for all of its activities including providing security. USA Information Management (IM) Functional Policy & Procedure (FPP) D-03-02, IT Security Risk Assessment & Planning, defines the risk assessment and security planning process. FPP D-03-05, IT Security Requirements, documents all NPR 2810.1 IT Security controls as-well-as other controls that are considered industry best practices. The USA SRB Element contains six (6) IT systems. Each USA-managed government (NASA) system has a current security plan.

FPP D-03-05, IT Security Requirements, addresses the NIST 17 critical elements through 10 categories that contain a subset of the 17 critical elements. These 10 categories are: Continuity of Operations, Monitoring, Configuration Management, Physical, File Protection, Userid, Network, Security Program, Training, and Hazard Mitigation. These categories form the basis of the IT security risk assessment, required risk reduction/mitigation, and the subsequent security posture presentation to USA Facility/System Management (FSM), NASA Line Management, NASA Senior Management (with fiduciary responsibility for the system) and the NASA CIO required to obtain Authorization to Process (ATP) or accreditation of a system.

18.1.4.2 How is security accomplished?

USA Information Management (IM) Functional Policy & Procedure (FPP) D-03-02, IT Security Risk Assessment & Planning, defines the risk assessment and security planning process. FPP D-03-05, IT Security Requirements, documents all NPR 2810.1 IT Security controls as-well-as other controls that are considered industry best practices. The USA SRB Element contains six (6) IT systems. Each USA-managed government (NASA) system has a current security plan.

FPP D-03-05, IT Security Requirements, addresses the NIST 17 critical elements through 10 categories that contain a subset of the 17 critical elements. These 10 categories are: Continuity of Operations, Monitoring, Configuration Management, Physical, File Protection, Userid, Network, Security Program, Training, and Hazard Mitigation. These categories form the basis of the IT security risk assessment, required risk reduction/mitigation, and the subsequent security posture presentation to USA Facility/System Management (FSM), NASA Line Management, NASA Senior Management (with fiduciary responsibility for the system) and the NASA CIO required to obtain Authorization to Process (ATP) or accreditation of a system.

The investment meets the security requirements by following NASA policy and guidance

documents NPD and NPR 2810, adhering to updates from NIST guidelines and incorporating OMB polices as issued.

USA Information Management (IM) Functional Policy & Procedure (FPP) D-03-01, IT Security Accreditation, defines the accreditation process. All security plans are accredited in accordance with NPR 2810.1 and have current NASA Authorization to Process (ATP) documents signed by the NASA Director of Shuttle Processing and the KSC NASA IT Security Manager (IT) (KSC NASA Chief Information Office). GO System's Accreditation dates are:

Critical / SMA Systems: LTS&G – USA000624 (7/31/03), NAVAIDS (formerly MSBLS) – USA003070 (11/30/03), SMIS – USA002482 (4/30/04), LIVIS/CWLIS – USA001107 (9/30/03), RKDN – USA003057 (6/30/03), SPDMS – USA002856 (10/31/03), GPSS – USA002945 (4/30/04), GSDE – USA002847 (5/31/03), INCS – USA008291 (3/31/04),

General Support Systems: WALDPS – USA003121 (5/31/03), GMS/PMS – USA002883, (7/30/01), USAGO-D – USA001156 (10/31/03), EMDS – USA007032 (11/30/03) and Maximo – USA005516 (1/31/04).

IT Security incidents are handled and reported in accordance with FPP D-03-06, IT Security Incident Reporting. Incidents involving NASA IT resources are reported to the NASA Shuttle Processing Computer Security Manager and the KSC NASA ITSM/CIO. USA IT Security also maintains a 7x24 Incident Response Team (IRT) capability that allows all employees and subcontractors (as well as NASA) to report suspected IT Security incidents via a 1-888 # paging system.

Logs are reviewed daily, intrusion detection is run continuously, and the network is scanned quarterly for vulnerabilities. Information Technology Security (ITS) is implemented in accordance with NASA Procedures and Guidelines (NPR) 2810.1, Security of Information Technology. For reporting, we use an approved Kennedy Process, KDP-KSC-P-1839. All incidents are reported to DHS' Fed CIRC.

USA IT Security provides copies of all system security plans to NASA. USA IT Security provides system security posture presentations (obtained from the results of system IT security risk assessments) to the NASA Shuttle Processing Computer Security Manager, NASA Director of Shuttle Processing, and the KSC NASA ITSM/CIO in order to obtain NASA 's Authorization to Process (ATP) concurrence for each system.

Yes

The system is operated by contractors. All contracts include specific security requirements required by law and policy. The NASA KSC Shuttle Processing OCSM has access to the USA policies and desk instructions. Access is also provided to security plans, risk assessments, incident response and audit data. The OCSM tracks and provides inputs into agency security requirements and contractor security modifications. The OCSM coordinates and integrates the Authority To Proceed for the ITSAA on KSC Shuttle Processing Systems. All security plans are approved by ITSAA. The OCSM coordinates the development and execution of the scanning of contractor resources located in Customer Owned & Maintain (COAM) networks. In addition

the OCSM also assesses contractor's performance to NPG 2810, "IT Security Requirements" and to USA internal processes and procedures.

18.1.4.3 *Effective use of security, controls and authentication tools*

Not Applicable, since the Ground Operations does not allow public access.

18.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000. The date of the most recent update to the agency GPEA plan, the 2003 progress update is provided below.

19 Kennedy Space Center (KSC) – Integrated Logistics

Project Description

The Space Shuttle program plays a vital role in enabling NASA's vision and mission. This includes advancing human exploration and providing safe access to space in support of human operations in low-earth orbit. In order to maintain a viable human transportation capability that will operate and support NASA's launch requirements, specific program investments are required. NASA is revamping its approach to selecting and managing these investments to ensure Shuttle operability into the next decade and avoid future project overruns. These investments will be consistent with NASA's strategy of ensuring the Space Shuttle remains viable until a new transportation system is operational. These projects will provide revitalization of the infrastructure, and combat obsolescence of vehicle, ground systems, and facilities.

The Integrated Logistics organization supports NASA's strategies for future IT initiatives while complying with consolidated IT standards. The Integrated Logistics organization maintains current Logistics systems as well as spares and provides repair support for the Operations Center for Shuttle Avionics Integration Laboratory (SAIL), Training Operations Center (TOC) and Integration and Program Requirements-Multi-facility.

The Integrated Logistics organization provides spares/repairs for IT hardware and software supporting NASA Shuttle Logistics Depot (NSLD) Special Test Equipment and CAD systems that support manufacturing and repair activities.

The Integrated Logistics organization continues to support current and future process improvements and support the IT requirements for the migration of the Logistics systems to the enterprise Peoplesoft Tool. PeopleSoft Inventory - The first release of the PeopleSoft Inventory and Manufacturing system was completed in July 2002. The focus is on system improvements such as the streamlined demand process, inventory out-of-balance corrections, Shelf-Life Management, Contamination /Decontamination requests, ASRS Mini-loader interface.

Peoplesoft is required to process the Space Shuttle at KSC.

The Integrated Logistics function is in the operational phase. The Space Flight Operations Contract (SFOC) covers all Information Technology (IT) related activities including the design, development, implementation and maintenance of computer-related hardware and software systems as required to process the Space Shuttle at KSC. This includes Integrated Logistics which provides for repairs, spare parts, and warehousing for the Space Shuttle Orbiters, and associated Ground Support Equipment (GSE).

The Integrated Logistic investment reduces lifecycle cost of replacement equipment. The requirements for lifecycle cost for replacement of Ground Support Equipment (GSE) is the only supported funding in the lifecycle cost of this GSE.

The FY04 information technology annual review/approval (Capital Planning and Investment Control process) for this investment was held September 26, 2003 by the Shuttle Program IT CPIC Review Board. The SSP Program Integration (PI) Information Technology (IT) plan is a part of the Space Flight Operations Contract (SFOC) overall annual Level A (5 year) and Level B (annual Fiscal Year) Information Technology Plan deliverables to the Space Shuttle Program (SSP) Chief Information Officer (CIO). FY04 Plans reviewed and approved in September 2004 by the SSP CIO with concurrence from the Johnson Space Center (JSC) CIO, Kennedy Space Center CIO and Marshall Space Flight Center CIO. The major IT expenses deal with either sustaining the above systems or migrating mainframe projects to a web-based, client-server environment using state of the art technology for data access, availability and transfer.

This investment is closely coupled with Shuttle Processing. The loss of this investment would require us to revert to manual based systems. This would increase our headcount and impact our processing schedule.

Architecture

19.1.1 Business

19.1.1.1 Process simplification/reengineering/design projects

None. The Project is currently in the mission operations phase. Organizational restructuring, training ,and change management have been accomplished throughout the project's life cycle.

19.1.1.2 Major organization restructuring, training and change management projects

None. The Project is currently in the mission operations phase. Organizational restructuring, training ,and change management have been accomplished throughout the project's life cycle.

19.1.2 Data

19.1.2.1 *Types of Data*

Data is various types of planning, processing, maintenance and other data related to the different Integrated Logistics managed systems, networks and processes.

19.1.2.2 *Existing Data Access*

19.1.3 Application and Technology

19.1.3.1 *Relationship to Service Component Model*

Table 35

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Customer Services	Customer Relationship Management	Customer Analytics	No	
Customer Services	Customer Relationship Management	Product Management	No	
Customer Services	Customer Relationship Management	Contact Management	No	
Customer Services	Customer Relationship Management	Partner Relationship Management	No	
Customer Services	Customer Relationship Management	Customer Feedback	No	
Back Office Services	Assets / Materials Management	Asset Cataloging / Identification	No	
Back Office Services	Assets / Materials Management	Asset Allocation, Transfer, and Maintenance	No	
Back Office Services	Assets / Materials Management	Facilities Management	No	

Process Automation Services	Tracking Workflow	and	Process Tracking	No
Process Automation Services	Tracking Workflow	and	Conflict Resolution	No
Process Automation Services	Management Process	of	Change Management	No
Process Automation Services	Management Process	of	Configuration Management	No
Process Automation Services	Management Process	of	Requirements Management	No
Process Automation Services	Management Process	of	Program / Project Management	No
Process Automation Services	Management Process	of	Governance / Policy Management	No
Process Automation Services	Management Process	of	Quality Management	No
Process Automation Services	Management Process	of	Risk Management	No
Process Automation Services	Investment Management		Strategic Planning and Mgmt	No
Process Automation Services	Investment Management		Performance Management	No
Process Automation Services	Supply Chain Management		Procurement	No
Process Automation Services	Supply Chain Management		Sourcing Management	No
Process	Supply Chain		Catalog	No

Automation Services		Management	Management	
Process Automation Services		Supply Chain Management	Ordering / Purchasing	No
Process Automation Services		Supply Chain Management	Invoice / Tracking and Requisition Approval	No
Process Automation Services		Supply Chain Management	Returns Management	No
Back Office Services		Financial Management	Expense Management	No
Back Office Services		Financial Management	Payroll	No
Back Office Services		Financial Management	Payment / Settlement	No
Back Office Services		Assets / Materials Management	Property / Asset Management	No
Back Office Services		Financial Management	Revenue Management	No
Back Office Services		Financial Management	Auditing	No
Back Office Services		Financial Management	Financial Reporting	No
Digital Asset Services		Knowledge Management	Information Retrieval	No
Digital Asset Services		Knowledge Management	Information Sharing	No
Digital Asset Services		Knowledge Management	Categorization	No
Digital Asset Services		Knowledge Management	Knowledge Engineering	No
Digital Asset Services		Knowledge Management	Knowledge Capture	No
Digital Asset Services		Knowledge Management	Knowledge Discovery	No

Digital Services	Asset Management	Knowledge Management	Knowledge Distribution and Delivery	No
Back Office Services	Office Management	Financial Management	Billing Accounting	No
Back Office Services	Office Management	Financial Management	Credit / Change	No
Back Office Services	Office Management	Data Management	Data Classification	No
Back Office Services	Office Management	Data Management	Data Recovery	No
Business Analytical Services		Analysis Statistics	and Modeling	No
Business Analytical Services		Analysis Statistics	and Predictive	No
Business Analytical Services		Analysis Statistics	and Simulation	No
Business Analytical Services		Analysis Statistics	and Mathematical	No
Business Analytical Services		Visualization	Graphing / Charting	No
Business Analytical Services		Visualization	Imagery	No
Business Analytical Services		Visualization	Multimedia	No
Business Analytical Services		Visualization	CAD	No
Business Analytical Services		Business Intelligence	Demand Forecasting / Mgmt	No
Business		Business	Balanced Scorecard	No

Analytical Services		Intelligence			
Business Analytical Services		Business Intelligence	Decision and Planning	Support	No
Business Analytical Services		Business Intelligence	Data Mining		No
Business Analytical Services		Reporting	Ad-Hoc		No
Business Analytical Services		Reporting	Standardization Canned	/	No
Back Office Services		Data Management	Data Exchange		No
Back Office Services		Data Management	Data Warehouse		No
Back Office Services		Data Management	Loading and Archiving	and	No

19.1.3.2 Relationship to Technology Component Model

Table 36

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access and Delivery	Access Channels	Web Browser	
Service Access and Delivery	Access Channels	Wireless / PDA	
Service Access and Delivery	Access Channels	Collaboration Communication	
Service Access and Delivery	Access Channels	Other Electronic Channels	
Service Access and Delivery	Delivery Channels	Internet	
Service Access and Delivery	Delivery Channels	Extranet	

Service Access and Delivery	and	Delivery Channels	Intranet
Service Access and Delivery	and	Delivery Channels	Peer to Peer (P2P)
Service Access and Delivery	and	Delivery Channels	Virtual Private Network (VPN)
Service Access and Delivery	and	Service Requirements	Legislative Compliance /
Service Access and Delivery	and	Service Requirements	Hosting
Service Access and Delivery	and	Service Transport	Supporting Network Services
Service Access and Delivery	and	Service Transport	Test Management
Service Platform and Infrastructure	and	Database / Storage	Database
Service Platform and Infrastructure	and	Database / Storage	Storage
Service Platform and Infrastructure	and	Hardware Infrastructure	/ Servers / Computers
Service Platform and Infrastructure	and	Hardware Infrastructure	/ Embedded Technology Devices
Service Platform and Infrastructure	and	Hardware Infrastructure	/ Peripherals
Service Platform and Infrastructure	and	Hardware Infrastructure	/ Wide Area Network (WAN)
Service Platform and Infrastructure	and	Hardware Infrastructure	/ Local Area Network (LAN)
Service Platform and Infrastructure	and	Hardware Infrastructure	/ Network Devices / Standards
Service Platform and Infrastructure	and	Hardware Infrastructure	/ Video Conferencing
Component Framework		Security	Certificates / Digital Signature
Component Framework		Security	Supporting Security Services

Component Framework	Presentation Interface	/ Static Display
Component Framework	Presentation Interface	/ Dynamic / Server-Side Display
Component Framework	Presentation Interface	/ Content Rendering
Component Framework	Presentation Interface	/ Wireless / Mobile / Voice
Component Framework	Data Interchange	Data Transformation
Service Interface and Integration	Integration	Middleware
Service Interface and Integration	Integration	Enterprise Application Integration
Service Interface and Integration	Interoperability	Data Format / Classification
Service Interface and Integration	Interface	Service Discovery
		Service Description / Interface

19.1.3.3 Partnerships

None.

19.1.4 Security and Privacy

19.1.4.1 How is it provided and funded?

In FY2005 four percent of the Integrated Logistics budget supports the IT security investment.

19.1.4.2 How is security accomplished?

USA Information Management (IM) Functional Policy & Procedure (FPP) D-03-02, IT Security Risk Assessment & Planning, defines the risk assessment and security planning process. FPP D-03-05, IT Security Requirements, documents all NPR 2810.1 IT Security controls as-well-as other controls that are considered industry best practices. USA Integrated Logistics contains six

(2) IT systems. Each USA-managed government (NASA) system has a current security plan.

FPP D-03-05, IT Security Requirements, addresses the NIST 17 critical elements through 10 categories that contain a subset of the 17 critical elements. These 10 categories are: Continuity of Operations, Monitoring, Configuration Management, Physical, File Protection, Userid, Network, Security Program, Training, and Hazard Mitigation. These categories form the basis of the IT security risk assessment, required risk reduction/mitigation, and the subsequent security posture presentation to USA Facility/System Management (FSM), NASA Line Management, NASA Senior Management (with fiduciary responsibility for the system) and the NASA CIO required to obtain Authorization to Process (ATP) or accreditation of a system.

USA Information Management (IM) Functional Policy & Procedure (FPP) D-03-01, IT Security Accreditation, defines the accreditation process. All security plans are accredited in accordance with NPR 2810.1 and have current NASA Authorization to Process (ATP) documents signed by the NASA Director of Shuttle Processing and the KSC NASA IT Security Manager (IT) (KSC NASA Chief Information Office). IL System's Accreditation dates are:

General Support Systems: LAWCS – USA002532 (2/28/04), CRCA – USA008119 (3/31/04), and FDM – USA002233 (3/31/04)

IT Security incidents are handled and reported in accordance with FPP D-03-06, IT Security Incident Reporting. Incidents involving NASA IT resources are reported to the NASA Shuttle Processing Computer Security Manager and the KSC NASA ITSM/CIO. USA IT Security also maintains a 7x24 Incident Response Team (IRT) capability that allows all employees and subcontractors (as well as NASA) to report suspected IT Security incidents via a 1-888 # paging system.

USA IT Security Audit, Investigation, and Reporting (ITSAIR) conducts hands-on audits of USA-managed systems. USA Information Management (IM) Functional Policy & Procedure (FPP) D-03-12, IT Security Audits, defines the audit process. These audits are conducted independent from and are not part of the system risk assessments conducted by USA IT Security Computer Security Officials (CSO's). Audits are conducted periodically depending on the criticality of the system – but not to exceed a three-year period. The audits include verification of IT Security controls documented in the security plan (based on the CSO's risk assessment), running penetration-type software programs to test password controls, etc., as-well-as system configuration controls. In addition to (ITSAIR) audits, ITSAIR also conducts NASA-mandated network vulnerability scans on a quarterly basis of USA-managed systems that reside behind USA-managed firewalls. System vulnerability data and risk reduction status reports are provided to the KSC IT Security Manager / CIO. IL Audits dates are:

General Support Systems: LAWCS (9/02/02), FDM (5/25/04), and CRCA – Audit date TBD (new facility accredited in March 2004).

USA IT Security provides copies of all system security plans to NASA. USA IT Security provides system security posture presentations (obtained from the results of system IT security risk assessments) to the NASA Shuttle Processing Computer Security Manager, NASA Director of Shuttle Processing, and the KSC NASA ITSM/CIO in order to obtain NASA's Authorization to Process (ATP) concurrence for each system

19.1.4.3 *Effective use of security, controls and authentication tools*

Not Applicable, since Integrated Logistics does not allow public access.

