

AWARD/CONTRACT	1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 350)	RATING	PAGE OF PAGES 1 235
-----------------------	---	--------	------------------------

2. CONTRACT (Proc Inst Ident) NO. HSTS03-06-D-CIO500	3. EFFECTIVE DATE January 7, 2006	4. REQUISITION/PURCHASE REQUEST/PROJECT NO. 21-06-206C10500
---	--------------------------------------	--

5. ISSUED BY Transportation Security Administration 601 South 12 th Street Arlington, VA 22202	6. ADMINISTERED BY (if other than item 5)
--	---

7. NAME AND ADDRESS OF CONTRACTOR (No. street, county, state and ZIP Code) Unisys Corporation 11720 Plaza America Drive Tower III Reston, VA 20190	8. DELIVERY <input type="checkbox"/> FOB ORIGIN <input checked="" type="checkbox"/> OTHER (See below)
--	--

10. SUBMIT INVOICES (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN:	ITEM See Section G
--	-----------------------

11. SHIP TO/MARK FOR N/A	12. PAYMENT WILL BE MADE BY See Section G
-----------------------------	--

13. AUTHORITY FOR USING OTHER FULL AND OPEN COMPETITION: <input type="checkbox"/> 10 U.S.C. 2304(c) <input checked="" type="checkbox"/> 41 U.S.C. 253(c)(1)	14. ACCOUNTING AND APPROPRIATION DATA N/A
--	--

15A. ITEM NO.	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
	See Section B				The ceiling price for this contract is \$750 M

15G. TOTAL AMOUNT OF CONTRACT

16. TABLE OF CONTENTS								
(✓) SEC.	DESCRIPTION			PAGE(S)	(✓) SEC.	DESCRIPTION		PAGE(S)
PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES				
X	A	SOLICITATION/CONTRACT FORM			X	I	CONTRACT CLAUSES	
X	B	SUPPLIES OR SERVICES AND PRICE/COST			PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.			
X	C	DESCRIPTION/SPECS./WORK STATEMENT			X	J	LIST OF ATTACHMENTS	
X	D	PACKAGING AND MARKING			PART IV - REPRESENTATIONS AND INSTRUCTIONS			
X	E	INSPECTION AND ACCEPTANCE			K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS		
X	F	DELIVERIES OR PERFORMANCE			L	INSTRS., CONDS., AND NOTICES TO OFFERORS		
X	G	CONTRACT ADMINISTRATION DATA			M	EVALUATION FACTORS FOR AWARD		
X	H	SPECIAL CONTRACT REQUIREMENTS						

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

17. CONTRACTOR'S NEGOTIATED AGREEMENT (Contractor is required to sign this document and return ___ copies to issuing office.) Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (Attachments are listed herein.)

18. AWARD (Contractor is not required to sign this document.) Your offer on Solicitation Number _____ including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the items listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your offer, and (b) this award/contract. No further contractual document is necessary.

19A. NAME AND TITLE OF SIGNER (Type or print)
Marlene L. Emmons, Sr. Manager of Contracts
Unisys Corporation

20A. NAME OF CONTRACTING OFFICER
Christopher E. Zelaznik

19B. NAME OF CONTRACTOR
Marlene L. Emmons
(Signature of person authorized to sign)

19C. DATE SIGNED
12/30/05

20B. UNITED STATES OF AMERICA
Christopher E. Zelaznik
(Signature of Contracting Officer)

20C. DATE SIGNED
12/30/05

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # i
-----------------	------------------------------------	--	-------------

TABLE OF CONTENTS

B.1	SCHEDULE OF SUPPLIES AND SERVICES AND PRICES/COSTS	2
B.2	UPDATED SECTION B TABLES	2
B.3	ESTIMATED CONTRACT VALUE	2
B.4	BURDENED RATES (APPLICABLE TO TIME AND MATERIALS ORDERS ONLY)	2
C.1	BACKGROUND	3
C.2	SCOPE OF WORK	3
C.3	CURRENT ENVIRONMENT	5
C.3.1	User Population	5
C.3.2	Seats	5
C.3.3	Facilities	5
C.3.4	Sites	5
C.4	REQUIREMENTS	6
C.4.1	Requirements Objectives	6
C.4.1.1	Partnership Philosophy	7
C.4.1.2	Desired Results	8
C.4.1.3	Transition of Existing Services/Work in Progress	8
C.4.1.4	Staff	9
C.4.2	Network Management	9
C.4.2.1	Command Information Center	13
C.4.2.2	Security Management	14
C.4.2.3	Interoperability	14
C.4.2.4	Service Level Agreements (SLAs)	14
C.4.2.5	DHSNet	15

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # ii
----------	------------------------------------	--	--------------

C.4.3	Global Managed Services	15
C.4.3.1	Capacity Management	15
C.4.3.2	Configuration Management	17
C.4.3.3	Image Management	19
C.4.3.4	Change Management	19
C.4.3.5	Configuration Reporting	21
C.4.3.6	Review/Control Boards	21
C.4.3.7	Software Management	21
C.4.3.8	Equipment Maintenance	25
C.4.3.9	Spare Parts	27
C.4.3.10	Warranty	28
C.4.3.11	Equipment Refresh	29
C.4.3.12	Asset Management	29
C.4.3.13	Contingency Planning	31
C.4.3.14	Online Catalog of Services	33
C.4.3.15	Deployment of Products and/or Services	34
C.4.3.16	Help Desk Services	35
C.4.3.17	Installation, Moves, Adds, Changes (IMAC)	42
C.4.3.18	Software Support	45
C.4.3.19	Operational Infrastructure Security	47
C.4.3.20	Work Breakdown Structure (WBS)	55
C.4.3.21	Compliance with SDLC	55
C.4.3.22	Subject Matter Expert (SME) Support Services	55
C.4.4	Desktop Managed Services	55
C.4.4.1	Seat Management	56
C.4.4.2	Peripheral Devices	58

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # iii
-----------------	------------------------------------	--	---------------