19.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

20 Kennedy Space Center (KSC) – Launch Control System (LCS)

Project Description

The Launch Control System (LCS) function is in the operational phase of the NASA Capital Planning and Investment Control (CPIC) process. The Launch Control System (LCS) is required at Kennedy Space Center to process and launch the Space Shuttle. It consists of Shuttle Data Center (SDC), Checkout Control and Monitor Subsystem (CCMS) Operations, Record and Playback Subsystem (RPS), and Other Non-System Specific Systems (Other O&M). The Shuttle Data Center provides storage and recall of all shuttle processing and launch data. The CCMS is a custom design computer hardware and software system for processing and launching the Space Shuttle. The system currently operates with 100 consoles, 240 peripherals, 12 million lines of Launch Processing System (LPS) source code, and 1.6 million lines of executable Ground Operations Aerospace Language (GOAL) code. The Record and Playback Subsystem (RPS) primary function is to record unprocessed Shuttle on board instrumentation data during tests and launch countdowns.

The FY04 information technology annual review/approval (Capital Planning and Investment Control process) for this investment was held September 26, 2003 by the Shuttle Program IT CPIC Review Board. The SSP Program Integration (PI) Information Technology (IT) plan is a part of the Space Flight Operations Contract (SFOC) overall annual Level A (5 year) and Level B (annual Fiscal Year) Information Technology Plan deliverables to the Space Shuttle Program (SSP) Chief Information Officer (CIO). FY04 Plans reviewed and approved in September 2004 by the SSP CIO with concurrence from the Johnson Space Center (JSC) CIO, Kennedy Space Center CIO and Marshall Space Flight Center CIO. The major IT expenses deal with either sustaining the above systems or migrating mainframe projects to a web-based, client-server environment using state of the art technology for data access, availability and transfer.

Shuttle Engineering and the Business Office review each element on a yearly basis to address supportability, maintainability and upgrades. All elements are required for KSC to process and launch the Space Shuttle and/or its payloads.

This investment is closely coupled with shuttle processing. The loss of this investment would

require us to revert to manual based systems. This would increase our headcount and impact our processing schedule.

Architecture

20.1.1 Business

20.1.1.1 *Process simplification/reengineering/design projects*

None. The Project is currently in the mission operations phase. Organizational restructuring, training, and change management have been accomplished throughout the project’s life cycle.

20.1.1.2 *Major organization restructuring, training and change management projects*

None. The Project is currently in the mission operations phase. Organizational restructuring, training, and change management have been accomplished throughout the project’s life cycle.

20.1.2 Data

20.1.2.1 *Types of Data*

In addition to Shuttle telemetry data there are various types of planning, processing, maintenance and other data related to the different Launch Control Systems managed systems, networks and processes.

20.1.2.2 *Existing Data Access*

20.1.3 Application and Technology

20.1.3.1 *Relationship to Service Component Model*

Table 37

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Customer Services	Customer Relationship Management	Call Center Management	No	

Customer Services	Customer Relationship Management		Product Management	No
Customer Services	Customer Relationship Management		Customer / Account Management	No
Customer Services	Customer Relationship Management		Contact Management	No
Customer Services	Customer Relationship Management		Partner Relationship Management	No
Customer Services	Customer Relationship Management		Customer Feedback	No
Customer Services	Customer Relationship Management		Surveys	No
Customer Services	Customer Preferences		Profile Management	No
Customer Services	Customer Initiated Assistance		Online Help	No
Customer Services	Customer Initiated Assistance		Online Tutorials	No
Customer Services	Customer Initiated Assistance		Assistance Request	No
Customer Services	Customer Initiated Assistance		Scheduling	No
Process Automation Services	Tracking Workflow	and	Process Tracking	No
Process Automation Services	Tracking Workflow	and	Case / Issue Management	No
Process Automation	Tracking Workflow	and	Conflict Resolution	No

Services

Process Automation Services	Routing and Scheduling	Inbound Correspondence Management	No
Process Automation Services	Routing and Scheduling	Outbound Correspondence Management	No
Process Automation Services	Management of Process	Change Management	No
Process Automation Services	Management of Process	Configuration Management	No
Process Automation Services	Management of Process	Requirements Management	No
Process Automation Services	Management of Process	Program / Project Management	No
Process Automation Services	Management of Process	Governance / Policy Management	No
Process Automation Services	Management of Process	Quality Management	No
Process Automation Services	Management of Process	Business Management	Rule No
Process Automation Services	Management of Process	Risk Management	No
Process Automation Services	Organizational Management	Workgroup/Groupware	No
Process Automation Services	Organizational Management	Network Management	No
Process Automation Services	Investment Management	Strategic Planning and Mgmt	No

Process Automation Services	Investment Management	Performance Management	No
Digital Asset Services	Content Management	Content Authoring	No
Digital Asset Services	Content Management	Content Review and Approval	No
Digital Asset Services	Document Management	Document Imaging and OCR	No
Digital Asset Services	Document Management	Document Referencing	No
Digital Asset Services	Document Management	Document Revisions	No
Digital Asset Services	Document Management	Library / Storage	No
Digital Asset Services	Document Management	Document Review and Approval	No
Digital Asset Services	Document Management	Document Conversion	No
Digital Asset Services	Document Management	Indexing	No
Digital Asset Services	Document Management	Classification	No
Digital Asset Services	Knowledge Management	Information Retrieval	No
Digital Asset Services	Knowledge Management	Information Sharing	No
Digital Asset Services	Records Management	Record Linking / Association	No
Digital Asset Services	Records Management	Document Classification	No
Digital Asset Services	Records Management	Document Retirement	No
Business Analytical Services	Analysis and Statistics	Modeling	No
Business	Analysis and	Predictive	No

Analytical Services	Statistics			
Business Analytical Services	Analysis and Statistics	and	Simulation	No
Business Analytical Services	Analysis and Statistics	and	Mathematical	No
Business Analytical Services	Visualization		Graphing / Charting	No
Business Analytical Services	Visualization		Imagery	No
Business Analytical Services	Visualization		CAD	No
Business Analytical Services	Business Intelligence		Decision Support and Planning	No
Business Analytical Services	Business Intelligence		Data Mining	No
Back Office Services	Data Management		Data Exchange	No
Back Office Services	Data Management		Data Warehouse	No
Back Office Services	Data Management		Loading and Archiving	No
Back Office Services	Data Management		Data Recovery	No
Back Office Services	Financial Management		Payroll	No
Back Office Services	Financial Management		Auditing	No
Back Office Services	Financial Management		Financial Reporting	No

20.1.3.2 Relationship to Technology Component Model

Table 38

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access and Delivery	Access Channels	Web Browser	
Service Access and Delivery	Access Channels	Wireless / PDA	
Service Access and Delivery	Delivery Channels	Internet	
Service Access and Delivery	Delivery Channels	Intranet	
Service Access and Delivery	Delivery Channels	Extranet	
Service Access and Delivery	Delivery Channels	Peer to Peer (P2P)	
Service Access and Delivery	Delivery Channels	Virtual Private Network (VPN)	
Service Access and Delivery	Service Requirements	Legislative / Compliance	
Service Access and Delivery	Service Requirements	Authentication / Single Sign-on (SSO)	
Service Access and Delivery	Service Requirements	Hosting	
Service Access and Delivery	Service Transport	Supporting Services	Network
Service Access and Delivery	Service Transport	Test Management	
Service Access and Delivery	Service Transport	Modeling	
Service Infrastructure	Database / Storage	Database	
Service Infrastructure	Database / Storage	Storage	
Service Infrastructure	Hardware Infrastructure	Servers / Computers	
Service Infrastructure	Hardware	Embedded Technology	

Infrastructure	Infrastructure	Devices
Service Platform and Infrastructure	Hardware Infrastructure	/ Peripherals
Service Platform and Infrastructure	Hardware Infrastructure	/ Wide Area Network (WAN)
Service Platform and Infrastructure	Hardware Infrastructure	/ Local Area Network (LAN)
Service Platform and Infrastructure	Hardware Infrastructure	/ Network Devices / Standards
Service Platform and Infrastructure	Hardware Infrastructure	/ Video Conferencing
Component Framework	Security	Certificates / Digital Signature
Component Framework	Security	Supporting Security Services
Component Framework	Presentation Interface	/ Static Display
Component Framework	Presentation Interface	/ Dynamic / Server-Side Display
Component Framework	Presentation Interface	/ Content Rendering
Component Framework	Presentation Interface	/ Wireless / Mobile / Voice
Component Framework	Data Interchange	Data Transformation
Service Interface and Integration	Integration	Middleware
Service Interface and Integration	Integration	Enterprise Application Integration
Service Interface and Integration	Interoperability	Data Format / Classification
Service Interface and Integration	Interoperability	Data Types / Validation
Service Interface and Integration	Interoperability	Data Transformation
Service Interface and	Interface	Service Discovery

Integration

Service Interface and Interface Integration

Service Description / Interface

20.1.3.3 *Partnerships*

None.

20.1.4 Security and Privacy

20.1.4.1 *How is it provided and funded?*

IT security is provided by SFOC in accordance with NASA Policy, NPR 2810 and NPR 1620. The cost of IT security is fund by the Space Shuttle program.

20.1.4.2 *How is security accomplished?*

USA Information Management (IM) Functional Policy & Procedure (FPP) D-03-02, IT Security Risk Assessment & Planning, defines the risk assessment and security planning process. FPP D-03-05, IT Security Requirements, documents all NPR 2810.1 IT Security controls as-well-as other controls that are considered industry best practices. Each USA-managed government (NASA) system has a current security plan.

FPP D-03-05, IT Security Requirements, addresses the NIST 17 critical elements through 10 categories that contain a subset of the 17 critical elements. These 10 categories are: Continuity of Operations, Monitoring, Configuration Management, Physical, File Protection, Userid, Network, Security Program, Training, and Hazard Mitigation. These categories form the basis of the IT security risk assessment, required risk reduction/mitigation, and the subsequent security posture presentation to USA Facility/System Management (FSM), NASA Line Management, NASA Senior Management (with fiduciary responsibility for the system) and the NASA CIO required to obtain Authorization to Process (ATP) or accreditation of a system.

USA Information Management (IM) Functional Policy & Procedure (FPP) D-03-01, IT Security Accreditation, defines the accreditation process. All security plans are accredited in accordance with NPR 2810.1 and have current NASA Authorization to Process (ATP) documents signed by the NASA Director of Shuttle Processing and the KSC NASA IT Security Manager (IT) (KSC NASA Chief Information Office). LPS Accreditation dates are:

Critical / SMA Systems: CCMS – USA000395 (2/28/04), RPS USA000567 (8/31/03), CPCGOAL - USA001485 (9/30/03), CPCGOAL- Windows - USA008380 (3/31/04), SDC - USA001346 (4/30/04), SDC Lab – USA002416 (4/30/04), BASIS – USA006108 (11/30/03), COF – USA005039 (3/31/03), LON – USA005139 (11/30/03), LSDN – USA006884 (8/31/03),

and RSI – USA007976 (10/31/03).

General Support Systems: VSI – USA006252 (11/30/02).

IT Security incidents are handled and reported in accordance with FPP D-03-06, IT Security Incident Reporting. Incidents involving NASA IT resources are reported to the NASA Shuttle Processing Computer Security Manager and the KSC NASA ITSM/CIO. USA IT Security also maintains a 7x24 Incident Response Team (IRT) capability that allows all employees and subcontractors (as well as NASA) to report suspected IT Security incidents via a 1-888 # paging system.

Onsite. USA IT Security provides copies of all system security plans to NASA. USA IT Security provides system security posture presentations (obtained from the results of system IT security risk assessments) to the NASA Shuttle Processing Computer Security Manager, NASA Director of Shuttle Processing, and the KSC NASA ITSM/CIO in order to obtain NASA 's Authorization to Process (ATP) concurrence for each system.

20.1.4.3 *Effective use of security, controls and authentication tools*

There is no public access allowed to these systems. LPS systems process shuttle flight hardware for flight readiness and launch. No Privacy Act information is maintained on any LPS IT resources.

20.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

21 Kennedy Space Center (KSC) – Operational Television System Modernization

Project Description

The Space Shuttle program plays a vital role in enabling NASA's vision and mission. This includes advancing human exploration and providing safe access to space in support of human operations in low-earth orbit. In order to maintain a viable human transportation capability that will operate and support NASA's launch requirements, specific program investments are required. NASA is revamping its approach to selecting and managing these investments to ensure Shuttle operability into the next decade and avoid future project overruns. These investments will be consistent with NASA's strategy of ensuring the Space Shuttle remains viable until a new transportation system is operational. These projects will provide revitalization of the infrastructure, and combat obsolescence of vehicle, ground systems, and facilities.

The Operational Television System function is in the operational phase of the NASA Capital Planning and Investment Control (CPIC) process. OTV provides operational and safety situational awareness required by the KSC test team in support of Launch & Landing functions by being a second set of eyes or even being the only method of viewing hazardous or high energy activities in support of Shuttle Processing and Launch. OTV is funded and managed by the Shuttle Program. OTV allows us to meet strict safety of flight requirements. OTV is not a general-purpose television system. It is a closed network used for operations, launch and landing system.

The OTV Investment includes the acquisition of hardware and associated software required for the upgrade of the KSC Shuttle video system, which includes items such as cameras, lenses, recorders, monitors, routing switcher, control system(s), and video processing modules. The Investment also includes labor costs associated with design engineering, installation, testing, and training.

The capability provided by this investment mitigates risks, due to obsolescence of existing system elements that contribute to increased operations and maintenance (O&M) costs due to failure rate and repair/replacement costs. The obsolescence risk provides a threat to Shuttle processing schedules as the OTV system provides required surveillance of operations. This threat is also mitigated by this investment. Additionally, the new capability provided by this investment will meet the requirement from the NASA Inter-Center Photo Working Group (IPWG) for improving imaging quality through digital techniques that resulted from the Columbia Accident Investigation Board recommendations.

The FY04 information technology annual review/approval (Capital Planning and Investment Control process) for this investment was held September 26, 2003 by the Shuttle Program IT CPIC Review Board. The SSP Program Integration (PI) Information Technology (IT) plan is a part of the Space Flight Operations Contract (SFOC) overall annual Level A (5 year) and Level B (annual Fiscal Year) Information Technology Plan deliverables to the Space Shuttle Program (SSP) Chief Information Officer (CIO). FY04 Plans reviewed and approved in September 2004 by the SSP CIO with concurrence from the Johnson Space Center (JSC) CIO, Kennedy Space Center CIO and Marshall Space Flight Center CIO. The major IT expenses deal with either sustaining the above systems or migrating mainframe projects to a web-based, client-server environment using state of the art technology for data access, availability and transfer.

This investment is closely coupled with shuttle processing. The loss of this investment would require us to revert to manual based systems. This would increase our headcount and impact our processing schedule.

Architecture

21.1.1 Business

21.1.1.1 Process simplification/reengineering/design projects

None . The Project is currently in the mission operations phase. Organizational restructuring, training, and change management have been accomplished throughout the project’s life cycle.

21.1.1.2 Major organization restructuring, training and change management projects

None. The Project is currently in the mission operations phase. Organizational restructuring, training, and change management have been accomplished throughout the project’s life cycle.

21.1.2 Data

21.1.2.1 Types of Data

Used for viewing hazardous or high energy activities in support Shuttle Processing and Launch. OTV allows us to meet strict safety of flight requirements. OTV is not general-purpose television.

21.1.2.2 Existing Data Access

21.1.3 Application and Technology

21.1.3.1 Relationship to Service Component Model

Table 39

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Back Office Services	Development and Integration	Data Integration	No	
Back Office Services	Development and Integration	Instrumentation and Testing	No	

21.1.3.2 Relationship to Technology Component Model

Table 40

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Platform and Infrastructure	Hardware Infrastructure	/ Embedded Technology Devices	

21.1.3.3 Partnerships

None.

21.1.4 Security and Privacy

21.1.4.1 How is it provided and funded?

By the KSC Shuttle Processing Directorate as defined by the Project Manager. In FY2005 one percent of the OTV budget supports the IT security investment.

21.1.4.2 How is security accomplished?

The investment meets the security requirements by following NASA policy and guidance documents NPD and NPG 2810, adhering to updates from NIST guidelines and incorporating OMB polices as issued.

"The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures, when NIST completes this process NASA will revisit it's policy and procedures to conform with NIST new guidance."

Logs are reviewed daily, intrusion detection is run continuously, and the network is scanned quarterly for vulnerabilities. Information Technology Security (ITS) is implemented in accordance with NASA Procedures and Guidelines (NPG 2810.1), Security of Information Technology. For reporting, we use an approved Kennedy Process, KDP-KSC-P-1839. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. The NASA KSC Shuttle Processing OCSM has access to the USA policies and desk instructions. Access is also provided to security plans, risk assessments, incident response and audit data. The OCSM tracks and provides inputs into agency security requirements and contractor security modifications. The OCSM coordinates and integrates the Authority to Proceed for the ITSAA on KSC Shuttle Processing Systems. All security plans are approved by ITSAA. The OCSM coordinates the development and execution of the scanning of contractor resources located in Customer Owned & Maintain (COAM) networks. In addition the OCSM also assesses contractor's performance to NPG 2810, "IT Security Requirements" and to USA internal processes and procedures.

21.1.4.3 *Effective use of security, controls and authentication tools*

OTV does not allow public access.

21.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

22 Kennedy Space Center (KSC) – Shuttle Processing Support

Project Description

The Shuttle Processing Support investment is in the Control phase of the NASA Capital Planning and Investment Control (CPIC) process. Kennedy Space Center (KSC) still uses a significant portion of converted Apollo infrastructure, facilities and equipment for Shuttle Processing. The Launch Site Equipment (LSE) budget helps maintain this aged infrastructure, facilities and equipment with a current replacement value (CRV) in excess of \$3B. Space Flight Operations Contract (SFOC) and other contractors maintain current capability and replace equipment with similar equipment. The LSE's budget funds the major refurbishment of ground equipment and provides new capabilities when required. LSE projects typically involve redesigns driven by obsolescence problems or to correct problems necessary to "keep the doors open". Only summary data, a brief project description and Part II are provided. This investment is used to support Space Shuttle processing, launches, and landings. An example of the current FY year and FY 05 planned major investments include replacement of the Crawler Transporter Shoes, since the existing shoes are exhibiting extremely high failure rates and can no longer be utilized after 38 years of support.

The Shuttle Processing Support investment reduces lifecycle cost of maintenance replacement equipment. The requirements for lifecycle cost for maintenance replacement of obsolete Ground Support Equipment (GSE) only support funding if the lifecycle cost of the replacement GSE is less than the existing GSE.

The FY04 information technology annual review/approval (Capital Planning and Investment Control process) for this investment was held September 26, 2003 by the Shuttle Program IT CPIC Review Board. The SSP Program Integration (PI) Information Technology (IT) plan is a part of the Space Flight Operations Contract (SFOC) overall annual Level A (5 year) and Level B (annual Fiscal Year) Information Technology Plan deliverables to the Space Shuttle Program (SSP) Chief Information Officer (CIO). FY04 Plans reviewed and approved in September 2004 by the SSP CIO with concurrence from the Johnson Space Center (JSC) CIO, Kennedy Space Center CIO and Marshall Space Flight Center CIO. The major IT expenses deal with either sustaining the above systems or migrating mainframe projects to a web-based, client-server environment using state of the art technology for data access, availability and transfer.

This investment is closely coupled with shuttle processing. The loss of this investment would require us to revert to manual based systems. This would increase our headcount and impact our processing schedule.

Architecture

22.1.1 Business

22.1.1.1 *Process simplification/reengineering/design projects*

None . The Project is currently in the mission operations phase. Organizational restructuring, training, and change management have been accomplished throughout the project’s life cycle.

22.1.1.2 *Major organization restructuring, training and change management projects*

None. The Project is currently in the mission operations phase. Organizational restructuring, training, and change management have been accomplished throughout the project’s life cycle.

22.1.2 Data

22.1.2.1 *Types of Data*

In addition to Shuttle telemetry data there is various types of planning, processing, maintenance and other data related to the different Shuttle Processing support managed systems, networks and processes.

22.1.2.2 *Existing Data Access*

22.1.3 Application and Technology

22.1.3.1 *Relationship to Service Component Model*

Table 41

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Process Automation	Tracking and Process Tracking	Process Tracking	No	

Services	Workflow				
Process Automation Services	Tracking and Workflow	and	Case Management	/ Issue	No
Process Automation Services	Tracking and Workflow	and	Conflict Resolution		No
Process Automation Services	Routing and Scheduling	and	Inbound Correspondence Management		No
Process Automation Services	Routing and Scheduling	and	Outbound Correspondence Management		No
Process Automation Services	Management of Process		Change Management		No
Process Automation Services	Management of Process		Configuration Management		No
Process Automation Services	Management of Process		Requirements Management		No
Process Automation Services	Management of Process		Program Management	/ Project	No
Process Automation Services	Management of Process		Governance Management	/ Policy	No
Process Automation Services	Management of Process		Quality Management		No
Process Automation Services	Management of Process		Business Management	Rule	No
Process Automation Services	Management of Process		Risk Management		No
Process Automation Services	Organizational Management		Workgroup/Groupware		No

Process Automation Services	Organizational Management	Network Management	No
Process Automation Services	Investment Management	Strategic Planning and Mgmt	No
Process Automation Services	Investment Management	Portfolio Management	No
Process Automation Services	Investment Management	Performance Management	No
Process Automation Services	Supply Chain Management	Procurement	No
Process Automation Services	Supply Chain Management	Sourcing Management	No
Process Automation Services	Supply Chain Management	Catalog Management	No
Process Automation Services	Supply Chain Management	Ordering / Purchasing	No
Digital Asset Services	Content Management	Content Authoring	No
Digital Asset Services	Content Management	Content Review and Approval	No
Digital Asset Services	Content Management	Tagging and Aggregation	No
Digital Asset Services	Content Management	Content Publishing and Delivery	No
Digital Asset Services	Content Management	Syndication Management	No
Digital Asset Services	Document Management	Indexing	No
Digital Asset Services	Document Management	Document Imaging and OCR	No

Digital Asset Services	Document Management	Document Referencing	No
Digital Asset Services	Document Management	Document Revisions	No
Digital Asset Services	Document Management	Library / Storage	No
Digital Asset Services	Document Management	Document Review and Approval	No
Digital Asset Services	Document Management	Document Conversion	No
Digital Asset Services	Knowledge Management	Information Retrieval	No
Digital Asset Services	Knowledge Management	Information Mapping / Taxonomy	No
Digital Asset Services	Knowledge Management	Knowledge Discovery	No
Digital Asset Services	Knowledge Management	Knowledge Capture	No
Digital Asset Services	Knowledge Management	Knowledge Distribution and Delivery	No
Digital Asset Services	Knowledge Management	Knowledge Engineering	No
Digital Asset Services	Records Management	Record Linking / Association	No
Digital Asset Services	Records Management	Document Classification	No
Digital Asset Services	Records Management	Document Retirement	No
Digital Asset Services	Records Management	Digital Management Rights	No
Business Analytical Services	Analysis and Statistics	Modeling	No
Business Analytical Services	Analysis and Statistics	Predictive	No
Business	Analysis and	Simulation	No

Analytical Services	Statistics			
Business Analytical Services	Analysis Statistics	and	Mathematical	No
Business Analytical Services	Analysis Statistics	and	Structural / Thermal	No
Business Analytical Services	Analysis Statistics	and	Radiological	No
Business Analytical Services	Analysis Statistics	and	Forensics	No
Business Analytical Services	Visualization		Graphing / Charting	No
Business Analytical Services	Visualization		Imagery	No
Business Analytical Services	Visualization		Multimedia	No
Business Analytical Services	Visualization		Mapping / Geospatial / Elevation / GPS	No
Business Analytical Services	Visualization		CAD	No
Business Analytical Services	Business Intelligence		Demand Forecasting / Mgmt	No
Business Analytical Services	Business Intelligence		Balanced Scorecard	No
Business Analytical Services	Business Intelligence		Decision Support and Planning	No
Business Analytical	Business Intelligence		Data Mining	No

Services

22.1.3.2 Relationship to Technology Component Model

Table 42

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access and Delivery	Access Channels	Web Browser	
Service Access and Delivery	Access Channels	Wireless / PDA	
Service Access and Delivery	Access Channels	Collaboration Communication	
Service Access and Delivery	Access Channels	Other Electronic Channels	
Service Access and Delivery	Delivery Channels	Internet	
Service Access and Delivery	Delivery Channels	Intranet	
Service Access and Delivery	Delivery Channels	Extranet	
Service Access and Delivery	Delivery Channels	Peer to Peer (P2P)	
Service Access and Delivery	Delivery Channels	Virtual Private Network (VPN)	
Service Access and Delivery	Service Requirements	Legislative / Compliance	
Service Access and Delivery	Service Requirements	Authentication / Single Sign-on (SSO)	
Service Access and Delivery	Service Requirements	Hosting	
Service Access and Delivery	Service Transport	Supporting Services	Network
Service Access and Delivery	Service Transport	Test Management	
Service Access and Delivery	Service Transport	Modeling	

Service Platform and Infrastructure	Database / Storage	Database
Service Platform and Infrastructure	Database / Storage	Storage
Service Platform and Infrastructure	Hardware Infrastructure	/ Servers / Computers
Service Platform and Infrastructure	Hardware Infrastructure	/ Embedded Technology Devices
Service Platform and Infrastructure	Hardware Infrastructure	/ Peripherals
Service Platform and Infrastructure	Hardware Infrastructure	/ Wide Area Network (WAN)
Service Platform and Infrastructure	Hardware Infrastructure	/ Local Area Network (LAN)
Service Platform and Infrastructure	Hardware Infrastructure	/ Network Devices / Standards
Service Platform and Infrastructure	Hardware Infrastructure	/ Video Conferencing
Component Framework	Security	Certificates / Digital Signature
Component Framework	Security	Supporting Security Services
Component Framework	Presentation Interface	/ Static Display
Component Framework	Presentation Interface	/ Dynamic / Server-Side Display
Component Framework	Presentation Interface	/ Content Rendering
Component Framework	Presentation Interface	/ Wireless / Mobile / Voice
Component Framework	Data Interchange	Data Exchange
Service Interface and Integration	Integration	Middleware
Service Interface and Integration	Integration	Enterprise Application Integration

Service Interface and Interoperability Integration	Data Format / Classification
Service Interface and Interoperability Integration	Data Types / Validation
Service Interface and Interoperability Integration	Data Transformation
Service Interface and Interface Integration	Service Discovery
Service Interface and Interface Integration	Service Description / Interface

22.1.3.3 Partnerships

None.

22.1.4 Security and Privacy

22.1.4.1 How is it provided and funded?

In FY2005 two percent of the Shuttle Processing Support budget supports the IT security investment. USA Information Management (IM) Functional Policy & Procedure (FPP) D-03-02, IT Security Risk Assessment & Planning, defines the risk assessment and security planning process. Appendix A of the FPP documents all NPG 2810.1 IT Security controls as-well-as other controls that are considered industry best practices. Ground Operations contains numerous IT systems. Each USA-managed government provided system has a current security plan.

Critical systems [e.g., systems requiring Special Management Attention (SMA)] are assessed on a twelve – eighteen month cycle (depending on overall security posture) or upon significant change. General Support Systems (GSS) are assessed every three years or upon significant change. In addition, Annual Reviews of GSS Security Plans are conducted to ensure security documentation remains current. Note: All security plan dates are tracked by the last day of the month that the plan was signed.

Shuttle Processing Support Security plan dates are: KSC Complex Control System (KCCS) (8/30/03) and Surveillance Data Systems (9/28/01).

22.1.4.2 How is security accomplished?

The investment meets the security requirements by following NASA policy and guidance documents NPD and NPG 2810, adhering to updates from NIST guidelines and incorporating OMB polices as issued.

"The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures, when NIST completes this process NASA will revisit it's policy and procedures to conform with NIST new guidance."

Logs are reviewed daily, intrusion detection is run continuously, and the network is scanned quarterly for vulnerabilities. Information Technology Security (ITS) is implemented in accordance with NASA Procedures and Guidelines (NPG) 2810.1, Security of Information Technology. For reporting, we use an approved Kennedy Process, KDP-KSC-P-1839. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. "The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures, when NIST completes this process NASA will revisit it's policy and procedures to conform with NIST new guidance."

22.1.4.3 *Effective use of security, controls and authentication tools*

Shuttle Processing Support does not allow public access.

22.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000. The date of the most recent update to the agency GPEA plan, the 2003 progress update is provided below.

23 Langley Research Center (LaRC) – NASA Technology Transfer Systems (NTTS)

Project Description

The importance of technology transfer within NASA can be traced back to its establishing space act; Section 305 of the National Aeronautics and Space Act of 1958 (42 U.S.C. Sec. 2457), as amended, states that inventions, discoveries, improvements, and innovations made in the performance of any work there under, whether patentable or not, should be promptly reported to NASA. The objective of this requirement is to protect the Government's interest and to provide the widest practicable and appropriate dissemination, early utilization, expeditious development, and continued availability for the general public. The Agenda for Change, dated July 1994, was the Agency's blueprint for elevating the commercial technology mission to a fundamental NASA mission, important as any in the Agency. Each NASA program office and Center is responsible for incorporating new commercial technology business practices into their program management system and ensuring that their use is understood. The reporting of new technologies by NASA contractors during contract performance is a basic and vital element to achieving the goals of the Agenda for Change. NASA's Strategic Plan 2000 stated NASA mission was to advance and communicate scientific knowledge and also to transfer advanced aeronautics and space technologies. The technology transfer mission was also identified as part of the crosscutting processes of the Provide Aerospace Products and Capabilities and Communicate Knowledge. NPD 7120.4 further emphasized commercial technology planning within NASA's management system for programs and projects. To better solidify and clarify the Agency's technology transfer and commercialization activities the Agency issued, in March 2000, NPD 7500.2, NASA Technology Commercialization policy. NPD 7500.2 established NASA TechTracS (TTS) as the agency wide technology transfer and commercialization information system and designated the Associate Administrator for the Office of Aero-Space Technology (OAT) responsible for developing and maintaining TTS. In December 2001, NPG 7500.1 established NASA's Technology Commercialization process. In addition to the noted policies that have directly resulted in the creation of the NASA Technology Transfer Systems (NTTS), there are numerous laws and congressional findings, Federal Regulations, and other NASA policies which are supported in some degree by NTTS. See the NTTS Project Plan for more information on the customer base and supported processes.

As – Is

NTTS supports the entire technology transfer process and is the Agency's one system with all of its technological assets. NTTS is a closely integrated set of information systems. The four major components comprising NTTS are as follows and are shown in Figure 1.

- **eNTRe**—the **electronic new technology reporting** system provides a tool for electronically capturing and submitting new technology reports.
- **TechTracS (TTS)**—this center-based component of NTTS provides the day-to-day core backbone of the NTTS while providing each center a major productivity tool for accomplishing its technology transfer activities;
- **KIMS**—the **Knowledge Integration and Management System** provides NASA enterprise, center and program managers up to date information on the technology transfer status of their activities.
- **TechFinder**—this is the public technology transfer gateway; providing access to NASA's technology assets.

Figure 1, U.S. Public

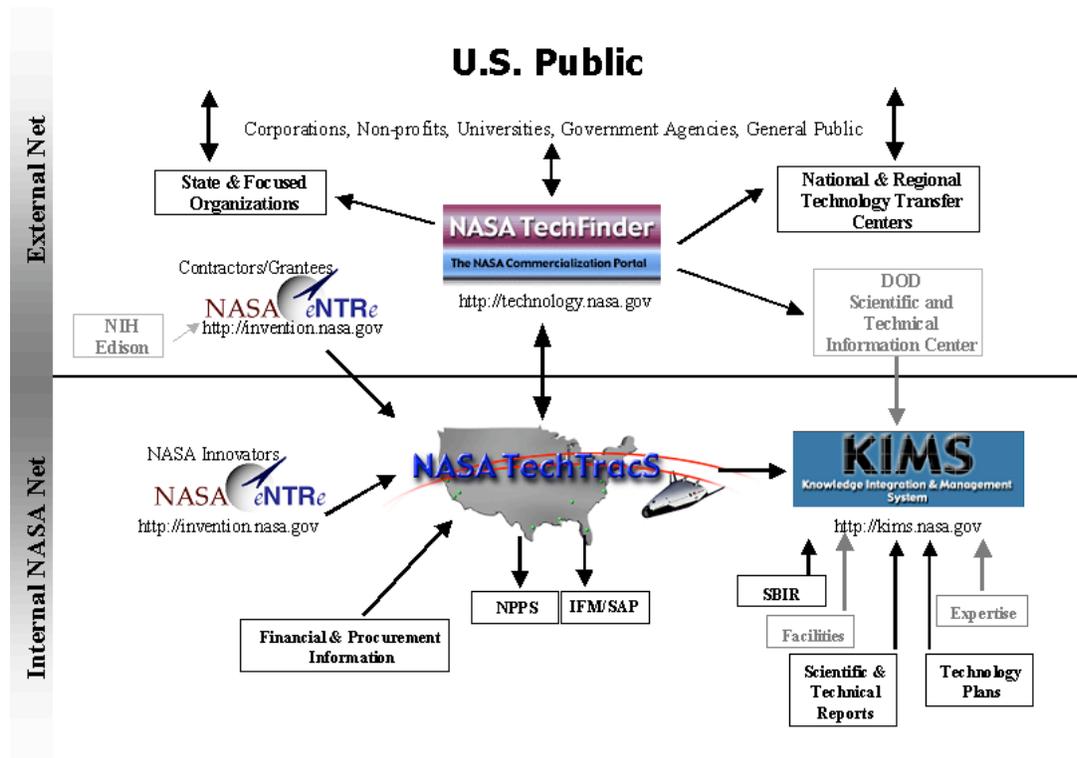


Figure 1 also illustrates that the NTTS is not a stand-alone, isolated system but rather there is integration of data from other existing NASA data repositories where such data is directly applicable to and supportive of NASA’s overall technology transfer mission. Such an approach leverages other key NASA information assets while facilitating a single interface point for the external commercial technology community; as well as a key asset for NASA internal scientists, researchers, engineers and technologists.

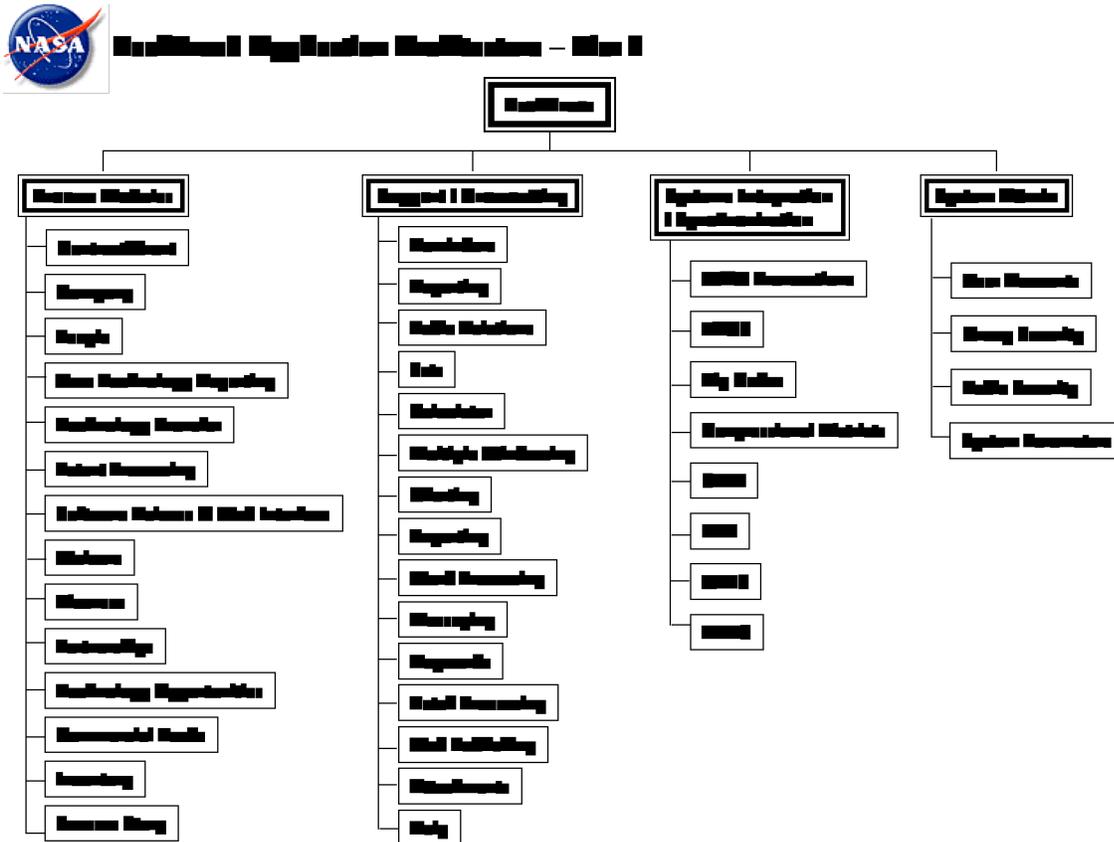
Systems Description and Operational Concept

The NTTS application architecture (Figure 2) below shows the key application components (eNTRe, TechTracS, KIMS, TechFinder, and NTTS Support) and the first level application modules.

- Contract/Grant Module
- Inventory Module
- NTR Module
- Patent Module
- Waiver Module
- Commercial Leads Module
- License Module
- Partnership Module
- TOPS Module
- People Module
- Success Story Module
- Software Release Module

In total there are over 100 tables and 2000 data fields in the standard TTS core. Figure 3 provides the TTS Application Architecture.

Figure 3, TechTracS Application Architecture



Each Centers' TTS updates the agency-wide TTS server with selected data. Each Center has control over which records are transmitted to the agency-wide system. There are certain areas in each Centers' TTS where no data is provided to the agency-wide system. Technology commercialization metrics are calculated locally on each Center's TTS and then submitted to the Agency-wide TTS. An estimated 9 million transactions annually are automatically executed throughout the network between the Centers' TTS and the agency-wide TTS. Monthly synchronization procedures ensure information is concurrent across the Agency.

23.1.3 KIMS

KIMS provides NASA program and project managers' real time status of technology transfer related activities and standard monthly metric reports. For the researcher or technologist, KIMS provides search access to all of NASA's technologies, technology producers, and technology partnerships. KIMS consists of the following key technical components.

- Knowledge Grid
- MapIt
- Commercial Assessment
- Searching

- Metrics Reporting / Charting
- Help
- Feature Request/Bug Reporting
- Account Administration

KIMS provides data from either an Enterprise perspective or a Center perspective. In either the Enterprise or Center view, data is available at the program level.