C.4.4.3	Personal Wireless (PDA and PED)	59
C.4.4.4	Service Provisioning	59
C.4.4.5	Grades of Service	61
C.4.5	Managed Network Services	61
C.4.5.1	Performance Management	63
C.4.5.2	Monitor Network Performance	68
C.4.5.3	Operations and Maintenance	68
C.4.5.4	LAN	69
C.4.5.5	WAN	69
C.4.5.6	VPN Services	70
C.4.6	Telecommunications Services—CONUS/OCONUS	70
C.4.7	Special Services/Systems	77
C.4.7.1	Electronic Surveillance	77
C.4.7.2	Managed Applications Services	77
C.4.7.3	Email Services	78
C.4.7.4	Internet Services	79
C.4.7.5	Intranet Services	79
C.4.7.6	Extranet Services	79
C.4.7.7	Proxy Services	79
C.4.8	Data Center Operations Management	81
C.4.8.1	Maintenance Records	82
C.4.8.2	Audits	82
C.4.8.3	Data Center Disaster Recovery	82
C.4.8.4	Operations Process and Planning	83
C.4.8.5	Operations Support	83
C.4.8.6	Server Management	84

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # iv
C.4.8.7	Storage Management		85
C.4.8.8	Database Management		86
C.4.8.9	Backup and Recovery		86
C.4.8.10	Tape Operations		87
C.4.8.11	Participation on Boards		87
C.4.8.12	Network Security Operations		87
C.4.8.13	Security Audits/Audit Log		88
C.4.8.14	Network Intrusion Devices/Host Intrusion Devices		88
C.4.8.15	Firewall support		88
C.4.9	Infrastructure Engineering		88
C.4.9.1	Tier III support		90
C.4.9.2	Software Upgrades/Patch Implementation		91
C.4.9.3	Internet Protocol Telephony (IPT)		92
C.4.10	Testing		94
C.4.10.1	Integration Testing		95
C.4.10.2	Subsystem/System Testing		95
C.4.10.3	Security Testing		95
C.4.10.4	Acceptance Testing		95
C.4.10.5	Product/Service Acceptance		96
C.4.11	Program Management		97
C.4.11.1	Program Office		97
C.4.11.2	Progress Reports		98
C.4.11.3	Risk Management		99
C.4.11.4	Issues Management		100
C.4.11.5	Performance Standards and Quality Assurance Plan (QAP)		100
C.4.11.6	Co-Chair of Configuration Control Board and Change Management Review Board		100

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # v
C.4.12	Project Management		101
C.4.13	Additional Services		102
C.4.14	Documentation		102
C.5	SPECIAL SITE REQUIREMENTS		103
C.5.1	TSA Headquarters		103
C.5.2	TSOC		105
C.5.2.1	Management		106
C.5.2.2	Tier II support		107
C.5.2.3	Tier III support		107
C.5.2.4	Operations		108
C.5.2.5	Monthly Progress Report Requirements		109
C.5.2.6	Government Property		110
C.5.2.9	TSOC Disaster Recovery		111
C.5.3	IT Requirements in support of International Programs		114
C.5.4	TSA Cat X and Cat 1 Airport locations		117
C.6	DHS HEADQUARTERS		121
C.6.2	DHS HEADQUARTERS PERFORMANCE WORK STATEMENT REQUIREMENTS		121
C.6.2.1	BACKGROUND		121
C.6.2.1.1	Baseline Services		121
C.6.2.2	SCOPE OF DHS HEADQUARTERS WORK		121
C.6.2.3.2	Facilities:		123
C.6.2.4	REQUIREMENTS		124
C.6.2.4.1	List of Applicable Laws, Regulations, Policies, and Guidelines		124
C.6.2.4.3	Deliverables		125
C.6.3	TASK ORDER OBJECTIVES STATEMENT		126

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # vi
----------	------------------------------------	--	--------------

C.6.3.1.	Task Order Information	126
C.6.3.1.2.	Statement of Work Description	126
C.6.4.1.	PROGRAM MANAGEMENT SERVICES	139
C.6.4.1.1.	KEY INTEGRATION FUNCTIONS OF THE PMO	141
C.6.4.1.2.	PROGRAM MANAGEMENT OFFICE STRUCTURE	144
C.6.4.1.3.	GOVERNMENT PROPERTY REPORT	144
C.6.4.1.4.	SEAT MANAGEMENT	144
C.6.4.2.	ENGINEERING OPERATIONS	145
C.6.4.2.2.	On-Site Engineering Support	148
C.6.4.2.4.	Technical Services Management	151
C.6.4.3.	END USER SERVICES	162
C.6.4.3.1	Help Desk Services (SPOC) – Tier 1 Support Team	162
C.6.4.4.	APPLICATION SERVICES	169
C.6.4.4.1.	Infrastructure Maintenance Services	169
C.6.4.4.2.	Availability of Qualified Personnel and Approved Maintenance Downtime	169
C.6.4.4.3.	DHS-Approved Maintenance Downtime	169
C.6.4.4.4.	Materiel Transportation and Travel Requirements	169
C.6.4.4.5.	Application Status and Performance Reports	169
C.6.4.5.	SECURITY SERVICES	173
C.6.4.5.1.	Requirements Definition	173
C.6.4.5.2.	Key Responsibilities	173
C.6.4.5.3.	Contingency Planning	173
C.6.4.5.4.	DHS' Desired Approach to Solution	174
C.6.4.5.5.	Work Order Management Structure and Approach	174
C.6.4.5.6.	Team Structure	175
C.6.4.5.7.	Approach	175

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page #. vii
-----------------	------------------------------------	--	----------------