23.1.4 TechFinder

TechFinder is the public commercial technology portal providing public access to NASA's technological assets, technology activities, and technology transfer success stories. Key features include quick links to NASA's technologies available for licensing and software technologies, simple and advanced searching, GIS mapping, customer inquiry processing and E-mail notification on new technologies.

NTTS Support

User and Technical documentation, a bug/feature on-line request system, and Project Status are maintained on <http://ncis.nasa.gov> located on the NTTS Support system. Additionally the NTTS mail server and KIMS datapump applications reside on NTTS Support.

23.1.5 NASA Interfaces

NTTS interfaces with several other NASA systems (ONS). Table 1 below provides the system name, expected data flow, and frequency. Further information on what fields are transmitted between the systems can be found in the documentation section of <http://ncis.nasa.gov>.

Table 43, NTTS Interfaces to Other NASA Systems

Other NASA System	Data Flow	Frequency
Technology Inventory	Meta-data Input to NTTS Search Results Output	Annual Input Real-time Output
ERASMUS	Selected Data Input to NTTS Detail Record Updates	Quarterly
SBIR	Meta-data Input to NTTS Search Results Output Detail Record Updates	Quarterly
IFMP	Selected Data Output to ONS	Biweekly
STI	Meta-data Input to NTTS Search Results Output	Annual Input Real-time Output
MFI	Meta-data Input to NTTS Search Results Output	Annual Input Real-time Output
HQ FACS	Selected Data Input to NTTS Detail Record Updates	Monthly
NPPS	Selected Data Output to ONS	Biweekly
Center Web Sites	Selected Data Output to ONS Web Page Output to ONS	Real-time

23.1.6 External Interfaces

Table 44 provides the NTTS interfaces with external entities.

Table 44, External Interfaces

Entity	Data Flow	Frequency
Annual Department of Commerce Metrics	Output Report to DOC	Annual
External data source – maps & zip codes/Congressional districts	Input Data to NTTS	Weekly
DTIC	Output Data to DTIC	As Requested
AIAA	Output Data to Public Server	Monthly

Production Network Diagram

The NTTS technology architecture is the physical configuration, network, hardware, and software components that enable the NTTS application architecture. Several COTS products are integrated together to respond to the defined requirements. Relational database technology is used due to its logical approach to information storage that matches with a user's perception of information and its controlled redundancy that supports relations of many to one and simplifies data manipulation logic. Two relational database systems are used in NTTS; 4th Dimension (4D) and MS SQL Server. Both systems support industry standards and are ODBC compliant. In addition to the database engine, 4D provides a family of products that are an integral part of the NTTS operational capabilities.

MS SQL Server is used as the database engine for KIMS. A new application was developed to allow real-time data exchange of information between TTS and KIMS; DataPump. The DataPump employs both database engines' compatible features in its processing.

There are several web sites in NTTS that are supported by the database engines in conjunction with two web applications; Cold Fusion and NetLink. Web services are provided using Apache and Netscape. Centralized secured file sharing services are provided using Webdav.

NTTS is compatible with both PC's running Windows 98, NT, or 2000 and Macintosh systems running MacOS 9.x or higher. Refer to NTTS_System_Requirements located on <http://ncis.nasa.gov> for the most recent recommended machine configurations.

NTTS is a distributed system with physical locations at each NASA Center. Each Center has a 4D database server and an intelligent background processor that facilitates the real time synchronization between the Center systems and the Agency systems. All agency systems are located at Langley Research Center.

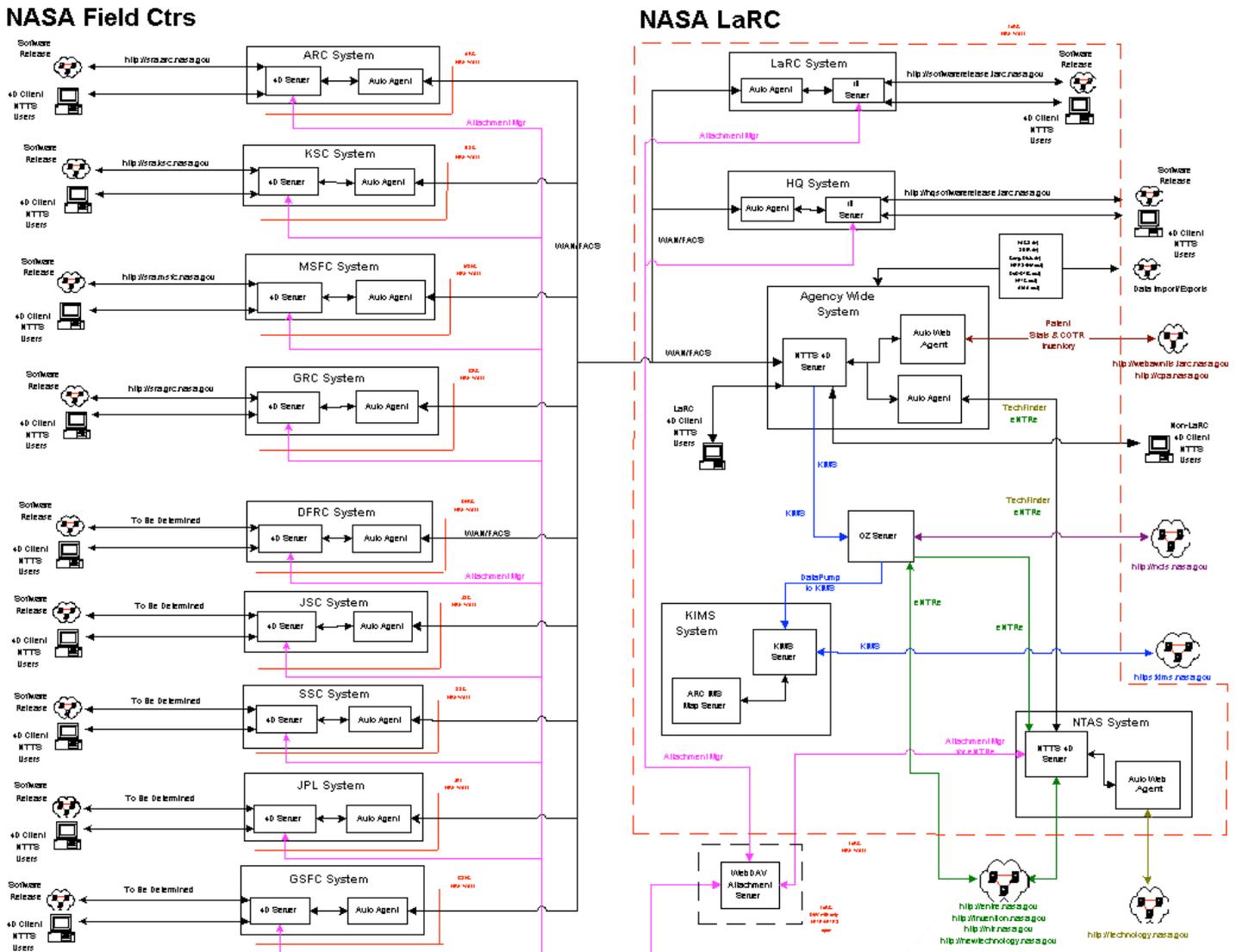
The NTTS network utilizes the public network, NISN, and center virtual private networks (VPN). NASA users within Centers use Center internal networks for connection to local servers

and NISSN for connection to the agency systems. NASA users outside centers and the technical support team use identified center VPN's and the public network for connection to NTTS. Users on NASA funded agreements use the public network and secure socket layer.

Figure 4 provides an overview of the NTTS system components, NTTS application components, web sites, information flow and physical location.

See System_Architecture on <http://ncis.nasa.gov> under documentation for higher resolution image.

Figure 4, NTTS Systems Architecture



Systems and Support

The management, configuration and support for NTTS are performed as defined in the NTTS Project Plan. The Project is managed out of the Program Development and Management Office at Langley Research Center. The owning organizations are the Innovative Technology Transfer Partnerships Theme within OAT and the Patent Counsel within the Office of the Chief Counsel at NASA HQ.

Support for NTTS is acquired through the NTTS Technical Support Contract, currently NAS1-00113, by ODIN, by the Langley CONITS contract, and by each Centers' IT support contracts.

Facilities

The NTTS systems located at Langley are located in room 140 in building 1229 and in ODIN server room(s) in building 1268. Standard Langley network and phone systems are used. Rooms containing NTTS systems have restricted card key access. Locations of systems at other Centers follow the guidelines provided in the NTTS Operation Guidelines. The NTTS test environment is located at the NTTS Technical Support Contractor's site.

Technology Flashpoints

The current NTTS configuration and architecture is one that has resulted from an evolutionary path reflective of the growth of NASA's Technology Transfer Program. To support the program's rapid evolution, NTTS development employed a prototyping and refinement development cycle. Formal requirements analysis and implementation processes have been used in the development of NTTS. Activities defined in the NTTS Project Plan will ensure NTTS, as a system, is configured for sustained operations, NTTS risks are managed, and will align the NTTS architecture, where possible, with the defined NASA Enterprise Architecture and IT security policies. To achieve the goal of the plan activities, new technologies and centralized configurations will be examined and incorporate into the application and architectural configurations. See the NTTS Project Plan, Thrusts 2 and 3 for more information.

Compliance

As presented in the Introduction, there are several NASA policies, legislation, and federal regulations supported by NTTS. Table 3 provides a list of the guiding items with which NTTS complies and therefore supports NASA's compliance with listed items.

Table 45, NASA Policies, Legislation, Federal Regulations Supported by NTTS by Element

*** Denotes element was specifically designed to support noted policy.**

Identifier	Title	NTTS Element
NPD 1000.1B	NASA Strategic Plan	Tech Finder* KIMS
NPG 1000.2	NASA Strategic Management Handbook	Tech Finder* KIMS*
NPD 1050.1F	Authority to Enter Into a Space Act	TechTracS
NPD 1050.1	Space Act Agreements	TechTracS
NPD 1080.1	Generate Knowledge (GK) Process	Tech Finder* KIMS* TechTracS
NPD 1440.6	NASA Records Management	TechTracS*

NPD 2091.1	Government Employee-Created Software	TechTracS* ENTRe*
NPD/G 2092.1	Royalties And Other Payments Received By NASA From The Licensing Of Patents And Patent Applications	TechTracS*
NPD 2110.1E	Foreign Access to NASA Technology Transfer Material	TechFinder KIMS TechTracS*
NPD 2190.1	NASA Export Control Program	TechTracS
NPG 2200.2A	Guidelines for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information (STI)	KIMS
NPD/G 2210.1A	External Release of NASA Software	TechFinder* KIMS TechTracS*
NPD 2220.5E	Management of NASA Scientific and Technical Information (STI)	KIMS
NPD/G 2800.1	Managing Information Technology	TechFinder KIMS TechTracS eNTRe
NPD/G 2810.1	Security of Information Technology	TechFinder KIMS TechTracS eNTRe
NPD 2820.1	NASA Software Policies	TechFinder KIMS TechTracS eNTRe
NPG 3451.1	NASA Awards and Recognition Program	TechTracS*
NPD 7120.4B	Program/Project Management	KIMS*

		eNTRe*
NPG 7120.5B	NASA Program and Project Management Processes and Requirements	KIMS* eNTRe*
NPD 7500.2	NASA Technology Commercialization Policy	TechFinder* KIMS* TechTracS* eNTRe*
NPG 7500.1	NASA Technology Commercialization Process	TechFinder* KIMS* TechTracS* eNTRe*
Public Law 85-568	National Aeronautics and Space Act of 1958	TechFinder KIMS TechTracS eNTRe
Public Law 96-480	Stevenson-Wydler Technology Innovation Act of 1980	TechFinder KIMS TechTracS eNTRe
Public Law 96-517	Bayh-Dole Act of 1980	TechFinder KIMS TechTracS eNTRe
Public Law 99-502	Federal Technology Transfer Act of 1986	TechFinder KIMS TechTracS eNTRe
Public Law 101-189	National Competitiveness Technology Transfer Act of 1989	TechFinder KIMS TechTracS

		eNTRe
P.L. 102-245	American Technology Preeminence Act of 1991	TechFinder KIMS TechTracS eNTRe
Public Law 104-113	National Technology Transfer and Advancement Act of 1995	TechFinder KIMS TechTracS eNTRe
Public Law 106-404	Technology Transfer Commercialization Act of 2000	TechFinder KIMS TechTracS eNTRe
FAR	Government Agencies must monitor and enforce small entity contractor's reporting and use of inventions.	TechTracS eNTRe
FAR	To protect the Government's interest and the public's investment, Agencies shall maintain appropriate follow-up procedures.	TechTracS eNTRe
FAR	NASA contracts with large businesses require prompt reporting of inventions, discoveries and innovations.	TechTracS eNTRe
14 CFR 1240	Inventions And Contributions	TechTracS*

Capabilities

In support of the functional requirements NTTS has a set of operational requirements ranging from user reminders to dynamic web page publishing. Operational requirements are divided into two types; user and administrative. User operations provide the user with automated capabilities that have been developed with a specific understanding of how the user routinely processes information. These operational processes free the user from performing routine, repetitive tasks. This, in turn, allows the Technology Transfer (TTO) and Patent Counsel (PCO) Offices to focus on managing and utilizing information rather than generating information. User Operations consists of the following capabilities.

Reminders – A large percentage of the information processed by the TTO and the PCO results in a related action, immediate or future. NTTS responds to information entered by the user with E-mail notifications, action items, and/or chronology entries. The reminder module in NTTS is very robust and approaches being a mini-programming interface, in that, it provides the user with the capability to build custom reminders incorporating several conditions across multiple tables. There is virtually no step in the technology transfer process in which the reminders cannot provide benefit.

Calculator – As defined by NPG 7500, the dollar value of activities are an integral part of the commercialization metrics. The statistics calculator provides the user a quick calculator capability on any numeric field in the database.

Reports – NTTS has two report capabilities; predefined and adhoc, that can include any field in the database and span across related tables. In both areas, the reporting features support user customization, formulas, and database field merging. Reports can be printed or saved to disk in a variety of formats.

Table Relations – NTTS is a relational database supporting an unlimited number of relation levels. Both the user screen interface and the reporting tools provide easy processing for moving across related tables and displaying related information.

Sets – NTTS uses the database's powerful Sets feature. Sets offer users swift means for manipulating record selections. In addition to the ability to create sets, relate them to the current selection, and store, load, and clear sets, this feature offers three standard set operations: Intersection, Union, and Difference.

Multiple Windowing – Routinely users need to view information from a number of processes and NTTS supports this by supporting an unlimited windowing capability.

User Home – Each user of NTTS can save a set of personal preferences that allow user customization of how the tools operate. One of these preferences is the ability to set which table and set of information will be displayed at initial login and whenever the Home button is pressed. Since users of the system are routinely working with the set of activities to which they are assigned, this intelligent startup process allows the user to easily begin work upon login.

Word Processing – NTTS provides an enhanced set of word processing features that supports the offices' letter and report generation. Information from the database can be merged into documents. In some instances, documents are automatically generated in response to an action a user takes. NTTS is designed to allow the user to review the document before final delivery is completed.

Charting – NTTS provides the user with bar and pie charting capabilities using data directly from the database. Charts produced can be integrated into presentations produced by other applications.

Web Publishing – The web interfaces in NTTS range from the reporting on patent statistics to COTR commercial potential assessment to marketing and information dissemination. Web pages

are built real-time directly from the database. Part of NASA's collaboration with its technology transfer partners, TechFinder is designed to pass information on visitor registration directly to the supporting partner.

Attachments – Using WebDav and web linking technology, NTTS supports attachment of related documents to any record in the database.

Messaging – NTTS employs a dual type user messaging service; messages of the day and E-mails. A table driven daily message delivers information to users at login and on user request. Using the features of the reminder module E-mail messages can be sent to anyone in the people table.

Keywords – Searching by keywords is available in NTTS modules and interfaces. Keywords are created in three ways;

System generated - an algorithm is activated on information entry

User generated – users can add, delete, or modify any keyword

Multiple words - users can create keywords and save them on multiple records.

Administrative Operations provide Centers the capability to tailor the user environment to meet a Center's unique requirements; automates the exchange of information between the Centers and the Agency or external systems to the point of real-time delivery of information; and provides both a test environment and support website.

Administrative Operations consists of the following capabilities.

Batch Processing – Each center server has a companion machine, the Auto Agent, which processes reminders, auto-generated letters, wide area networking transmissions, and batch/background printing.

Synchronization Module – Using the Auto Agent, Centers' information is sent real-time to the Agency and public systems.

Security – Security is provided in several layers and configurations. Secure Socket Layer is employed for secure web transmission. Each user account can be configured for table access of read-write, read-only, and no access. Additional permission to delete can be activated. Field level security is attained by employing views. Refer to the NTTS Security Plan for more detail.

Monthly / End of Year Processing – Each month financial, procurement, and programmatic is loaded and metric reports are produced for each Center and the Agency. At the end of each fiscal year, close-out processing is performed.

Test Environment – A duplicate test/training version of NTTS is maintained to support NASA's review of new software versions and user training.

Support Website – SupportBase (<http://ncis.nasa.gov>) provides technical and user documentation of NTTS, a bug/feature reporting capability, work status, and a modification request system. This is NASA's on-line support site for NTTS.

To - Be Condition

As described in the Technology Flashpoints, activities defined in the NTTS Project Plan will ensure NTTS, as a system, is configured for sustained operations, NTTS risks are managed, and will align the NTTS architecture, where possible, with the defined NASA Enterprise Architecture and IT security policies.

24 Marshall Space Flight Center (MSFC) – Payload Operations and Integration Center

Project Description

The Payload Operations Integration Center (POIC), located within the Huntsville Operations Support Center (HOSC) at Marshall Space Flight Center, is the primary single NASA ground system responsible for integrated operational payload flight control and planning for the International Space Station program supporting the Biological and Physical Research and Space Flight Enterprises. The POIC is in the Operations phase of the NASA IT Capital Planning and Investment Control (CPIC) process, and this IT investment is managed as a component of the International Space Station Program under NASA's NPG 7120 process. Per NASA agreement with OMB - NASA Mission Specific major investments are reported in an abbreviated format. Only summary data, a brief project description and Part II are provided.

The POIC provides payload telemetry processing, command uplink, and planning capabilities for a large number of local POIC Cadre flight controllers and remote ISS payload users/customers and other facilities located throughout the world. Additionally, the Telescience Resource Kit (TReK) software is provided to remote customers in order to simplify interaction with the ISS vehicle and the POIC information systems. POIC software is provided to other NASA centers and customers including: the Kennedy Space Center (KSC) (which utilizes a copy of the POIC software within the Payload Test and Checkout System (PTCS)); and a multitude of ISS payload customers using TReK software.

The POIC integrates/controls: ISS payload flight operations, simulation, and mission-test preparation activities. ISS core systems and payload telemetry data is received, processed, stored, retrieved, displayed, and distributed to local and remote payload users/controllers. The POIC provides the capability to receive commands from local and remote users, analyze the uplinks for authenticity/authorization, performs required hazardous command checks, transmit the commands to the ISS (via the Mission Control Center-Houston (MCC-H)), and log all the command system activities for analysis/ troubleshooting purposes. The POIC provides the capability to uplink/downlink files to/from the ISS and store/retrieve mission-related documents, procedures, and files. The POIC also provides the integration point for planning all ISS payload operations by: assessing/integrating user operational requirements, analyzing available on-orbit and ground resources, and generating detailed execution timelines scheduling the user operations in a safe and efficient manner.