C.6.4.5.8. Solutions	176
C.6.4.5.9. Information Security Policy and Planning	177
C.6.4.6. ASSET INVENTORY MANAGEMENT	189
C.6.4.6.2. Asset Inventory Control	191
APPENDIX A – PROGRAM MANAGEMENT SERVICES WBS	194
APPENDIX B – ENGINEERING OPERATIONS WBS	198
APPENDIX D – APPLICATION SERVICES WBS	203
APPENDIX E – SECURITY SERVICES WBS	204
APPENDIX F – ASSET INVENTORY MANAGEMENT WBS	206
APPENDIX H – SERVICE LEVEL AGREEMENTS	210
D.1 PACKAGING AND MARKING	232
E.1 GENERAL	233
E.2 TSA 3.1.1 CLAUSES INCORPORATED BY REFERENCE	233
F.1 CLAUSES INCORPORATED BY REFERENCE (TSA 3.1.1)	234
F.2 PERIOD OF PERFORMANCE	234
F.3 PLACE OF PERFORMANCE	234
F.4 DELIVERY OF REPORTS	234
F.5 DELIVERABLES	234
F.6 DATA ITEMS	235
F.7 SUBCONTRACT REPORTS	235
F.8 MONTHLY SUBCONTRACTING ACTIVITY REPORT (MSAR)	236
F.9 VENDOR REPORT: CONTRACTUAL FINANCIAL OPERATIONS AND PROJECTIONS	236
F.10 TRANSITION TO OWNERSHIP/TRANSITION TO REMOVAL (TTO/TTR) REPORT	237

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # viii
-----------------	------------------------------------	--	----------------

G.1	CONTRACT OFFICER (CO)	241
G.2	CONTRACT OFFICER'S TECHNICAL REPRESENTATIVE (COTR) AND TECHNICAL MONITORS	241
G.3	ORDERING (TSA 3.2.4.16) (JUN 2005)	243
G.4	ACCOUNTABILITY OF COSTS/SEGREGATION OF TASK ORDERS	243
G.5	INVOICE REQUIREMENTS	244
G.7	METHOD OF PAYMENT	246
G.8	PRICING OF ADJUSTMENTS	246
G.9	TRAVEL AND PER DIEM (APPLICABLE TO T&M ORDERS ONLY)	247
G.10	IMPLEMENTATION OF TASK/DELIVERY ORDERS	247
G.11	PURCHASE AGENT AUTHORITY	247
G.12	GOVERNMENT-FURNISHED FACILITIES AND EQUIPMENT	248
H.1	TYPE OF CONTRACT (TSA 3.2.4.1) (FEB 2003)	249
H.2	EQUAL OPPORTUNITY PREAWARD CLEARANCE OF SUBCONTRACTS (TSA 3.6.2.10) (FEB 2003)	249
H.3	INSURANCE (TSA 3.4.1.12) (FEB 2003)	249
H.4	INSURANCE-WORK ON A GOVERNMENT INSTALLATION (TSA 3.4.1.10)	250
H.5	AUTHORIZED USERS	251
H.6	DISCLOSURE OF INFORMATION	251
H.7	STANDARD CONDUCT AT GOVERNMENT INSTALLATIONS	251
H.8	SUBSTITUTION OF KEY MANAGEMENT PERSONNEL	251
H.9	SUBSTITUTION OF KEY PERSONNEL FOR DELIVERY AND TASK ORDERS	252

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # ix
-----------------	------------------------------------	--	--------------

H.10	ORGANIZATIONAL CONFLICT OF INTEREST	253
H.11	CONTRACTOR'S RESPONSIBILITY FOR ASSIGNED SPACE, EQUIPMENT, AND SUPPLIES	254
H.12	WARRANTY PERIOD	254
H.13	PUBLICITY AND DISSEMINATION OF CONTRACT INFORMATION	254
H.14	PROCEDURES FOR CORRESPONDENCE	254
H.15	PERSONNEL ACCESS	255
H.16	INTERRELATIONSHIP OF ASSOCIATE CONTRACTORS	255
H.17	PERMITS	255
H.18	PRODUCT SUBSTITUTIONS	255
H.19	SPECIAL PROJECTS	255
H.20	ENHANCEMENTS OR SPECIALIZED EQUIPMENT TO ACCOMMODATE USERS WITH DISABILITIES (SECTION 508 OF THE REHABILITATION ACT)	256
H.21	COMMERCIALY AVAILABLE ITEMS	256
H.22	LABOR CATEGORIES – DELETED, (DELETE TABLE)	256
H.23	NON-PERSONAL SERVICES	257
H.24	CONTRACTOR RESPONSIBILITIES	258
H.25	QUALIFICATIONS OF EMPLOYEES	258
H.26	NON-DISCLOSURE AGREEMENTS	258
H.27	TSA DATA PROTECTED BY THE PRIVACY ACT	259
H.28	TSA REQUIREMENTS AND DUTIES FOR HANDLING SENSITIVE SECURITY INFORMATION (SSI)	259
H.29	PRE-EMPLOYMENT INVESTIGATIVE STANDARDS FOR CONTRACTORS	259

Contract	Document No.	Document Title	Page #
	HSTS03-06-D-CIO500	ITMS Bridge Contract	x
H.30		DHS MENTOR-PROTÉGÉ PROGRAM (DEC 2003)	260
H.31		OPTION TO EXTEND THE TERM OF THE CONTRACT (TSA 3.2.4-35) (FEB 2003)	260
H.32		OBSERVANCE OF LEGAL HOLIDAYS	261
H.33		ORDER OF PRECEDENCE	262
H.34		COST DISCLOSURE	262
H.35		USE OF PRICING TOOLS	262
H.36		BILLING AND PRICING	262
I.1		TSA 3.1.1 CLAUSES INCORPORATED BY REFERENCE	263
I.2		RESERVED	265
I.3		NOTIFICATION OF OWNERSHIP CHANGES (TSA 3.2.2.3.37) (FEB 2003)	265
I.4		REQUESTS FOR CONTRACT INFORMATION (TSA 3.2.2.3.75) (FEB 2003)	265
I.5		OFFICIALS NOT TO BENEFIT (TSA 3.2.5.1) (FEB 2003)	265
I.6		RESERVED	266
I.7		WHISTLEBLOWER PROTECTION FOR CONTRACTOR EMPLOYEES (TSA 3.2.5.8) (FEB 2003)	266
I.8		TSA COST PRINCIPLES (TSA 3.3.2.1) (FEB 2003)	266
I.9		ERRORS AND OMISSIONS (TSA 3.4.1.13) (FEB 2003)	267
I.10		UTILIZATION OF SMALL BUSINESS CONCERNS (TSA 3.6.1.3) (FEB 2003)	267
I.11		RESERVED	268
I.12		LIQUIDATED DAMAGES – SUBCONTRACTING PLAN (TSA 3.6.1.6) (FEB 2003)	268
I.13		AFFIRMATIVE ACTION FOR SPECIAL DISABLED AND VIETNAM ERA VETERANS – (TSA 3.6.2.12) (FEB 2003)	269

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # xi
-----------------	------------------------------------	--	--------------

I.14	AFFIRMATIVE ACTION FOR WORKERS WITH DISABILITIES (TSA 3.6.2-13) (FEB 2003)	272
I.15	NOTICE OF DELAY (TSA 3.10.1.24) (FEB 2003)	273
I.16	SUBCONTRACTS FOR COMMERCIAL ITEMS (TSA 3.10.2.6) (FEB 2003)	273
I.17	DEFINITIONS - --GOVERNMENT PROPERTY (TSA 3.10.3.1) (FEB 2003)	274
I.18	SEGREGATION OF GOVERNMENT PROPERTY (TSA 3.10.3.13) (FEB 2003)	278
I.19	INVENTORIES (TSA 3.10.3.14) (FEB 2003)	279
I.20	DISPOSITION OF GOVERNMENT PROPERTY (TSA 3.10.3.15) (FEB 2003)	280
I.21	SEAT BELT USE BY CONTRACTOR EMPLOYEES (TSA 3.13.5) (FEB 2003)	281
I.22	CONTRACTOR PERSONNEL SUITABILITY REQUIREMENTS, AS PER U.S. DHS MANAGEMENT DIRECTIVE NO. 11055 AND TSA MANAGEMENT DIRECTIVE NO. 2800.71 AND ALL UPDATES	281
I.23	SENSITIVE UNCLASSIFIED INFORMATION (SUI) (TSA 3.14.5) (FEB 2003)	283
I.24	PUBLIC COMMUNICATION (TSA 3.14.7) (JAN 2005)	284
	SECTION J – LIST OF ATTACHMENTS	285

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 2
-----------------	------------------------------------	--	-------------

PART I - THE SCHEDULE

SECTION B—SUPPLIES AND SERVICES AND PRICES/COSTS

B.1 SCHEDULE OF SUPPLIES AND SERVICES AND PRICES/COSTS

The Transportation Security Administration (hereafter referred to as TSA, the Government, or we) requires the Contractor to provide all of the Contract Line Items (CLINs) incorporated as Attachment 6, Section J. These CLINs specify pricing for each of the deliverables and data items (see Section F) associated with the scope and objectives described in Section C of this contract. While the Government expects to procure most or all of these CLINs, we reserve the right to award some, all, or none of these CLINs at Government discretion option.

The total minimum amount the Government will acquire under this contract is \$1 million.

CLINs provided in the B-Table Section B represent those CLINs the Contractor has identified thus far for transfer to the ITMS Bridge Contract. The Contractor shall work to finalize this list during the transition phase from the existing ITMS Task Order to the ITMS Bridge Contract.

B.2 UPDATED SECTION B TABLES

The Contractor shall provide updated, electronic Section B tables on a monthly basis on the 15th of each month to the Contract Officer. The Section B Tables contain the labor categories and labor rates as well as information regarding the ITMS CLINs. The updated Section B tables will be incorporated into the contract via contract modification on a monthly basis.

B.3 ESTIMATED CONTRACT VALUE

The combined value of all orders issued under this contract is estimated at \$750,000,000.00.

B.4 BURDENED RATES (APPLICABLE TO TIME AND MATERIALS ORDERS ONLY)

Fixed loaded labor rates shall include all direct labor costs, indirect costs, overhead, general and administrative (G&A) expenses, and profit.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 3
-----------------	------------------------------------	--	-------------

SECTION C—DESCRIPTION/SPECIFICATIONS/PERFORMANCE WORK STATEMENT

C.1 BACKGROUND

In response to the events of 11 September 2001, TSA was established via the Aviation and Transportation Security Act to support the Administration's mandate to improve the security of the nation's transportation systems.

The Information Technology Managed Services (ITMS) Program provides the Transportation Security Administration (TSA) with day-to-day operational Information Technology (IT) services necessary for TSA users of voice, video and data computational capabilities, as well as, connectivity and interface with the Border and Transportation Security (BTS), the Department of Homeland Security (DHS) and external law enforcement entities for their overall mission achievement. The existing IT requirement could expand due to the addition of inter-modal requirements (rail/highway/transit/maritime/pipeline/infrastructure, etc.) requiring core IT infrastructure augmentation and enhancements.

The Associate Under-Secretary for Information Technology and Chief Information Officer has the responsibility to provide all IT equipment, infrastructure and management services requisite to meet TSA operational needs, and ensure those services are efficient, timely, cost-effective and meet established performance levels.

The ITMS Program objectives are as follows:

- Ensure that TSA and DHS staff continue to have the computing and communications hardware, software and services required at the best value to the Government;
- Ensure that the IT capabilities can accommodate surges in demand and changes in types of demands for IT capabilities;
- Ensure that contracting arrangements are flexible enough to accommodate changes in capability "ownership," i.e., transition core capabilities to DHS when the Department is capable of providing the necessary services;
- Ensure that the appropriate controls are in place to prevent the loss or misuse of taxpayer resources; and
- Ensure that the contracting arrangements and acquisition vehicles provide the best possible value to taxpayers

C.2 SCOPE OF WORK

The Contractor shall provide the IT, voice and data telecommunications, and related services to provide and manage an architecture and IT infrastructure that is timely, standardized, stable, reliable, secure, flexible, responsive, compliant, with applicable standards, statutes and departmental mandates, and cost effective in meeting the needs of TSA and its stakeholders.

The Contractor shall provide the IT and telecommunications services as ordered to include, but not limited to: hardware, software, maintenance, asset tracking, help desk, security, data center, WAN/LAN, server, wireless, PDA, land mobile radio, voice and data telecom, training and program management that meet or exceed TSA's ITMS Program objectives (Section C.1).