Architecture

24.1.1 Business

24.1.1.1 *Process simplification/reengineering/design projects*

The International Space Station Program Office and NASA headquarters approval of the POIC project predates an Agency EA Review committee. However, all Agency programs and projects are reviewed and approved through an established Agency process that ensures that all new endeavors are consistent with the current Agency and Organizational mission, vision, and strategic plans.

24.1.1.2 *Major organization restructuring, training and change management projects*

Activities are underway to reengineer the systems within the POIC to lower the long-term recurring operations and maintenance costs of the systems, including the: Payload Data Services System (PDSS) Redesign, ISS Downlink Enhancement Architecture, POIC UNIX Workstation to Microsoft Windows 2000 Intel PC Platform Migration and POIC Server Architecture Redesign/Consolidation to Linux/Intel Servers.

24.1.2 Data

24.1.2.1 *Types of Data*

The following types of human spaceflight vehicle and payload/experiment data are used in this project:

- ISS Flight Science/Payload and Core Systems Telemetry
- Space Shuttle Orbiter Telemetry
- ISS Flight Payload/Core Systems Command & Control Uplink/Downlink Data/Files
- ISS Flight Mission Operations Documentation/Procedures Files
- ISS Flight Mission Payload Planning/Trajectory Data Files/Products
- ISS Flight Mission Operations Voice and Video
- Tracking and Data Relay Satellite (TDRS) System (TDRSS) Performance/Quality Data
- Simulation and Test Data (associated with previously mentioned items)

24.1.2.2 *Existing Data Access*

24.1.3 Application and Technology

24.1.3.1 Relationship to Service Component Model

Table 46

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
				<p>The POIC aligns with the Service Component Reference Model via the Digital Asset Service, Business Analytical Service, Back Office Service and Process Automation Service Domains. For the Digital Asset Service Domain the Knowledge Management Type applies to and includes the following components: Information Retrieval, Information Sharing, Knowledge Engineering, Knowledge Capture and Knowledge Distribution and Delivery. For example, the POIC provides all command, control, telemetry processing, information management systems, payload planning systems, voice/video systems, remote-user "Telescience" systems, and facilities support infrastructure for operation of ISS payloads and payload support systems. The POIC provides direct and service-unique support functions for all local POIC Cadre flight controllers, remote Principal Investigator (PI) teams/sites, NASA Telescience Support Center (TSC's), and International Partner (IP) payload ground facilities located throughout the world. For the Back Office Service Domain, the Data Management Type applies to and includes the following components: Data Exchange, Data Warehouse, Meta Data Management, Data Cleansing and Extraction and Transformation. For example, the POIC provides for the storage, using integrated Storage Area Network (SAN)/Network Attached Storage (NAS), and retrieval of mission science data for up to 2 years, during which time the data is made available to the scientific payload user community for long-term storage and archival. In addition for the Business Analytical</p>

Services Domain, Analysis and Statistics, Reporting and Visualization Types (including the Mathematical, Ad Hoc and Graphing/Charting components); capabilities are provided for the real-time processing, non-real-time analysis, display/visualization, and output reporting of mission telemetry data to local and remote payload users. For the Process Automation Service Domain, the Tracking and Workflow Type applies including the Process Tracking component; which is utilized within the Payload Information Management System (PIMS) for the automation of real-time flight mission operations change requests submitted by payload users for subsequent evaluation/approval and implementation.

24.1.3.2 Relationship to Technology Component Model

Table 47

Service Area	Service Category	Service Standard	Relation to SRM of FEA
			<p>The overall POIC data systems infrastructure is diverse and based upon multiple standards/technologies including the following items noted in the Technical Reference Model (TRM). Examples of the alignment of the POIC data systems with the Technical Reference Model are as follows:</p> <p>Service Access and Delivery, Access Channel, Web Browser: Internet Explorer, Netscape Navigator Service Access and Delivery, Access Channel, Collaboration Communications: Electronic Mail, Fax Service Access and Delivery, Access Channel, Other Electronic Channels: System to System, Web Service, URL Service Access and Delivery, Delivery Channels: Internet, Intranet, Extranet, Virtual Private Network (VPN) Service Access and Delivery, Service Requirements, Legislative/Compliance: Section 508, Web Content Accessibility, Security Service Access and Delivery, Service Requirements: Authentication/Single Sign-on</p>

**Service Access and Delivery, Service Requirements,
Hosting: Internal (within Agency)
Service Access and Delivery, Service Transport,
Supporting Network Services: IMAP/POP3, MIME,
SMTP, T.120, H.323, SNMP, LDAP, DHCP, DNS, BGP,
X.400
Service Access and Delivery, Service Transport,
Service Transport: TCP, IP, HTTP, HTTPS, FTP, IPSEC**

24.1.3.3 Partnerships

24.1.4 Security and Privacy

24.1.4.1 How is it provided and funded?

The International Space Station program office provides security funding for this project as part of the overall integrated POIC funding.

The POIC implements management, technical systems, and operational controls necessary to fulfill and execute the security guidelines specified within NPD 2810.1, “NASA Policy Directive for the Security of Information Technology”, and NPG 2810.1, “NASA Procedures and Guidance for the Security of Information Technology”, in addition to other ISS program unique requirements.

Assigned Marshall Space Flight Center (MSFC) Flight Project Directorate (FPD) civil service and POIC contractor staff personnel have been designated to actively manage the security activities of the POIC. An ongoing security risk management process is in place within the POIC. All systems in development and/or operations are routinely reviewed during the product life cycle to determine the threats posed by an implementation and/or external threats potentially/actually encountered. Before a new system is brought online a detailed security risk assessment is performed, in addition to detailed testing of the security features of the architecture. A new system is only authorized to process data after this certification and accreditation has been achieved. An IT Security Plan, identifying the security features and risks associated with a system, is maintained for each system and is updated annually.

Technical system oriented high-level requirements flow down into detailed requirements and system specifications for implementation. A controlled software development process is in place by the contractor for custom-developed application software. System features (including security) to be implemented in COTS hardware and software products require a detailed technical assessment/ evaluation before incorporation into the architecture; with subsequent configuration managed baseline versions delivered for use. The final integrated architecture is then verified and validated against all requirements and operational conditions before it is certified for operations.

Operational controls are in place for security requirements implemented in personnel, processes and/or procedures. Key personnel within the organization critical to the security and operations of the systems are trained and certified. Training includes: general security awareness, COTS & contractor-developed product usage and security features, industry best-practices information, risk management techniques, threat prevention/control, etc. Specific contractor personnel are responsible for: network security, operating system/COTS tool security, application development, and testing activities enforcing security/access controls, security operational procedures, and documentation.

24.1.4.2 *How is security accomplished?*

The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures Guide. This NPG employs standards guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures, when NIST completes this process NASA will revisit its policy and procedures to conform with NIST new guidance.

The POIC contractor is responsible for reviewing, implementing (when necessary), and responding to all NASIRC/CERT security alerts and vulnerability patches through the NASA civil service IT Computer Security Official. The NASA civil service IT Computer Security Official is responsible for coordinating back the response of these activities to Marshall Space Flight Center (MSFC) level computer security personnel; who subsequently coordinate these activities with other NASA centers, NASA headquarters, and the DHS' FedCIRC. The contractor routinely reviews security audit logs along with other monitoring methods associated with intrusion detection (in firewalls, routers, servers, desktop platforms, etc.) for security related incidents. Any identified incidents/attacks observed are immediately reported to the NASA civil service IT Computer Security Official for subsequent reporting up to the FedCIRC. For real-time ISS mission support, the POIC also works with NASA Integrated Services Network (NISN), Mission Control Center-Houston (MCC-H), International Partner (IP), and U.S. remote payload site personnel in the isolation, control, and elimination of unauthorized external access attempts to the ISS mission support ground and flight systems. All incidents are reported to DHS' Fed CIRC.

The system is operated by contractors. All contracts include specific security requirements required by law and policy. The contractor is required to comply with MSFC-RQMT-2467 for all IT systems supported under the contract. MSFC-RQMT-2467 identifies detailed system/personnel requirements and guidelines compatible with the NASA IT Security procedures and guidelines (NPG 2810.1); which are derived from NIST guidelines and OMB policies. The NASA civil service IT Computer Security Official for the POIC coordinates with the contractor-designated equivalent IT computer security representative to insure the contractor meets the relevant computer security procedures and guidelines. These personnel are responsible for insuring that the information systems within the POIC are maintained current with NASIRC/CERT alerts and vulnerability patches for all affected systems; with associated metrics

generated. In addition these IT computer security officials must review and approve all routine system configuration changes, new engineering/software design modifications, new systems/software under evaluation, user account/access changes/additions, and updated facility operational procedures/documentation affecting security, etc. The POIC maintains an IT Security Plan for each of the individual subsystems.

24.1.4.3 *Effective use of security, controls and authentication tools*

No access is provided to POIC systems to promote or permit public access. The only access to POIC systems is for specific ISS payload flight operations usage.

However, POIC does provide the capability for authorized users to connect via open networks (such as Abilene/Internet 2), for which NASA/POIC has no inherent control. To protect the POIC and the ISS in the usage of these open networks, the POIC utilizes/enforces VPN technology for encrypted authenticated access with requisite user ID/password login requirements. Routers and firewalls have also been setup to deny access unless specifically authorized by POIC security personnel previously (for designated external IP addresses and protocols accessing specific POIC information system services).

In addition the POIC is inherently designed to only allow user access to authorized products and services; through unique user accounts with specific configuration-controlled pre-defined privileges/settings. These configurations can be modified in real-time if necessary. The design also supports the fundamental ISS program concept of the originating payload being responsible for end-to-end data encryption if extreme customer concerns exist about data protection (e.g. privacy act, company proprietary, etc.).

24.1.5 Government Paperwork Elimination Act

This system does not support transactions or record keeping covered by GPEA. The POIC does not handle electronic transactions or record-keeping information covered by GPEA. For reference only: the initial NASA Agency- wide GPEA plan was delivered on 10/31/2000. The date of the most recent update to the agency GPEA plan, the 2003 progress update is provided below.

25 NASA Enterprise Architecture

Project Description

NASA plans to evolve its EA program over the next five years – FY06 to FY10. It builds on the NASA EA Version 2.3 completed in July 2004.

The NASA EA is a strategic tool that links NASA's mission, business and Information Technology (IT) strategies. The architecture provides the fundamental methodology and

framework for defining how NASA's IT will be implemented and managed. Key elements of the architecture include a description of the current "as-is" state and a projection of the "to-be" state, a clear governance model, a Capital Planning and Investment process, and Information Technology service delivery models.

The NASA EA focuses on leveraging the Agency's investment in legacy systems and driving the design on our emerging systems. The EA leverages existing systems that NASA has in place, built separately by Centers and Programs over several decades. The NASA EA and the associated reference models mold those systems into an integrated or federated infrastructure aligned with the Agency's mission and business needs.

The NASA EA provides a mission driven approach to designing and implementing, partnering, or procuring new information technology systems and services. The true value of EA is achieved when the architecture increases NASA's ability to deliver on our core missions. The NASA information technology systems and the EA exist to support the vision presented in the NASA Strategic Plan and the three core missions and ten major goals of the Agency.

NASA's EA must support the unique science and research and technology missions of the agency and the business processes and general-purpose infrastructure required to support the Agency's operations. The NASA EA is structured into three major service component areas: Office Automation, IT infrastructure, and Telecommunications (OAIT), Multi-Program/Project IT, and Program Unique IT. This structure allows the Agency to group items based on how they support NASA achieving our overall strategic missions.

Architecture

25.1.1 Business

25.1.1.1 *Process simplification/reengineering/design projects*

The NASA Enterprise Architecture is structured into three major service component areas:

- (1) Office Automation, IT infrastructure, and Telecommunications (OAIT) This category includes Office Automation investments that provide general purpose computing (e.g. email, desktops, helpdesk services) for both civil servants and contractor personnel, regardless of the program or project supported or fund source. Nine portfolios (Voice, WAN, LAN, Video, Desktop Hardware/Software, Data Centers, Application Services, Messaging and Collaboration, and Public Web) have been defined across three major service areas (Communications, Computing, and Electronic Work Environment.)
- (2) Multi-Program/Project IT is defined as IT infrastructure, products, and services that are not part of OAIT but do meet IT requirements that are not unique to a single program/project. These investments typically benefit multiple missions, programs or projects and "end of life" for a single project would not eliminate the need for the investment. Three major service areas and nine portfolios have also been defined for this

category. The service area names are identical to those in the OAIT category, as are the portfolio names with one exception: Compute Engine Hardware/Software replaces the Desktop Hardware/Software portfolio. This is in recognition that in this investment category, computing platforms may range from science and engineering workstations to supercomputers. If the platform is used as an employee's workstation it should be reported as OAIT even though it might be used for development as well as for office automation and back office services. Compute engines, as referenced here, are intended to capture equipment in laboratories and other facilities. Examples of Multi-Program/Project IT are the Space Network, Ground Network, Flight Dynamics Facility (FDF), NASA Center for Computational Sciences (NCCS), EOSDIS, NAS.

- (3) Program Unique IT is defined as infrastructure, products and services that are either physically embedded in a flight or test article, or exist solely to meet the requirements of a single specific program or project. These investments would typically not be needed after "end of life" of the unique program or project that generated the requirements for the investment. It is possible that equipment purchased as part of these investments could be reused. It is expected that this would be reported as part of a new investment. The portfolio structure for this category is based on the NASA theme(s) and program(s) of which these investments are a part.

25.1.1.2 Major organization restructuring, training and change management projects

25.1.2 Data

25.1.2.1 Types of Data

25.1.2.2 Existing Data Access

25.1.3 Application and Technology

25.1.3.1 Relationship to Service Component Model

Table 48

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Back Office Services	Development and Integration	Enterprise Application Integration	No	
Business Management	Management of Process	Configuration Management	No	The Enterprise Architecture Project includes processes for

Services

management of the configuration of the architecture elements.

Business Management Services

Management of Process

Change Management

No

The Enterprise Architecture Project includes processes for management of changes to the architecture.

Business Management Services

Management of Process

Requirements Management

No

Business Management Services

Management of Process

Business Rule Management

No

Business Management Services

Management of Process

Governance / Policy Management

No

The Enterprise Architecture Project includes a process for the governance of the architecture.

Business Management Services

Investment Management

Strategic Planning and Mgmt

No

25.1.3.2 Relationship to Technology Component Model

Table 49

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Delivery	Access and Service Requirements	Legislative Compliance	/
Service Delivery	Access and Delivery Channels	Internet	
Service Delivery	Access and Delivery Channels	Intranet	
Service Delivery	Access and Delivery Channels	Extranet	
Service Delivery	Access and Delivery Channels	Peer to Peer (P2P)	
Service Delivery	Access and Delivery Channels	Virtual Private	

Delivery		Network (VPN)
Service Platform and Infrastructure	Database / Storage	Storage
Service Platform and Infrastructure	Delivery Servers	Media Servers
Service Platform and Infrastructure	Delivery Servers	Web Servers
Service Platform and Infrastructure	Delivery Servers	Application Servers
Service Platform and Infrastructure	Delivery Servers	Portal Servers
Service Platform and Infrastructure	Hardware Infrastructure	/ Servers / Computers
Service Platform and Infrastructure	Hardware Infrastructure	/ Local Area Network (LAN)
Service Platform and Infrastructure	Hardware Infrastructure	/ Wide Area Network (WAN)
Service Platform and Infrastructure	Hardware Infrastructure	/ Network Devices / Standards
Component Framework	Security	Supporting Security Services
Component Framework	Data Management	Database Connectivity

25.1.3.3 Partnerships

25.1.4 Security and Privacy

25.1.4.1 How is it provided and funded?

The NASA EA is a process/policy, therefore there are no security plans.

25.1.4.2 How is security accomplished?

The NASA EA is a process/policy, therefore there is no security plan.

25.1.4.3 *Effective use of security, controls and authentication tools*

The NASA EA is a process/policy, therefore there is no security plan.

25.1.5 Government Paperwork Elimination Act

26 NASA Integrated Financial Management Program (IFMP)

Project Description

The Integrated Financial Management (IFM) Program is a large and complex initiative that will change the way financial and business management is performed throughout NASA. Center and/or Enterprise unique approaches will be replaced with a single set of standard integrated business processes. Each and every NASA employee will be impacted by these changes. New IFM systems will improve business processes by minimizing data redundancy, standardizing information and electronic data exchanges, processing and recording financial events effectively and efficiently, and ensuring consistent information throughout the Agency. The IFM Program consists of functional module projects that effect business process changes and that acquire and implement appropriate information technology tools to substantially improve the Agency's performance.

The Program was reformulated in March 2000 and will complete implementation of all modules within the CPIC process by the end of FY 2006.

IFMP is composed of the 8 integrated projects listed below of which 1-4 are fully implemented, 5 and 6 are in formulation/development phases, and 7 and 8 are scheduled to begin in FY04/05 and be completed by the end of FY06.

(System upgrade to new software version is not considered a separate project in the Exhibit 300.)

Project, Completion Date

- (1) Resume Management, FY02
- (2) Position Description, FY02
- (3) Travel Management, FY03
- (4) Core Financials, FY03
- (5) Budget Formulation, FY04
- (6) Integrated Asset Management, FY06
- (7) Contract Management, FY06
- (8) Human Resources, FY06

NASA is the first Federal agency to implement a commercially provided Enterprise Resources Planning (ERP) system across the entire organization. The IRS and other Federal agencies are benchmarking IFMP's success for their own ERP implementation planning. A detailed description of each project is provided below.