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 4
-----------------	------------------------------------	--	-------------

The Contractor shall provide the services needed to analyze requirements, develop and implement recommended solutions, and operate all IT products and services needed to deploy, as well as maintain, IT and telecommunication services for TSA.

The Contractor shall provide services in response to this PWS at, but not limited to, any of the following designated TSA locations:

- TSA Headquarters in Arlington, VA
- TSA Hosting Center in St. Louis, MO
- 600+ CONUS/OCONUS airports (onsite & offsite location included) (Contractor proposed labor rates are for use within the United States, including Alaska and Hawaii. Other OCONUS requirements will be reviewed on a case-by-case basis, as requested.)
- Approximately 150 Federal Security Director (FSD) offices
- Transportation Security Operations Center (TSOC)
- Primary and alternate COOP locations
- 5 Mission Support Center offices
- Approximately 25 Specialized mission locations (IE: TSIS, STDO, CSOC, ONRA, training facilities)
- Approximately 18 International Regional Support offices

The Contractor shall provide support for several major and minor future projects during this bridge period which will be initiated in accordance with Section G.3 "Ordering" to continue the technology expansion begun during ITMS. Some of these major projects are as follows:

- Voice over Internet Protocol (VoIP)
- Multi-Protocol Label Switching (MPLS)
- Full Hi-SOC LAN/WAN Connectivity for the TSA controlled spaces at 50-75 additional airport and office locations
- Application integration projects
- Desktop software enhancement projects
- SDLC Requirement

The Contractor shall support and extend the TSA operational environment in accordance with requirements set forth in this PWS. The technological environment includes, but is not limited to:

- LAN/WAN network equipment, Microsoft Windows servers, desktops, and laptops will be refreshed using the same OEMs currently supported under ITMS
- The TSA standard desktop and laptop office automation software will be upgraded to Microsoft Office 2003
- Implement and support an automated software distribution and patch management system
- Implement and support an upgrade to the BlackBerry Enterprise Server version 4.0
- Quantities in the existing infrastructure are approximately:
 - 263 routers
 - 613 switches
 - 18,188 desktop and laptop Seats
 - 2 Microsoft Domains
 - 70,523 Microsoft Exchange mailboxes
 - 4,579 local and network printers
 - 300 Personal Communications devices (RIM Blackberries)
 - 444 Uninterruptible Power Supplies
 - 724 Equipment Cabinet Sensors
 - 6 Application Server Load Balancers
 - 2 Virtual Private Network (VPN) Concentrators.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 5
-----------------	------------------------------------	--	-------------

C.3 CURRENT ENVIRONMENT

C.3.1 User Population

1. Total Number of Users: 56,000
 - a) Number of users in HQ: 1,900
 - b) Other large groups of users: 45,000 (Screeners)

C.3.2 Seats

The Contractor shall provide seat support services for the following estimated quantities of Information Technology (IT) equipment.

1. Number of desktop PCs: 13,110
2. Number of laptops: 5,088
3. Number of routers: 251
4. Number of switches: 605
5. Number of circuits (major): 250
6. Number of cellular devices (leased): 3,651 (*numbers are dynamic*)
7. Number of cellular devices (Government Property): 4,016 (*numbers are dynamic*)
8. Production Servers: 457 (includes 24 UNIX servers)
9. Printers: 4579

C.3.3 Facilities

1. Number of data centers: 2 (St Louis, MO; Arlington, VA)
2. Number of data center servers: 457
3. Number of integrated test facilities: 1 (Reston, VA)

C.3.4 Sites

1. Number of Sites: 900+
2. Number of Airports: 471

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 6
-----------------	------------------------------------	--	-------------

C.4 REQUIREMENTS

Managed Services is an efficient and effective way to handle systems monitoring and management. The Contractor shall provide TSA with a performance-based managed services agreement that establishes and then maintains IT and telecommunications infrastructure support and services for more than 50,000 TSA employees, TSA Headquarters, over 400 airports, and numerous operational field sites.

Under this managed services agreement, the Contractor shall provide to TSA IT and telecommunications services to include hardware and software services, help desk services, application services, and telecommunication services to TSA. Performance evaluation standards (SLAs) shall be used to measure delivery of services, based on defined service levels. Performance evaluation factors will be utilized to assess quality of service. Required service levels are conveyed in subsequent paragraphs of this Performance Work Statement and Attachment 5 (See Section J). Satisfactory Contractor performance, defined as meeting or exceeding the baseline performance objectives as provided in the Performance Management Incentive Plan (PMIP), will determine the Contractor's eligibility for incentive payments as detailed in the PMIP Attachment 5, Section J.

C.4.1 Requirements Objectives

The objective of TSA's ITMS requirement is to efficiently, effectively, and economically maintain and enhance a standard IT platform and infrastructure to support TSA employees in meeting TSA's mission. As such, the objectives of this contract are to:

- 1) Receive, under a performance-based arrangement, highly reliable and secure, IT managed services and support that meets or exceeds customer requirements and expectations;
- 2) Continuously seek ways to apply IT to improve TSA mission performance;
- 3) Throughout the life of this effort, demonstrate improved performance; reliability, security, and reduced cost of the delivered service;
- 4) The Government intends to move from a leased to an owned or furnished environment for all equipment, software and licenses. The Government will progressively assume ownership of equipment, parts, software, and licenses as the lease arrangement for these service related components expire. The Government will purchase through the contract and assume ownership for all newly acquired service related equipment, parts, software or licenses typically listed as "other direct costs". The Government may grant an exception to this requirement, typically in cases where the equipment, part or software supports a service provided by the Contractor through a shared environment. Exceptions shall be provided by the Government on a case by case basis through signed acknowledgement of the COTR;
- 5) Transition legacy IT services to emerging DHS service providers in 2006 and beyond. These activities are anticipated to include Web services, data centers, infrastructure, email/active directory, NOC/SOC, and desktop standardization;
- 6) Maintain the highest level of service consistent with cost effectiveness;
- 7) Be able to provide audit and oversight activities as convincing proof that TSA is receiving superior service at a fair and reasonable price;
- 8) Provide an effective and efficient management information system that provides insightful, accurate, and timely information and data on program status and performance reporting;