- (1) Resume Management, (called NASA STARS) implemented in FY 02, supports the PMA Strategic Management of Human Capital Initiative; introducing a new process and system that has changed how NASA's Human Resources (HR) offices fulfill their recruiting and staffing responsibilities, and is helping shift the role of HR professionals from administrators to consultative partners. The new resume management capability has reinvented the manner in which applicants apply for jobs and how referral lists are provided to hiring managers. It also generates Internet job postings that allow employees and the general public to apply for NASA jobs using an on-line resume builder. It includes a computer assisted rating and referral system (Resumix) to simplify, to provide more accuracy, and to expedite hiring. It enables creation of a skills database. It links directly with OPM's USA Jobs system and received an E-Gov Explorer's award as an outstanding e-gov best practice. Resume Management provides a citizen-centered hiring capability that is responsive to both our applicants and our managers. This resume-based hiring system has decreased the time to fill jobs by 35%, generated savings of 40,000 hours annually through the elimination of rating panels and, compared to the old manual process, has provided over 4 times the number of applicants to hiring managers. NASA STARS has served as a model to the OPM-led e-Gov initiative called Recruitment One.
- (2) Position Description, implemented the end of FY02, automates the position classification functions. It uses preexisting classifications or allows the user to alter the parameters to generate a new position classification. These classifications are linked to the appropriate GS level and provide workforce information needed to plan for future personnel actions. The web-based Position Description tool has reduced from days to hours the time it takes for NASA managers and human resources staff to create and grade new employee position descriptions. Through a "one stop" system for retrieving and creating positions descriptions, NASA has achieved consistency of position classification decisions across the Agency.
- (3) Travel Management, implemented in FY03, streamlines the travel process by using an end-to-end electronic system. This system allows travelers to initiate and process travel authorizations and travel vouchers electronically, automates routing for approval and payment of expenses and interfaces travel costs with the accounting system. It provides a point-of-entry data validation thereby reducing the errors on travel documents. It provides funding and accounting code verification. It allows random post-payment statistical sampling of travel vouchers. Travelers receive email notifications that their authorizations have been approved. Time to process approvals is reduced, no longer requiring the physical movement of a piece of paper to multiple desks. They are also notified when disbursements have been processed. No longer do travelers need a paper copy of the authorization or payment, it is all electronic, a significant contribution to the GPEA. Travel Management has made a tremendous contribution to the One NASA goal, standardization across ten geographically separated Centers.
- (4) Core Financials, implemented in FY03, is NASA's first fully integrated financial management system. This gives the Agency timelier, more consistent and reliable information for management decisions and improves accountability to enable full-cost accounting. Core Financial functionality includes: Budget Execution, Purchasing, Cost Management, Accounts Payable, Accounts Receivable, Standard General Ledger, and general systems management. In implementing the Core Financial module, NASA fully standardized its requirements, processes, and data across all its Centers. By eliminating

140 disparate legacy financial systems and implementing a single instance of an industry-standard product, called SAP R/3, we have achieved remarkable improvements in the timeliness, usefulness, reliability of, and access to financial management data. For example, since October 2002, we consolidated the following information into a single database:

- a. Over 1,700 Customer Master Records
- b. Nearly 36,000 Vendor Master Records
- c. Over 8,700 Fund Centers
- d. Over 8,800 Project Structures
- e. Over 46,000 Budget Distribution Transactions
- f. Over 3,800 Purchase Requisitions
- g. Over 41,000 Purchase Orders and Contracts

As a real-time transaction system, the Core Financial system provides virtually instantaneous access to funds availability, actual costs and disbursements incurred, cost allocation information, purchasing data, payable and receivable information, and other financial data. Faster processing time has been achieved in several key business processes, including acquisition of goods and services, month-end closings, and payment processing. For example, closings now are accomplished in 1 to 3 days instead of 1 to 3 weeks. An IT "backbone" enables additional integration or addition of new applications. It supports the President's Management Agenda (PMA) and provides essential management tools to achieving the "One NASA" philosophy.

5. Budget Formulation, implemented FY '04, supports budget development, advocacy, internal/external reporting, and full cost budgeting and management. It includes templates, reports, and associated processing within a software and data warehouse tool set to facilitate G&A and service pool planning, workforce planning, Center POP submissions and phasing plans, NASA budget aggregation, and the NASA budget submission and pass back process with OMB and Congress.

6. Integrated Asset Management, currently in formulation, encompasses four major areas of the management of facilities, logistics, aircraft, and environmental programs. This includes management of assets and inventories, maintenance, and reporting internally to NASA and externally. Current asset management systems do not comply with specific mandates, such as OMB's regulation on aircraft operations. NASA struggles to have visibility into contractor-held assets (e.g., Form 1018s). As a result, the agency received a material weakness for the agency's FY 2002 Financial Statements from the NASA Inspector General on NASA's management of contractor-held property. With the implementation of this module, this material weakness will be resolved.

7. Contract Management, formerly referred to as Procurement, is scheduled to be implemented in FY 06. It will provide a comprehensive tool to support contract writing, contract administration, procurement management, and data and reporting management materials for NASA. It will provide detailed and quantitative data to facilitate, economize and expedite procurement processes and will be integrated with existing IFMP systems. Other procurement functions are now being evaluated by the functional community for inclusion in this project.

8. Human Capital, formerly referred to as Human Resources is scheduled to be implemented in FY '05 & '06. It will integrate traditional HR functions with other IFMP modules as well as ePayroll. The Human Capital module will support a broad range of HR functions across the Agency. Functionality being considered are Awards, labor distribution, performance and training and events management.

Architecture

26.1.1 Business

26.1.1.1 Process simplification/reengineering/design projects

The IFM Program is in the midst of implementing a modular and incremental re-engineering of business processes and implementation of COTS software prioritized by contribution to agency goals, Center needs, design and implementation complexity, data dependencies, and available budget. Success of the program will be judged on the basis of achievements in terms of measurable project success metrics. The mission statement proper is supported by the Agency Business Drivers and was developed based on the Enterprise Strategic Plans and Agency Strategic Plan. Each project will establish Functional Drivers for that project that materially contribute to achievement of the Agency Business Drivers. They will also establish performance metrics that are measurable and establish the Minimum Success Criteria for the project. Thus, there is a continuous flow of accountability from the mission support objectives identified in the Strategic Plans to the applicable financial and human resources management process and technological improvements to be provided by IFMP in support of those objectives, and ultimately to the functional objectives to be achieved by the individual IFMP projects. To ensure alignment to the Agency EA framework and provide input for technology-related management decisions, the Program continues to build-out its Business Reference Model (BRM) of the IFMP EA framework. This includes mapping preliminary To-Be processes against current As-Is processes to discover integration points between potential Module applications and existing applications (primarily SAP and eGov sites).

The IFM Program is a large and complex initiative that will change the way financial, physical, and business management is performed throughout the agency. Additionally, the IFM Program is charged with management and implementation of the Agency's electronic Government (eGov) initiatives, all of which are subject to the same management practices and processes as the IFM Project modules. Center and/or Enterprise unique approaches will be replaced with a single set of standard integrated business processes. Each and every NASA employee will be impacted by these changes. Given the magnitude of this effort, including large-scale changes and business process improvements overall program management is based at Headquarters with matrixed support from all Centers. Technical program management functions are being performed at Marshall Space Flight Center (MSFC) under the Integration Project Office.

The IFM Program has committed to re-engineer processes three times in order to achieve process optimization. For each project, the first re-engineering will be used to define existing processes across NASA's ten Centers and to establish a single preferred process that will form the basis for the initial set of project requirements. The second re-engineering will be done in the context of selected COTS software, and will align and standardize agency processes around the capabilities of the selected software. NASA is committed to adapt its processes and requirements to the commercial practices embodied in the COTS products. Consistent with external laws and requirements, the third and final re-engineering will be undertaken 18-24 months post implementation and will be used to restructure Agency and Center operations, based on the demonstrated capabilities of the selected software. The full benefit of IFM will be realized when the Agency has finished the third wave of process re-engineering and is leveraging the business process capabilities enabled by the software.

26.1.1.2 *Major organization restructuring, training and change management projects*

To achieve the Program Mission and Business Drivers, the Program establishes "module projects" under the auspices of a Lead Center. (Module Projects also include eGov projects, such as ePayroll and eTravel.) Through the work of the Module Projects and functional Steering Committees new and standardized business processes will be established across the Agency. The Core Financial project served as the foundation or "backbone" on which the total system will be built. This Project consolidated most of the previously separate financial management systems of individual NASA Centers into a single, integrated system. Other system deployment and integration are either completed or underway, including Budget Formulation and Travel Management. Additional Module Projects including Core Human Resources, Contract Management, Integrated Asset Management, ePayroll and eTravel will be similarly deployed and integrated over time.

IFMP, however, is more than just a technology implementation. The real value of the system comes from integration of information that is consistent, reliable, and timely across business functions, Centers and Programs thus enabling our vision -- one NASA, with 10 interdependent centers. In order to achieve the benefits of the IFM system and supporting Agency eGov initiatives move toward this vision, significant culture change will be required. It is also critical that these projects be functionally aligned and implemented in a manner that facilitates acceptance across the diverse NASA organizations.

For IFMP to be successful NASA will have to adopt new behaviors and values that are different from the current cultural norms. For example, to realize our business driver of better decision-making, the Agency needs to move from a culture in which information is hoarded and shared only when there is a "need to know," towards a culture which values and encourages information sharing across horizontal and vertical boundaries and information based decision-making. Change management is the process of aligning NASA's people and culture with the changes in systems, business processes, organizational structures and business or operations strategy resulting from IFMP and eGov implementation. Alignment is achieved when employees at every level understand and buy-in to the benefits the new system and initiatives will bring, transition

into their new job/roles, and use the capabilities to improve or transform business processes. Aligning the NASA culture with the IFM environment will require a concerted effort on the part of the Program, its Projects and key stakeholders.

Therefore, the Program has adopted a two-pronged approach to managing IFM related change. The first component is a transactional change approach that focuses on the employee's acceptance of, and competence in, the new system/environment. The second component is a transformational change approach that focuses on changing the culture to drive the full benefit from the new technology tool. These approaches apply to both Program and Project level change management activities. Corporate Change Management support is performed at the Program level and focuses on capturing lessons learned across all modules and ensuring effective communication with external Program stakeholders.

IFMP's transactional change approaches are primarily the responsibility of the Module Projects and the Implementing Centers. The transactional change approaches are designed to help the Module Projects and Center Implementation teams "navigate the culture" in order to stand up the system and ensure that change management is more closely aligned with Module user and stakeholder needs and feedback. The domain of transactional change includes three major areas:

26.1.2 Data

26.1.2.1 *Types of Data*

Financial Data: The Financial capabilities of the IFM System are primarily enabled in the Core Financial Project, Budget Formulation Project, and the Travel Management Projects. These projects provide the ability to record, classify, and report all types of financial data in the areas of Federal financial management and accounting, including:

1. **Budget Execution:** Records budget authority and resources available, tracks apportionment and allotments, permits the establishment of spending limits, and collects financial actuals, permitting the comparison of budget to actual data. Records the commitments and obligation, including verifying and tracking the availability of funds.
2. **Budget Formulation:** Allows users to record, maintain, communicate, and report formulation budget data in real time across the agency and facilitates "what-if" analysis.
3. **Purchasing:** Records the accounting impacts associated with obligations from contract awards, purchase orders, grants, and modifications by associating procurement line items with the respective accounting line items.
4. **Cost Management:** Uses workforce, cost, labor, and other inputs to determine cost information and the allocation of costs.

5. Accounts Payable: Prepares and delivers payments, as well as advanced payment processing for services rendered.
6. Accounts Receivable: Creates, processes, and manages reimbursable and non-reimbursable bills for accounts receivable.
7. Standard General Ledger (SGL): Establishes SGL accounts and code, maintains the financial classification structure (FCS) and SGL, and reports financial information.
8. Travel Management: Streamlines the travel process by using an end-to-end electronic system. Creates a standardized, fully-integrated, comprehensive travel management system.
9. General: Requirements common to all of Core Financial, including audit trails and financial reporting.

Human Resources: Employee name, grade, master pay record, SSN, series benefits, leave, dates of employment, attendance and payroll processes, employee training and development, employee performance, recognition and benefits programs, the resolving of disputes and complaints, and the administration of labor relations.

Resume Management: Employee name, experience, grade, education, training, certifications and job announcements.

Position Description: Job series, job descriptions, number of jobs.

26.1.2.2 Existing Data Access

26.1.3 Application and Technology

26.1.3.1 Relationship to Service Component Model

Table 50

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Back Office Services	Data Management		No	NASA's Integrated Financial Management Program consists of multiple projects, as part of a phased approach to an ERP implementation, which are aligned to the Back Office Services Domain and Support Services Domain in the Service Component Reference Model

Section of the Federal Enterprise Architecture. There is a strong correlation between several of the service types and the completed and future projects in IFMP.

Six different service types that are classified under the Back Office Services Domain have been identified as aligned to IFMP. The service types are the following: Data Management, Human Resources, Financial Management, Assets/Materials Management, Development and Integration, and Human Capital/Workforce Management.

For each of the service types, a number of components that can trace back to the functionality of the various IFMP projects were identified. Data Management (1) components were identified as the following: data exchange, data mart, data warehouse, meta data management, data cleansing, extraction and transformation, loading and archiving, data recovery, and data classification. Human Resources (2) components were identified as the following: recruiting, resume management, career development and retention, time reporting, awards management, benefits management, personnel administration, education/training, health and safety, and travel management. Financial Management (3) components were identified as the following: billing and accounting, credit/charge, expense management, payroll, payment/settlement, debt collection, revenue management, auditing, activity-

based management, and financial reporting. Assets/Materials Management (4) components were identified as the following: property/asset management, asset cataloging/identification, asset transfer, allocation and maintenance, facilities management, and computers/automation management. Development and Integration (5) components were identified as the following: legacy integration, enterprise application integration, data integration, instrumentation and testing, and software development. Human Capital/Workforce Management (6) components were identified as the following: resource planning and allocation, skills management, team/org structure, contingent workforce management, workforce acquisition/optimization.

Security Management was identified as the service type within the Support Services Domain that aligns with IFMP. The nine components to the Security Management service type are the following: identification and authentication, access control, encryption, intrusion detection, verification, digital signature, user management, role/privilege management, and audit trail capture and analysis.

Back Office Services Human Resources No

Back Office Services Financial Management No

Back Office Services	Assets / Materials Management	No
Back Office Services	Development and Integration	No
Back Office Services	Human Capital / Workforce Management	No
Back Office Services	Security Management	No

26.1.3.2 Relationship to Technology Component Model

Table 51

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Service Access Delivery	Access and Channels	Web Browser	<p>In the technical reference model, there are 4 service areas that apply. These Service Areas, with their Relevant Service Category and Relevant Service Standards are as follows:</p> <p>Service Access and Delivery</p> <ol style="list-style-type: none"> 1. Access Channels <ol style="list-style-type: none"> a. Proprietary Graphical User Interface (GUI) b. Browser (Microsoft Internet Explorer 6.0 for Windows) c. Windows Terminal Services (Citrix) 2. Delivery Channels <ol style="list-style-type: none"> a. Internal NASA local area and wide area networks b. The Internet c. Private, leased circuits 3. Service Requirements <ol style="list-style-type: none"> a. NASA policy compliance b. OMB policy compliance c. Formalized Service Level Agreements (SLA) 4. Service Transport <ol style="list-style-type: none"> a. Internet Protocol over Ethernet

and ATM

Service Platform & Infrastructure

- 1. Support Platforms
 - a. Java and J2EE (middleware)
- 2. Database/Storage
 - a. Relational databases (Oracle, limited SQL Server)
- 3. Delivery Servers
 - a. Database, application, web and standalone servers
- 4. Software Engineering
 - a. Mercury Test Director
- 5. Hardware/Infrastructure
 - a. Sun Microsystems, Compaq, DEC Alpha, EMC Symmetrix, StorageTEK, Cisco, Checkpoint

Component Framework

- 1. Security
 - a. Proprietary application-level security structures, Secure Socket layer, Citrix Secure ICA, limited strong authentication (RSA SecureID)
- 2. Data Interchange
 - a. XML
- 3. Presentation/Interface
 - a. Proprietary application mechanisms, HTML, JavaScript
- 4. Business Logic
 - a. Platform dependent (proprietary)
- 5. Data Management
 - a. ODBC, Crystal, Brio, SAP Business Warehouse

Service Interface and Integration

- 1. Integration
 - a. Enterprise Application Integration backbone (seeBeyond)
- 2. Interoperability
 - a. XML
- 3. Interface
 - a. Enterprise Application Integration backbone (seeBeyond)

Service Access Delivery	Delivery and Channels	Intranet
Service	Service	Static Display

Access and Delivery	and Requirements	
Service Access and Delivery	Service and Transport	Service Transport
Service Platform and Infrastructure	Supporting Platforms	Platform Independent
Service Platform and Infrastructure	Database and Storage	/ Database
Service Platform and Infrastructure	Software Engineering	Test Management
Service Platform and Infrastructure	Data Management	Reporting and Analysis
Service Platform and Infrastructure	Security	Supporting Security Services
Component Framework	Data Interchange	Data Exchange

26.1.3.3 Partnerships

IFMP is aware of, and is active in the planning of, several e-Government initiatives presently being pursued by other government agencies (i.e. OPM, DOI, GSA, DOHHS). The goal of IFMP is to ensure the deployed ERP solution will be compatible with these initiatives and will be able to leverage these components and/or applications to minimized waste and increase efficiency across all government entities.

Presently, IFMP is utilizing "USA Jobs" with the Resume Management module and is in the formulation stage of the e-Gov initiative of e-Payroll (OPM/DOI) to satisfy the requirement for payroll for the Agency, eTravel (GSA), and Recruitment One-Stop (OPM). Other future leverage Government systems include Integrated Acquisition Environment (GSA), and Enterprise HR Integration (OPM).

26.1.4 Security and Privacy

26.1.4.1 *How is it provided and funded?*

Information technology security for the Integrated Financial Management Program (IFMP) (in this context both infrastructure and application level) is provided and funded by the IFM Program. There is a level of oversight provided by the NASA CIO organization. IFMP complies with Federal, NASA and NASA Center standards for IT security for both access to networks and applications. Each Project has a Security Plan which identifies specific security/access requirements for that application. Additionally, COTS solutions include access security capabilities. Due to security issues, further definition of IFMP security cannot be provided in this document. IFMP has undergone independent audits of security controls by the NASA OIG, Price Waterhouse Coopers, and Booze Alan Hamilton. In addition, we run routine quarterly scans for system vulnerabilities. Please contact the IFMP Program Office for specific security questions.

26.1.4.2 *How is security accomplished?*

The investment meets the security requirements by following NASA policy and guidance documents NPD and NPG 2810, adhering to updates from NIST guidelines and incorporating OMB polices as issued.

The Project complies with the NASA Procedures and Guidance (NPG) 2810.1. This NPG is NASA's IT Security Procedures guide. This NPG employs standard guidance that had preceded the current approved standards and guidance from NIST and applies to the entire IT life cycle of the Project. NPG 2810.1 includes requirements for laws and regulations and provides NASA specific guidance. NASA understands that security is an ongoing challenge and that NIST is revising their procedures. When NIST completes this process NASA will revisit its policy and procedures to conform with NIST new guidance.

The IFMP COTS solution, SAP, is the world leader in financial systems. It provides single point of entry, role-based access controls, extensive audit logging, and many other capabilities that collectively ensure that NASA's financial users are accessing consistent, reliable information.

This product encompasses financial best practices, and has been certified by the federally recognized Joint Financial Management Improvement Program (JFMIP). IFMP also goes through FFMI compliance audits by external contractors.

The Integration Steering Committee, chaired by the Agency CIO, reviews the technical solution for each module. Prior to implementation, the technical infrastructure readiness is assessed. Operational Readiness Reviews (ORR) are conducted at each site prior to going live and approved for operational use by each Center. The Center CIO participates in the ORR.

Processes for incident handling are documented in the module security plans. A comprehensive intrusion detection capability has been implemented.

Incidents are reported to the IT Security Manager at Marshall Space Flight Center.

The system is operated by contractors. All contracts include specific security requirements required by law and policy.

All system processes are audited. Logs are viewed and where deemed necessary, two person control is used to ensure the integrity of the system and its data.

26.1.4.3 *Effective use of security, controls and authentication tools*

Extensive privacy measures are in effect for all IFMP modules. These are encompassed in planning and implementation of measures to protect the classic security elements for integrity, availability, and confidentiality. These measures include client to server data encryption, a locked-down Data Center, extensive system authorization design, and network-level security protection (firewalls).

26.1.5 Government Paperwork Elimination Act

This investment is included in NASA's GPEA plan. The Integrated Financial Management Program (IFMP) centralizes and integrate NASA's current financial, physical, and human resources business systems and processes using current technology coupled with commercial best practices. Utilizing state-of-the-art technology, IFMP provides the ability to perform and communicate financial-related tasks electronically. NASA is targeting a Enterprise Resource Planning (ERP) solution to incorporate "best practice" business processes. One anticipated outcome is a reduction in internal paper flow and paper-dependant transactions. NASA anticipates reaping many eGovernment benefits for the Agency's internal and external customers.

A fully implemented IFMP system will greatly reduce the internal paper-dependant workflow business processes. The processes will become electronic and when combined with digital signatures will require little in the way of hard copy. Formal approvals and distribution will all become electronic. As a more interactive means of disseminating information to the public at large, it is anticipated that most public interaction will be present within the Human Resource function. The Resume Management module of IFMP introduced a new process and system that changed how NASA's human resources offices accomplish recruiting and staffing, how applicants apply for jobs, and how referral lists are provided to hiring managers. The system is an automated Staffing And Recruiting System, which uses state of the art technology to produce Internet job postings (USAJobs) that provide the opportunity for employees and the public to apply for jobs using an on-line resume builder. It also includes a computer assisted rating and referral system to simplify and expedite hiring. NASA now announces vacant positions via the Internet, making this information available to the public. The Agency is receiving resumes electronically evaluating and referring them to hiring managers electronically. This enables all parties to view the status of a submission throughout the process. This improvement will reduce a highly manual and paper-dependant process to an expedient tool. There will be significant efficiencies gained through the use of e-commerce in the general procurement arena, as well as the aircraft component procurement. General procurement initiatives are examining the use of smart cards, e-mall, reverse auctions, the pooling of Center purchases to obtain quantity discounts, electronic approval routing, and electronic signatures. All this is supported via the Web, which inherently reduces paper-dependant transactions. Furthermore, NASA is looking to

build links with the Department of Defense to promote expedient and paperless purchase orders for aircraft components. IFMP implementation will promote stronger, more fluent, and less cumbersome communications with other Federal Agencies through the use of electronic communications and submission of required forms. Within Human Resources, efficiency gains are anticipated through the provisioning of personnel management and benefit administration via the Web. NASA employees will be able to initiate an increased variety of personnel actions via self-service transactions. Employees could transfer from one Center to another without having to process a 'losing action' at the old Center and a 'gaining action' at the new Center. Again, electronic routing and approval through electronic signatures will greatly increase the speed of transactions and also reduce the need for hard copy processes. For reference only: the initial NASA Agency-wide GPEA plan was delivered on 10/31/2000.

27 NASA OAIT Umbrella

Project Description

NASA's investment in Office Automation, IT Infrastructure, and Telecommunications is managed as the NASA Integrated Information Infrastructure Program. This program focuses on taking what NASA has in place, built and managed separately by individual Centers over several decades, and molding those systems into an integrated infrastructure aligned to mission and business needs to create a cohesive strategy of integration, automation, and virtualization.

Using the NASA Enterprise Architecture as the framework, the NASA Integrated Information Infrastructure Program incorporates NASA's ongoing operational infrastructure, along with new improvement initiatives, into service clusters that create a cohesive strategy of integration, automation, and virtualization. New initiatives were prioritized according to their impact on furthering the transition to a secure integrated infrastructure.

Project Consolidation

The President's Management Agenda (PMA) clearly identifies E-Government as a critical success factor for all Federal agencies. E-Government requires Agencies to use IT to transform their operations in ways that improve effectiveness, efficiency, and service delivery. The principles of E-Government include having market-based, result-oriented, citizen-centered IT initiatives that unify business lines within and across agencies while at the same time simplifying business processes.

As E-Government initiatives progress, the need to share information and tools across the Agency and the entire Federal Government continues to grow, and the need for a unified IT infrastructure becomes even more critical.

To facilitate the implementation of the E-Government principles NASA must:

- Transform its IT infrastructure to provide a secure and efficient interface between: NASA Centers, NASA and other government agencies, application service providers, partners and vendors, and the public.

- Be prepared with an IT infrastructure that provides a single interface and eliminates the need for application owners and service providers to negotiate multiple agreements and maintain costly separate systems.
- Remove the barriers to deployment of agency-wide systems and increase its security posture.

The NASA Integrated Information Infrastructure Program is the NASA strategy for managing the transformation of the Agency's IT infrastructure from a collection of eleven loosely connected architectures and multiple site-dependent systems to a single enterprise architecture providing Agency-wide IT infrastructure services (a One NASA environment). This One NASA IT environment is designed to support NASA's Strategic Plan and the President's expanding E-Government initiative. The Program has at its core the following objectives:

- Managing the NASA IT infrastructure as part of an integrated NASA Enterprise Architecture
- Providing an infrastructure that can evolve and adapt to emerging technologies and services models
- Providing information tools and services that enhance programs and management
- Emphasizing a customer focus in providing common IT infrastructure services across NASA
- Enabling effective and efficient integration with Federal E-Government applications

Specific One NASA services will be provided through a combination of the following coordinated approaches, appropriately selected to best deliver an efficient and effective infrastructure:

- Locally managed and provisioned
- Centrally managed and locally provisioned
- Centrally managed and provisioned

Technical Consolidation:

The NASA Integrated Information Infrastructure Program is built upon two overarching strategies:

1. Alignment with the Enterprise Architecture and
2. Creation of a secure computing foundation.

In FY03, teams examined the "to be" state of the Enterprise Architecture and identified information technology barriers to achieving One NASA, along with security vulnerabilities and system inefficiencies. Using specialized working teams and the NASA Capital Planning and Investment Control process, priorities were established and funding was requested to begin implementation of infrastructure enhancement initiatives in alignment with those priorities.

The following are the key One NASA components "clustered" into logical service categories:

- Overarching strategies/Cross-cutting services:

- The NASA Enterprise Architecture provides the framework for this Program. The information security strategy provides both an overarching system of protection, and removes many of the current barriers to One NASA caused by the eleven different systems that are in place today. Broad service areas consolidate systems at the agency-level to enable anywhere, anytime access to information and people. Through this approach, NASA can gain more effective use of its IT investments - closing the technology chasm created by the current widely distributed systems and creating the environment that will be critical to meeting NASA's mission objectives.
- Enterprise Architecture
 - The NASA Enterprise Architecture is a strategic tool that links NASA's mission, business and IT strategies. The architecture provides the fundamental methodology and framework for defining how NASA's IT will work. Key elements of the architecture include Customer Boards, Governance, Configuration Control Board(s), and the IT Service Model.
- Secure Computing Environment

Security crosscuts all of IT and is an integral component of all the service areas and each of the components included within this program. NASA policy for ensuring that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated is set out in NASA Procedural Requirements 2810.1, "Security of Information Technology."

Detailed procedures and guidance are contained in NASA Procedures and Guidelines 2810.1. These instructions provide direction for ensuring that safeguards for the protection of the integrity, availability, and confidentiality of IT resources (e.g., data, information, applications, and systems) are integrated into and support the missions of NASA.

In addition to Agency and Center-wide ongoing security operations, this program includes near term Agency-wide security initiatives to correct known vulnerabilities, reduce barriers to cross-Center collaboration, and provide cost-effective IT security services in support of Integrated Financial Management Program and e-Gov initiatives. These initiatives were proposed as new starts for FY04, and milestones developed assuming a first quarter FY04 start. However, due to delays in approval of NASA's FY04 Operating Plan, these initiatives were not able to be started until the fourth quarter. Two of the initiatives reported last year - Account Management and Cyber Identity Management - have been consolidated, and integrated with another related activity - Identity Management System - into a single initiative called the NASA Integrated Services Environment (NISE).

This consolidation occurred naturally as the requirements for the two initiatives evolved and the inter-dependencies between them and the Identity Management System became clear.

Convergence of the three efforts will enable NASA to implement an Agency-wide IT "services layer" that will function as a centrally managed, integrated environment used to (1) establish, track, and authenticate the identity of all end users entitled to physical access at NASA Centers and facilities; (2) supply logically integrated Agency directory services to authorized users and locations; and (3) grant end-user privileges and access to all managed IT resources. Specific goals of these three major complementary components of NISE are:

- Identity Management System (IDMS). In support of Code X, IDMS will serve as the authoritative source of validated identities for NASA and will use a Microsoft Identity Integration Server metadirectory implementation to provide the Agency directory service with a delegated replica of NASA identity information.
- Cyber Identity Management System (CIMS). CIMS will establish a unified directory that provides a secure, reliable, and accurate source for retrieving and managing end user IT identity and locator information such as name, title, expertise, organization, location, phone number, e-mail address, and other information.

NASA Account Management System (NAMS). NAMS will provide a secure, consistent, expedient and accurate account management environment across NASA. NAMS also will improve security and auditing capabilities, and it will reduce the cost of managing accounts within networks, applications, databases, and systems across NASA Centers and facilities.

In spite of a much delayed start, substantial progress has also been made toward establishing the One NASA Network Security Perimeter (NSP). This initiative will provide a consistent and managed interface for applications and services and will reduce deployment complexity and management risks. The objective is to improve Agency-wide interoperability, efficiency of operations, reliability, and most of all - security.

- Software Engineering
 - This program incorporates software engineering activities in support of the service areas defined below, including requirements development and management, configuration management, system testing and performance monitoring tools. NASA has specific governing policies with respect to software engineering:
 - NASA Policy Directive 2820.1, "NASA Software Policies"
 - NASA Standard 2100-91, "NASA Software Documentation Standard"
 - NASA Standard 2201-93, "Software Assurance Standard"
 - NASA Standard 2202-93, "Software Formal Inspection Process Standard"
 - NIST Standards

While historically NASA's software engineering activities have focused primarily on mission-specific systems, the Agency is currently in the process of chartering a Software Steering Board to ensure an integrated NASA-wide approach to the areas of software engineering, software assurance, Independent Verification and Validations (IV&V) of software, software related research, and training in software disciplines.

Agency is currently in the process of chartering a Software Steering Board to ensure an integrated NASA-wide approach to the areas of software engineering, software assurance, Independent Verification and Validations (IV&V) of software, software related research, and training in software disciplines.

- IT Asset Management

In recognition of the critical role and high-dollar value of capital assets, the NASA Strategic Plan contains a very specific goal of achieving excellence in the institutional management of capital

assets, including implementation of best practices. The NASA Associate Deputy Administrator for Institutions and Asset Management, along with the Institutional Committee, provide direction and oversight for capital asset management. The NASA Program Management Council also provides asset management oversight for specific programs. Additional requirements are found in the following instructions:

- NASA Policy Directive 4200.1, "Equipment Management"
- NASA Procedural Requirements 4200.1, "NASA Equipment Management Manual"
- NASA Procedural Requirements 4200.2, "Equipment Management Manual for Property Custodians"
- NASA Policy Directive 8831.1, "Maintenance of Institutional and Program Facilities and Related Equipment"

NASA Procedural Requirements 8831.2, "Facilities Maintenance Management"

NASA is in the process of defining requirements for an Integrated Asset Management (IAM) system planned for deployment as a component of the Integrated Financial Management (IFM) Program. The Integrated Information Infrastructure Program incorporates the legacy IT asset management systems and services. When the IAM system becomes operational, it will be incorporated into the Integrated Information Infrastructure Program as the legacy systems are phased out.

Service Areas

The NASA Integrated Information Infrastructure Program clusters operational activities and improvement actions into three service areas. Descriptions of each service area and the components within each service area are described below.

Communications Services Area

The Communications Services area includes the Agency's voice, data, and video network infrastructure, exclusive of any infrastructure elements that are unique to mission operations.

Wide Area Network (WAN):

This component consists of a set of wide area networks that support production services, as well as services provided by several Internet Service Providers (ISP). The bulk of these services are provided Agency-wide today within the NASA Integrated Services Network. However, performance and reliability has not been sufficient to meet the growing requirements generated by the Agency's increasing reliance on the network for conduct of its day-to-day operations.

Consequently, ISP services have been procured by several Centers as an alternative for direct access to the Internet.

An independent economic analysis by Tecolote Research, Inc., examined four cases for providing Wide Area Network capabilities to NASA, including maintaining the "as is" approach.

The most economical case is to replace/upgrade the existing network. This effort is one of the near-term projects planned within this program. Assuming a transition period beginning in May 2003, the breakeven point is achieved in FY08.

Local Area Network (LAN):

The LAN component incorporates all IT investments required to provide networking services within a building, campus, data center or Center, including hardware, software, and services (including wireless LANs, remote access, Domain naming services, network management, X500/directory services).

The operational state of LAN services varies greatly from Center to Center. Since this capability evolved over time, there are a diverse set of LAN architectures across the Agency. NASA's approach to integrating the management of the LAN environment is to define an Agency standard LAN architecture which Centers will build to as future LAN upgrades take place. The definition of this architecture was completed and approved in June 2003, and most Centers have LAN upgrade projects progressing as funding permits.

Voice

The Voice component includes all elements that provide voice services to users including hardware, software, services, and communications that are not provided by NASA WANs.

The voice element includes local and long-distance telephone services, cell phone service, satellite phone service, teleconferencing, voice mail, fax, and ancillary services such as two-way radios, emergency warning systems, and public address systems. Long Distance Service (LDS), 800 numbers, and calling cards are obtained from the GSA FTS2001 contract. Several Centers have upgraded their voice network infrastructure in recent years. At this time, integration and consolidation efforts are focused primarily on the use of common service providers where feasible. Transition to the use of Voice over Internet Protocol (VoIP) is viewed as the most viable means of consolidating this service Agency-wide in the future, but a recent feasibility study conducted by GSA on NASA's behalf determined that this is not a cost-effective approach for the Agency at this time. However, as the technology matures, the use of VoIP will potentially enable not only the consolidation of voice services, but also the convergence of the voice and data infrastructures.

Video

This category includes investments required to support video and video distribution and video conferencing services used by Agency or Bureau to include hardware, software, and support services - not including LAN or WAN. Video services include Video Teleconferencing Systems (ViTS0, digital video production equipment and facilities, video distribution systems and video repositories. ViTS capability is provided as part of an integrated Agency-wide service through NISN, as is video distribution between Centers. At this time, further integration and consolidation efforts are focused on setting Agency standards to which Center systems will be built, using common service providers where feasible, and the sharing of video repositories where practical. In addition, it is expected that as networks are upgraded and desktop videoconferencing becomes more widely available, that there will be an opportunity for convergence with the voice and data infrastructure.

Architecture

27.1.1 Business

27.1.1.1 *Process simplification/reengineering/design projects*

One of the goals of the NASA Integrated Information Infrastructure Program is to improve the operating efficiency, agility and flexibility of the agency such that it will be able to adjust to and meet future business conditions and demands. The NASA Integrated Information Infrastructure Program will take NASA from eleven "independent" architectures that created numerous barriers to deployment of agency-wide applications to a common architecture and consolidated management of agency-wide systems and applications. The Service Delivery Model that serves as the foundation for this Program, and each of the service areas identified by the program, require reengineering of how systems work. However, most of the reengineering is behind the scenes, simplifying the user interface and the operational demands on the IT community.

27.1.1.2 *Major organization restructuring, training and change management projects*

Since the NASA Integrated Information Infrastructure Program is comprised of front office, back office, and network infrastructures that include a multitude of integrated mixed life cycle projects, each service area will identify the associated process organization restructuring, training, and change management efforts and coordinate and integrate the efforts a part of the agency's Enterprise Architecture change management process.

27.1.2 Data

27.1.2.1 *Types of Data*

Since the NASA Integrated Information Infrastructure Program is comprised of front office, back office, and network infrastructures that include a multitude of integrated mixed life cycle projects, the data that will be used in the program is comprised of all of the data that NASA stores, processes, and communicates over its infrastructure. Information used in conducting the Agency's daily business - supported by this project falls into five categories.

Mission Information

This category consists of information that directly supports NASA's human space flight, launch operations, space vehicle operations, wind tunnel operations, training simulation vehicles, and other mission-related activities.

- NASA protects its mission information from alteration or destruction, particularly where proprietary or sensitive information is involved.
- NASA protects information related to individuals involved in NASA's missions.

With respect to information that involves risks to human health, safety, and the environment, NASA ensures that the following have been analyzed and/or documented, to the extent practical:

- Expected risks for each affected population;
- Acceptable upper and lower bounds of risk;
- Uncertainties identified during the risk assessment process and how the uncertainties were or will be addressed;
- Peer review studies related to risk estimates; and
- Methodologies used to reconcile inconsistencies in the scientific data.

Business and Restricted Technology Information

This category consists of information related to financial, legal, payroll, personnel, procurement, source selection, and other business and restricted technology activities.

NASA ensures that categories of information requiring protection or restricted access under law are appropriately handled and protected from inappropriate dissemination. Examples of the types of information to which public access may be prohibited or limited include national security classified information; export-controlled information; personal information subject to the Privacy Act; and documents disclosing inventions, proprietary information, trade secret information, or Small Business Innovation Research (SBIR) data (as defined in FAR 52.227-20).

In situations in which public access to data and methods will not occur due to reasons described above, NASA will apply especially rigorous robustness checks to analytic results. NASA will ensure the disclosure of, and appropriately document, the specific data sources, quantitative methods, and assumptions that have been employed.

Scientific, Engineering, and Research Information

This category consists of information that supports basic research, engineering, and technology development.

NASA ensures that its scientific, engineering, and research information is subject to the appropriate level of pre-dissemination review, commensurate with the nature, scope, purpose, and significance of the information and its intended audience.

NASA ensures that the underlying methodologies, data, and assumptions employed are appropriately transparent and documented to the greatest possible extent.

Administrative Information

This category consists of information such as general electronic or written correspondence, briefing information, program/project status documents, organizational documentation, strategic plans, and other information of an administrative or general nature.

NASA ensures that administrative information is reviewed regularly to ensure its continued relevance and accuracy.

27.1.2.2 *Existing Data Access*

27.1.3 Application and Technology

27.1.3.1 *Relationship to Service Component Model*

Table 52

Service Domain	Service Type	Component	New Component	Relation to SCRM of FEA
Support Services	Security Management	Access Control	No	This project will deliver a capability to manage computer access privileges within and between Centers for Agency-wide applications and services.
Support Services	Security Management	User Management	No	A key element of this project is the automation of the account management process.
Business Management Services	Organizational Management	Network Management	No	This project provides standard Agency LAN perimeter configuration including network monitoring and security services
Support Services	Security Management	Audit Capture Analysis	Trail and No	This project will include as part of its solution an audit trail of events that may be analyzed to provide information about network security perimeter events.
Customer Services	Customer Preferences	Profile Management	No	Agency system for identity management

				utilizing single LDAP directory coupled with Agency account management system.
Support Services	Security Management	Access Control	No	Integrates with Account Management System to provide uniform Agency-wide authentication service.
Customer Services	Customer Preferences	Alerts and Notifications	No	The WAN project provides subscription-invoked activity and outage notifications to users based on key words and phrases that appear in the notification. (Current capability)
Customer Services	Customer Initiated Assistance	Self-Service	No	The WAN project offers to its customers an online service request and work control system for generating, submitting, tracking, assigning, routing, approving, status, and reporting for customer requirements. (Current capability)
Business Management Services	Management of Process	Program / Project Management	No	Multiple monthly program management reviews are held to review highlights, service performance utilization, customer satisfaction, risks, cost/schedule status, and issues.