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 7
-----------------	------------------------------------	--	-------------

- 9) Develop, implement, and maintain appropriate inventory, security, quality control, architecture standards, and reporting requirements;
- 10) Develop and provide a system that supports TSA's compliance with Government and Industry standards and requirements (e.g., Clinger-Cohen architecture and program oversight, security, etc);
- 11) Receive appropriate data rights as well as cooperation for any transition to another provider to ensure continuity of service in the unlikely event of contract termination, or in the event this effort undergoes re-competition;
- 12) Transition of IT Equipment. In order to initiate the transition of IT equipment from leased services to government owned/furnished equipment, the government will execute the applicable TTO or TTR CLIN at the end of the lease term (i.e., 36 or 60 months);
- 13) In the event of termination, in whole or in part, for any reason, of the ITMS Bridge Contract, the government will execute the applicable TTO or TTR CLINs for all active orders to which the CLINs apply as of the contract's termination date.
- 14) Effectively use subcontract and teaming arrangements efficiently and effectively, including use of designated set-asides including small businesses, small disadvantaged businesses, women-owned businesses, veteran-owned businesses, HUBZone businesses, and service-disabled veteran-owned businesses;
- 15) Provide training to the Government as a discreet service based upon requirements documented in individual task or delivery orders. The Contractor shall receive no less than a 60-day notice for coordination of specific training classes. The Contractor shall response to training requests separately under the SR that requests specific training. For example, the creation of training that revolves around a new system will be priced when responding to the SR that requests the development and delivery of the new system; and
- 16) Develop and provide business continuity plans to include recovery procedures for ITMS; these plans and procedures must align with the risk and impact to TSA's mission and the ITMS technology platform and infrastructure.

C.4.1.1 Partnership Philosophy

In addition to meeting program objectives, the Contractor is encouraged to:

- 1) Consistently take steps to understand TSA's crucial business issues, needs, and opportunities;
- 2) Share the risks and responsibilities of joint implementations and initiatives;
- 3) Ensure its products and services deliver tangible and meaningful business benefits;
- 4) Work collaboratively with other Contractors, Government agencies, and business partners to ensure project success;
- 5) Resolve the complexities and difficulties that are characteristic of implementing, integrating, maintaining, and securing mission-critical IT systems and solutions for TSA and Departmental users; and
- 6) Periodically measure and forecast capacity and systems growth in sync with TSA capital planning requirements and constraints.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 8
-----------------	------------------------------------	--	-------------

C.4.1.2 Desired Results

- 1) Ensure seamless continuity of services from current support to replacement services through DHS platforms;
- 2) Provide thorough and documented deliverables;
- 3) Provide customer-centric deployment of services (customer quality project value attained, configuration controlled, and performance increased while cost savings are realized);
- 4) Provide effective, timely, cost-efficient coordination, planning execution, and reporting of all activities and events on a daily basis;
- 5) Support TSA with efforts to integrate existing TSA planning and monitoring;
- 6) Support TSA effort to integrate activities with other agencies that support TSA mission requirements;
- 7) Support the development of a TSA enterprise architecture and implementation of an OMB compliance to include the Capital Planning and Investment Control (CPIC) process (Section J, Attachment 14; Technical Reference Model); and
- 8) Provide superior managed services that are supported by SLAs and other metrics.

C.4.1.3 Transition of Existing Services/Work in Progress

The Contractor shall plan and manage those activities necessary to transition service from the existing service provider(s). Immediately after the notice to commence work, the Contractor shall perform due diligence through inventory of all the ITMS assets, system configuration information, current NOC operations, documentation. The incoming Contractor shall transition services to the updated ITMS Bridge CLINs. The Contractor shall document and provide findings to the Government in a Bridge Transition Plan. A Final Bridge Transition Plan shall be submitted by the Contractor 30 days after the ITMS Bridge contract award. The Bridge Transition Plan shall address technical, administrative, and financial impacts to assure smooth and transparent continuity of operations. During transition, the Contractor shall be responsible for maintaining continuity of operations and quality of service and shall become familiar with Government processes and methodologies. Objectives for transition are as follows:

- 1) No break in current service levels
- 2) No delay in support for new and ongoing projects
- 3) Existing ITMS projects shall continue as-is unless changes are directed by the Government

The Government and Contractor agree to transition (cut over) ITMS Contract Service Requests (SRs) from the ITMS Contract to the ITMS Bridge Contract in the following manner:

- 1) The ITMS SRs will continue to operate under the ITMS Contract, which will have its period of performance extended by Government through the period necessary to cut over all SRs to the ITMS Bridge Contract;
- 2) A joint working group/IPT will be formed by the Government and the Contractor to review, prioritize and reconcile the current list of ITMS SRs for appropriate action;
- 3) The joint working group/IPT will establish a mutually agreed upon schedule for the cut over of the ITMS SRs to the ITMS Bridge Contract; and
- 4) The Contractor shall propose SR solutions in accordance with the terms and conditions of the ITMS Bridge Contract.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 9
-----------------	------------------------------------	--	-------------

C.4.1.3.1 Transition out of the contract

The Contractor shall be responsive and assist in the transition of ITMS services to follow-on Contractor(s), as appropriate. The Contractor shall coordinate and transfer all ITMS management and technical data to other service providers, as directed. The ITMS Contractor shall identify a transition team to assist the Government and the follow-on ITMS Contractor(s) during the transition period.

The Contractor shall cooperate and comply with the arrangements made for the replacement and follow on to ITMS Bridge. The Contractor shall also recognize that "partial off-ramps" of services (as directed by TSA) are included within the scope of "follow-on" contracts. The Contractor shall coordinate and transfer the management and technical data as required to the incoming Contractor and/or the Government. The performance objectives include, but are not limited to, open partnership and coordination with the Government and the incoming Contractor(s); provide for continuity of operations and services, as required; transfer of products and services to the Government and/or to the follow-on contract.