Business Analytical Services	Analysis and Statistics	Modeling	No	(Current capability) Network modeling tools are used to assess the effect of new requirements and to isolate performance issues with existing services. (Current capability)
Back Office Services	Data Management	Data Exchange	No	The WAN project provides the communications circuits that support Agency-wide data exchange. (Current capability)
Support Services	Security Management	Intrusion Detection	No	Intrusion detection systems are used for detection, isolation, forensic analysis, preventing, documentation, and reporting of security incidents. (Current capability)
Customer Services	Customer Preferences	Profile Management	No	Service managers are responsible for matching customer requirements to service offerings, designing and operating systems, and selecting and managing contractors and providers. Service managers interact with vendors and customer technical points of contact.
Support Services	Communication	Audio Conferencing	No	The Voice Project provides the Agency's audio conferencing capability. (Current

Support Services	Communication	Computer Telephony Integration	/ No	capability) Some NASA Centers are conducting VoIP pilots. (Current capability)
Customer Services	Customer Relationship Management	Customer Feedback	No	For Agency-wide services, customers are requested to fill out a satisfaction survey after every service request is completed. Survey results are reviewed monthly and follow up is performed on negative surveys. (Current capability)
Customer Services	Customer Initiated Assistance	Scheduling	No	For Agency-wide services, customers may request that services be provided on a specified schedule via the online service request and work control system. (Current capability)
Customer Services	Customer Relationship Management	Call Center Management	No	Desktop support includes as a current capability provision of multipurpose help desks to assist customers in the use of their desktop hardware and software and in dispatching technicians to resolve problems.
Customer Services	Customer Relationship Management	Contact Management	No	The Desktop Hardware and Software Project includes as a current capability desktop software

					that supports contact management.
Customer Services	Customer Relationship Management	Partner Relationship Management	No		The Desktop Hardware and Software Project currently includes periodic meetings between the desktop outsourcing vendors and NASA personnel to exchange information and provide feedback on performance, issues, etc.
Business Management Services	Supply Chain Management	Catalog Management	No		The Desktop Hardware and Software Project includes as a current capability support for ordering of desktop hardware and software products via an online catalog.
Digital Asset Services	Content Management	Content Authoring	No		The Desktop Hardware and Software Project includes as a current capability desktop software that supports content authoring.
Digital Asset Services	Content Management	Content Review and Approval	No		The Desktop Hardware and Software Project includes as a current capability desktop software that supports content review and approval.

Digital Asset Services	Knowledge Management	Information Mapping Taxonomy	No /	The Desktop and Hardware and Software Project includes as a current capability desktop hardware and software that supports this component.
Digital Asset Services	Knowledge Management	Information Sharing	No	The Desktop and Hardware and Software Project includes as a current capability desktop hardware and software that support information sharing.
Digital Asset Services	Records Management	Document Classification	No	The Desktop and Hardware and Software Project includes as a current capability desktop hardware and software that support document imaging and OCR.
Business Analytical Services	Visualization	CAD	No	The Desktop and Hardware and Software Project includes as a current capability desktop hardware and software that support CAD.
Business Analytical Services	Business Intelligence	Balanced Scorecard	No	The Desktop and Hardware and Software Project includes as a current capability desktop hardware and software that support this component.
Business Analytical	Reporting	Ad-Hoc	No	The Desktop and Hardware and

Services				Software includes current desktop and software that support reporting.	Project as a capability hardware that ad hoc reporting.
Business Analytical Services	Reporting	Standardization / Canned	No	The Hardware and Software includes current desktop and software that support standardized reporting.	Desktop and Project as a capability hardware and software that support reporting.
Support Services	Security Management	Encryption	No	The Hardware and Software includes current desktop software that supports encryption.	Desktop and Project as a capability hardware and software that supports encryption.
Support Services	Security Management	Digital Signature	No	The Hardware and Software includes current desktop software that supports digital signature.	Desktop and Project as a capability hardware and software that supports digital signature.
Support Services	Search	Query	No	The Hardware and Software includes current desktop software that supports query.	Desktop and Project as a capability hardware and software that supports query.
Support Services	Systems Management	Remote Systems Control	No	Help desk support of desktop systems via remote control now provided at four NASA Centers, with	

					other Centers planning to have the capability by the end of FY 2005.
Customer Services	Customer Initiated Assistance	Assistance Request	No		The Agency-wide administrative systems provide as a current capability the ability for users to request online a change to system configuration or to report a problem.
Business Management Services	Supply Chain Management	Sourcing Management	No		The NASA Acquisition Internet System (NAIS) is a Web-based procurement system designed to allow NASA to post business opportunities, competitive solicitations over \$25,000, and acquisition forecasts on the Internet for all NASA Centers.
Digital Asset Services	Document Management	Document Imaging and OCR	No		The Applications Services project includes COTS packages that provide document imaging and OCR capabilities. (Current capability)
Digital Asset Services	Document Management	Document Review and Approval	No		The Applications Services project includes COTS packages that provide document review and approval capabilities. (Current capability)

Digital Asset Services	Knowledge Management	Information Retrieval	No	The NASA Center for AeroSpace Information Services (CASI), which supports the review, capture, collection, organization, and dissemination to NASA, its contractors and grantees, and the public of the published results of NASA-sponsored and funded scientific and technical information, performs information retrieval.
Digital Asset Services	Knowledge Management	Information Sharing	No	The NASA Center for AeroSpace Information Services (CASI), which supports the review, capture, collection, organization, and dissemination to NASA, its contractors and grantees, and the public of the published results of NASA-sponsored and funded scientific and technical information, performs information sharing.
Business Analytical Services	Visualization	Mapping / Geospatial / Elevation / GPS	No	NASA Centers use COTS Geographic Information Systems as a tool for conducting facilities master planning and analysis.

Back Office Services	Human Resources	Time Reporting	No	(Current capability)
				<p>The Web-based Time and Attendance Distribution System (WebTADS) implements new Agency-standard rules for time and attendance data and provides timekeepers a means to enter and edit time worked information, and for supervisory personnel to review and certify timesheets.</p>
Back Office Services	Assets / Materials Management	Property Asset Management	No	<p>The NASA Equipment Management System (NEMS) provides NASA an Agency-wide system to simplify, standardize, and reduce the cost of tracking and managing equipment. NEMS is a transaction-based system that links every controlled equipment item to a unique equipment control number (ECN).</p>
Back Office Services	Human Capital / Workforce Management	Workforce Directory Locator	No	<p>The NASA X.500 directory contains employee locator information and can be accessed via web browser or via email clients. (Current capability)</p>

Support Services	Security Management	Role / Privilege Management	No	The Applications Services Project as a current capability includes role/privilege management associated with applications.
Business Management Services	Management of Process	Change Management	No	The NASA Automated Data Processing Consolidation Center (NACC) provides change management capabilities related to management of the data center hardware and software assets. (Current capability)
Business Management Services	Management of Process	Quality Management	No	The NASA Automated Data Processing Consolidation Center (NACC) provides capabilities related to management of the quality of data center products and processes. (Current capability)
Business Analytical Services	Analysis and Statistics	and Modeling	No	The NASA Automated Data Processing Consolidation Center (NACC) provides modeling capabilities for system/application capacity planning and performance purposes. (Current capability)
Back Office Data		Data Exchange	No	The NASA

Services	Management			Automated Processing Consolidation Center (NACC) provides data exchange capabilities. (Current capability)
Back Office Services	Data Management	Data Recovery	No	The NASA Automated Processing Consolidation Center (NACC) provides data recovery capabilities. (Current capability)
Support Services	Security Management	Access Control	No	The NASA Automated Processing Consolidation Center (NACC) provides access control capabilities. (Current capability)
Support Services	Systems Management	Systems Resource Monitoring	No	The NASA Automated Processing Consolidation Center (NACC) provides system resource monitoring capabilities. (Current capability)
Customer Services	Customer Preferences	Subscriptions	No	The Messaging and Collaboration service area includes as a current capability the ability of users to subscribe to a listserv or mailing list.
Customer Services	Customer Initiated	Online Help	No	The currently-in-place email, calendaring, and

	Assistance			collaborative tool desktop client software include online help capabilities.
Customer Services	Customer Initiated Assistance	Online Tutorials	No	Many of the currently-in-place email, calendaring, and collaborative tool desktop client software include online help capabilities.
Support Services	Security Management	Identification and Authentication	No	The currently-in-place email, calendaring, and collaborative tools capabilities of the messaging and collaboration service area include user identification and authentication.
Support Services	Security Management	Encryption	No	The currently-in-place email capabilities of the messaging and collaboration service area includes encryption.
Support Services	Security Management	Digital Signature	No	The currently-in-place email capabilities of the messaging and collaboration service area includes digital signature.
Support Services	Collaboration	Email	No	The Messaging and Collaboration service area includes email as a current capability.

Support Services	Collaboration	Threaded Discussions	No	The Messaging and Collaboration service area includes threaded discussions as a current capability.
-------------------------	----------------------	-----------------------------	-----------	--

27.1.3.2 Relationship to Technology Component Model

Table 53

Service Area	Service Category	Service Standard	Relation to SRM of FEA
Component Framework	Security	Certificates / Digital Signature	Yes - Direct map to TRM
Service Access and Delivery	Service Transport	Supporting Services	Network
Service Platform and Infrastructure	Hardware Infrastructure	Servers / Computers	Yes - Direct map to TRM
Component Framework	Data Management	Reporting and Analysis	Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Collaboration Communication	Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Web Browser	Yes - Direct map to TRM
Component Framework	Presentation Interface	Wireless / Mobile / Voice	Yes - Direct map to TRM
Service Platform and Infrastructure			Yes - Direct map to TRM
Service Platform and Infrastructure			Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Collaboration Communication	Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Collaboration Communication	Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Collaboration Communication	Yes - Direct map to TRM
Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Yes - Direct map to TRM

Service Access and Delivery	Access Channels	Intranet		Yes - Direct map to TRM
Service Platform and Infrastructure	Software Engineering	Integrated Development Environment (IDE)		Yes - Direct map to TRM
Service Platform and Infrastructure	Software Engineering	Software Configuration Management		Yes - Direct map to TRM
Service Access and Delivery	Service Requirements			Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Other Channels	Electronic	Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Other Channels	Electronic	Yes - Direct map to TRM
Component Framework	Security	Supporting Services	Security	Yes - Direct map to TRM
Component Framework	Security	Supporting Services	Security	Yes - Direct map to TRM
Service Platform and Infrastructure	Hardware Infrastructure	/ Servers / Computers		Yes - Direct map to TRM
Service Platform and Infrastructure	Hardware Infrastructure	/ Peripherals		Yes - Direct map to TRM
Service Platform and Infrastructure				Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Collaboration Communication		Yes - Direct map to TRM
Component Framework	Security	Supporting Services	Security	Yes - Direct map to TRM
Service Platform and Infrastructure	Hardware Infrastructure	/ Servers / Computers		Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Other Channels	Electronic	Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Other Channels	Electronic	Yes - Direct map to TRM
Component Framework	Security	Supporting Services	Security	Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Other Channels	Electronic	Yes - Direct map to TRM

Service Platform and Infrastructure				Yes - Direct map to TRM	
Service Platform and Infrastructure	Hardware Infrastructure	/	Wide Area Network (WAN)	Yes - Direct map to TRM	
Service Access and Delivery	Service Transport		Service Transport	Yes - Direct map to TRM	
Service Access and Delivery	Service Transport		Service Transport	Yes - Direct map to TRM	
Service Platform and Infrastructure				Yes - Direct map to TRM	
Service Access and Delivery	Service Transport		Supporting Services	Network	Yes - Direct map to TRM
Service Platform and Infrastructure				Yes - Direct map to TRM	
Service Platform and Infrastructure	Hardware Infrastructure	/		Yes - Direct map to TRM	
Service Platform and Infrastructure	Database Storage	/	Database	Yes - Direct map to TRM	
Service Platform and Infrastructure	Hardware Infrastructure	/		Yes - Direct map to TRM	
Service Platform and Infrastructure	Database Storage	/	Database	Yes - Direct map to TRM	
Service Access and Delivery	Service Transport		Service Transport	Yes - Direct map to TRM	
Component Framework	Security		Supporting Services	Security	Yes - Direct map to TRM
Service Access and Delivery	Access Channels		Web Browser	Yes - Direct map to TRM	
Service Access and Delivery	Access Channels		Web Browser	Yes - Direct map to TRM	
Service Access and Delivery	Access Channels		Web Browser	Yes - Direct map to TRM	
Service Platform and Infrastructure				Yes - Direct map to TRM	
Service Access and Delivery	Access Channels		Collaboration Communication	Yes - Direct map to TRM	

Service Platform and Infrastructure				Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Collaboration Communication		Yes - Direct map to TRM
Service Access and Delivery	Access Channels	Web Browser		Yes - Direct map to TRM
Service Access and Delivery	Service Requirements	Authentication Sign-on (SSO)	/ Single	Yes - Direct map to TRM
Service Access and Delivery	Service Transport	Supporting Services	Network	Yes - Direct map to TRM

27.1.3.3 Partnerships

NASA will continue to look for every opportunity to leverage existing components and applications across the government. The Agency will continue to participate actively in the E-Gov initiatives, building upon the partnerships established through agreements with the managing partners for E-Authentication, E-Travel, E-Payroll, Integrated Acquisition Environment, and Federal Asset Sales. NASA currently has links directly to FirstGov from the home page within the OneNASA portal, and is making use of DISA’s XML registry as opposed to building an Agency unique solution.

27.1.4 Security and Privacy

27.1.4.1 How is it provided and funded?

IT security within NASA is addressed in a layered approach that manages security from the Agency Level, Center level, Program/Project and then system level.

The Agency addresses security by defining security policies and procedures that are implemented at the Agency, Center, Program/Project and system levels. The primary policy and guidance documents used are the NASA Policy Directive (NPD) and the NASA Procedures and Guidance (NPG) 2810 documents used in conjunction with the NIST standards and Special Publications.

NASA currently uses both token and Public Key technologies for strong authentication. The tokens are used both at the Center as well as the Program/Project and system level for two factor authentication to gain access to resources or data. The PKI is used across the Agency for secure messaging, digital signature as well as encrypted file storage and sharing. NASA was an early adopter of PKI, infrastructure was put into place over five years ago and was one of the first Agencies to cross certify with the Federal Bridge Authority. NASA has started to replace the existing failing and fragmented physical access control system with a single Agency wide system

for issuing badges that uses SmartCard technology. This is being worked through GSA and is expected to take several years to complete. The first phase, scheduled to be completed in the next 12 months is to replace the current aging systems for issuing and managing badges at each Center and to re-badge all employees. This first phase also provides SmartCards for a selected number of critical computer systems for access control. Over the next several years NASA will continue to expand the computer systems that are integrated into the SmartCard system.

The Agency has implemented a defense in-depth approach using firewall, VPN and IDS technologies. Each of these technologies is continually reviewed to ensure that the security controls perform as originally accepted and the threat situation reevaluated to determine if any changes requires updating or replacing the current security controls.

NASA manages its own wide area network (WAN) and monitors traffic passing between the NASA WAN and the Internet as well as implements rules to block unwanted traffic and probes. Each Center has a series of firewalls implemented at their perimeters supporting three different security zones. Each Program and or Project depending on the risk analysis and appropriate security controls may implement an additional firewall. In addition, NASA has implemented an Agency VPN service supporting remote and wireless services.

NASA has installed an IDS that monitors the network traffic moving between the different security zones at the Agency, Center and specific Program/Project and system levels.

27.1.4.2 *How is security accomplished?*

The existing systems used at the Agency, Center and Program/Project and system level all have approved ITS Plans in place following approved policy, standards, procedures and guidance. The new projects NAMS, CIMS and NSP each have an ITS plan under development as part of the beginning phase of the life cycle of each system. Since the number of plans is extensive (over 800), the list is provided under separate cover.

Please note: The information provided below for security plan date, review date, and test date is currently being reviewed and will be revised with the submission of the next FISMA report. NASA follows approved NASA policy and guidance documents NPD and NPG 2810 that are currently being updated to reflect the current direction from NIST. NASA Systems all have IT Security Plans and have been authorized to process following approval policies and procedures.

NASA has had an Incident Response capability for the last 15 years. NASA has constructed an Agency approach to IDS that utilizes data from the Agency and Center level IDSs and is reviewed by the Agency security operations of the NASA WAN Network Operations Center (NOC) combined with reviews conducted by NASIRC personnel. NASIRC and the NASA WAN NOC share this responsibility to produce a 24X7 operational capability. NASIRC is also responsible for operating the NASA system for recording and reporting all incidents associated with all NASA systems, internally and to FedCIRC. This information is shared with the Centers and the OIG's Office. NASA procedures for reporting incidents requires all incidents to be reported to NASRIC for reporting and tracking and to the OIG for investigation.

All participants in the NASA Integrated Information Infrastructure Program must comply with current NASA security policies regarding access to networks, servers, applications, and computers.

The NASA Federal Acquisition Regulations (FAR) Supplement section 1804.470 addresses IT security requirements in contracts. It requires that all contracts in which the contractor must have physical or electronic access to NASA's sensitive information in unclassified systems contain security requirements and that the contractor's approach to ensuring IT security be evaluated along with other technical requirements. The IT security requirements are implemented using NASA clause 1852.204-76, which requires contractors to comply with the security requirements outlined in NASA Procedures and Guidelines (NPG) 2810, "Security of Information Technology." Contractors demonstrate their compliance by submitting an IT Security Plan for approval after contract award and meeting the requirements of NPG 2810 regarding personnel screening and IT security awareness and training. In evaluating the contractor's performance, IT security is validated by following a surveillance plan for monitoring the contract. Failure to meet the IT security requirements frequently is cause of contract termination.

The clause above was incorporated into all applicable existing contracts by April 2002. NASA procurement requirements for IT security are frequently updated as NASA's IT security program matures, the last update being Procurement Information Circular 03-16, dated June 23, 2003.

27.1.4.3 *Effective use of security, controls and authentication tools*

Public access to NASA information is through NASA's publicly accessible Web sites. NASA follows OMB's policy on Web site privacy entitled "Privacy Policies on Federal Web Sites." In accordance with this policy and to ensure the protection of data obtained from the public, NASA has promulgated a directive that requires Center CIOs to publish Web site privacy statements, ensure Center compliance with the privacy statement, use persistent cookies sparingly, and track the use of these cookies. If authentication is required for a public site, web authentication tools are used to ensure confidentiality. Finally, at the network level, the agency uses an IT security infrastructure based on defense in depth principles to safeguard its systems. These defensive measures include screening routers, intrusion detection systems, and firewalls.

27.1.5 Government Paperwork Elimination Act

NASA's Integrated Information Infrastructure Program provides the hardware, software, and telecommunications support for some of the systems that support electronic transactions and recordkeeping covered by GPEA. For example, under the Application Services Component, the NASA Acquisition Internet Service (NAIS) provides synopses, solicitations, award notices, acquisition forecasts, regulations, forms, and small business assistance to current and potential agency business partners via the World Wide Web. Systems maintained by NASA's Center for Aerospace Information (CASI) support the review, capture, collection, organization, and dissemination of NASA's published scientific and technical information to NASA employees, contractors and grantees, and the general public. Electronic transactions related to NAIS and CASI are described in detail in the agency's GPEA plan and subsequent progress reports.

October 31, 2000 is the date (see below) of NASA's original GPEA plan. Annual progress reports have been submitted since that date, most recently on July 1, 2003.