C.4.1.4 Staff

- 1) Provide a fully integrated team experienced in required disciplines, and skill sets, including contract management, project and program management, IT management, internal controls, program control, disaster recovery, contingency planning, business continuity, security management, and other disciplines needed to execute the objectives of the Program, sized to provide support in these required disciplines and fully integrated with the ITMS Program Management Office (PMO).
- 2) Provide a fully integrated team that is knowledgeable and experienced in supporting complex programs of the size, scope, and complexity of the ITMS.
- 3) Provide experienced professional staff to work closely with TSA personnel and other concerned parties to successfully achieve TSA and ITMS objectives.
- 4) Design IT infrastructure and services to enhance TSA's ability to share knowledge through such techniques as distance learning and learning management for TSA staff.
- 5) Transfer knowledge of provided technology from the Contractor to TSA IT managers, engineers and end-users to better enable Government staff to accomplish TSA's mission and objectives.
- 6) Program managers shall meet the qualifications at the appropriate level as specified in DHS management directive 1400.

C.4.2 Network Management

The Contractor shall provide procedures, systems and tools in order to support a comprehensive approach to network management. That comprehensive approach shall better enable Contractor technicians and Government representatives to quickly assess the overall health of the network and its supporting devices. That same approach shall be employed to assist in troubleshooting and isolating problems in the environment and to routinely check overall performance. The Contractor

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 10
-----------------	------------------------------------	--	--------------

shall apply this comprehensive approach to ensure the Government of the following network characteristics:

Availability - The Contractor shall maintain network availability as defined by relevant SLAs in Attachment 5, Section J.

Survivability - The Contractor shall provide prioritized service restoration in the case of outages to those customers designated by the Government as critical. The total number of critical customers is expected to be five (5) percent of the total number of system customers. The Contractor understands that both the identity and the location of critical customers will vary over the life of the contract. Additionally, the Contractor shall develop a contingency plan for the network infrastructure (refer to the ODC and Travel requirements attachment listed in Section J), as specified in Section C.4.3.13. This plan shall describe in detail the method by which service will be restored or maintained under a number of situations. The contingency plan shall specify emergency maintenance actions to include a network recovery plan, assign responsibilities, and methods to communicate status to managers. The contingency plan shall address catastrophic loss of single and/or multiple users, catastrophic loss of single or multiple locations, the hosting site, and disruption in service to critical users. The contingency plan shall address the restoration of services to systems based on a prioritized list based on system criticality; the list is to be developed in conjunction with the Government.

The Contractor is responsible for providing 7x24x365 remote network management of TSA Enterprise network LAN/WAN components, sites, and devices from a centralized Network Operations Facility (NOC). The NOC provides technical subject matter experts (SME) on local and wide area networking disciplines.

The Contractor shall provide remote management services on the following list of components: Routers – 263 Cisco Routers in production, 6 in the lab (Cisco 3660 Series); 110 – Cisco 2600 Series; 59 – Cisco 3600 Series; 67 – Cisco 3700 Series; 27 – Cisco 7200 Series; Switches – 613 Cisco Switches in production, 54 in the lab; 1 – Cisco 2900 Series; 418 – Cisco 3500 Series; 178 – Cisco Catalyst 4000; 16 – Cisco Catalyst 6500; UPS Devices – 444 in production, 16 in the lab; Rack Botz Devices – 724; F5 Load Balancers – 6; VPN Concentrators – 2 (Cisco 3030).

ACS Service Management for Application Availability:

- 1) AMSS shall provide reporting on application availability and performance of significant events within the application shall be performed within the standard out of the box capability of the Site Scope Tool.
- 2) TOP Application Monitoring. AMSS shall provide reporting on application availability and performance of significant events within the applications shall be performed within the standard out of the box capability of the Quest Tool.

Work Product Reports - The Contractor shall routinely communicate network performance to the appropriate Government representatives by submitting status and performance reports on a daily, weekly and monthly basis. The summary of work product reports is as follows:

Up/Down Status Report

The Contractor shall provide an Up/Down Status report showing the proper time stamp of interfaces on routers, switches, and servers is needed on a daily basis. The root cause of such problems shall also be provided on a daily basis. If any monitored device (device that shall be monitored by the

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 11
-----------------	------------------------------------	--	--------------

Contractor) is unavailable for three (3) polling cycles (approx. 5 minutes) then the device shall be marked as "down" by the Contractor. If service is degraded to any monitored device, the point that the device appears unavailable or unreachable by the Network Management System the device shall be marked as "down" and will count as an outage against the Service Level Agreement as appropriate. The Network Management System shall be able to provide a real time event log that lags behind the actual real time by one polling cycle (approx. 5 minutes).

The Contractor shall provide Executive Reports, upon request, depicting a detailed summary of events from the Up/Down Status report(s).

Bandwidth Utilization Report

The Contractor shall provide a Bandwidth Utilization Report. This is a report that shall be provided on a daily, weekly and monthly basis. This report shall detail:

- 1) Bandwidth utilization over three (3) specified time periods (24 hours, 1 week, 1 month)
- 2) Bandwidth utilization trending information (historical bandwidth usage) over the course of the last year, if available at no cost, and the last two (2) years. This report shall use daily, weekly, monthly information for trending purposes, and for trend analysis and planning
- 3) Bandwidth trend reports shall be for Contractor managed WAN circuits, and major LAN segments (e.g., Hosting Centers and TSA HQ) that pertain to core network services (access to servers, applications, SANs, backup devices, etc.)
- 4) Latency figures shall be provided from various points throughout the network. By way of example, Contractor managed airports shall have latency statistics from the airport to the hosting center. The top ten (10) locations, and other sites as requested by the Government, should have latency statistics provided across their WAN connections to sites where resources are accessed (such as servers, applications, storage devices, etc.)
- 5) High traffic sites ("top talkers") shall be listed in these reports.

Real Time State of the Network Event Log

The Contractor shall maintain and provide to the Government, upon occurrence, a Real Time State of the Network Event Log. Network Management Systems typically funnel information (traps) into a central mechanism that correlates events and gives an "at a glance" look at failures, and degradations in the network. This Event Log shall also provide detail on any outage.

Resource Utilization Reports

The Contractor shall provide TSA with an operational Resource Utilization Report. This report shall detail server status and provide information on Contractor managed file servers, application servers, storage devices, and terminal servers. The Contractor shall provide the following information in the resource utilization reports:

- 1) CPU utilization over the course of a day
- 2) Memory utilization over the course of a day.
- 3) Disk utilization over the course of a day.
- 4) Bandwidth utilization over the course of a day.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 12
-----------------	------------------------------------	--	--------------

The Contractor shall maintain these statistics and provide them to TSA on monthly intervals to show trends and to aid in planning for future growth. The Contractor shall maintain data to establish trends over a two (2) year span.

For mail servers – the Contractor shall list the top 100 users (from a message storage perspective). For file servers the top 100 storage users shall be listed.

Intrusion Detection Reports

The Contractor shall provide Intrusion Detection Reports on a daily, weekly, and monthly basis showing Network Intrusion Detected Events, and Host Intrusion Detection Events. The source of the attempted access shall be provided as well as the mechanism employed to attempt to bypass security.

Access to Network Management and Monitoring Tools

The Contractor shall provide Government staff with:

- 1) Access to the network management systems and tools used to compile information for the reports listed above
- 2) Access to data and software to generate ad hoc reports .
- 3) Access to view the real time status
- 4) Access to view the detail of events throughout the network.

Applications' Status and Performance Reports

As required for network status and performance, the Contractor shall provide TSA with a set of reports, Application' Status and Performance Reports, for applications' status to include up/down status of major applications, and performance trends of major applications as indicated in the succeeding two (2) sections.

Up/Down status of Major Applications on the Network

The current status of Contractor managed major applications, as defined in Section J, integral to the network is a critical data set that must be maintained and available to the Government. In this regard, TSA requires Up/Down status of major applications, as defined in Section J, such as:

- 1) E-Mail (Exchange)
- 2) Server-based applications
- 3) Database engines that applications run on
- 4) Backup Systems were successfully run

The Contractor shall provide an Up/Down Status report showing the proper time stamp of the interfaces on routers, switches, and servers on a daily basis. The root cause of such problems shall also be provided on a daily basis. If any monitored device (device that shall be monitored by the Contractor) is unavailable for three (3) polling cycles (approximately 15 minutes) then the device shall be marked as "down" by the Contractor.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 13
-----------------	------------------------------------	--	--------------

Performance Trends of Major Applications on the Network

An application shall be regarded as any software application that runs on an engine which can be interpreted as a database, a loadable module, a daemon or a service that a server loads in order for the software application to operate properly. Any scheduled jobs, cron jobs or periodically timed/batched tasks shall also be considered applications.

TSA requires that the Contractor report upon availability and successful operation of these applications, and that historical data on each application performance shall also be kept and supplied to TSA in the form of trending reports so that TSA can ascertain how each application performs over the course of time by the Contractor. The Contractor shall keep data for a two (2) year period and this data shall be reported upon within a two (2) year span.

The Contractor shall provide reports on a daily, weekly, and monthly basis showing application availability, performance of significant events within the application (Example: Takes 30 seconds to send and e-mail within TSA and show it as being read by recipient. Example: Takes 32 seconds to search for a specific record in xyz database – using the following search criteria, etc.)

Specific Definition of a “Critical” Event or Outage

The Contractor shall provide TSA with specific definitions of events designated as “Severity level 1” (S1) and “Severity level 2” (S2).

The Contractor shall correlate events designated as severity level 1 and severity level 2. If an event is marked at severity level 1 and listed as red or critical in the event correlation tool it shall be on the morning outage report, and shall be considered a critical outage.

C.4.2.1 Command Information Center

The Contractor shall provide continuous support for the Command Information Center (CIC). The CIC is established to monitor special events. When directed, the Contractor shall provide a 24x7 CIC for the ITMS program TSA information systems organizations. The Contractor shall designate an incident coordinator who will be the point of contact for ITMS officials. The Incident Coordinator shall keep the Government officials apprised of special interest events and issues as well as critical system outages, security events and emergency patch management. The Contractor shall provide the Government with an Event Command and Control work product report detailing operational status of the network as well any related issues on a daily basis specific to the Event Command and Control Center.

Reports will be in a TSA and Unisys agreed format, TSA and the Contractor shall mutually agree on a date of implementation. The Contractor shall be responsible for sending severity pages to staff deemed by TSA. The Government will provide a cell phone list to the Contractor after award of the contract. A current phone list will be provided to the contractor 1 week after contractor award. Updates will be provided monthly.

Operational activities of the CIC shall include:

- 1) Provide 24x7 command and control status information services for the ITMS Program including: TSA information systems organizations.
- 2) Provide 24x7 command and control of information system services for the ITMS program including: TSA information systems organizations

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 14
-----------------	------------------------------------	--	--------------

- 3) Brief to federal ITMS personnel special interest events and issues of applicable significance
- 4) Provide command and control of specific outages, identify and notify the incident coordinator, and provide support for incidents as required. Examples include:
 - a. Critical system outages,
 - b. Security events, and
 - c. Emergency patch management.
- 5) Notify specific federal ITMS personnel of specific type of information systems events identified by exculpation processes.

Provide Critical Network Infrastructure Services Monitoring

- 1) Provide critical network infrastructure and server services monitoring.
- 2) Escalate and Monitor Repair Services for Critical System Issues
- 3) Provide escalation services regarding critical systems issues to specific federal and Contractor personnel.
- 4) Track Contractor deployment and change projects.

C.4.2.2 Security Management

Site inspections may take place at any time during the term of this contract and may include the use of spot checks, scheduled inspections, random sampling, user reports, and periodic review of Contractor's quality and control programs. The Contractor shall immediately correct any specific measures where the Contractor is found to be noncompliant with TSA's MD 1400.3 IT Security Policies and Security Architecture.

The SOC Infrastructure shall support 524 sites, 39 Firewalls, 60 NIDS, 387 HIDS, 375 ESM, 18,000 Seats, 55,000 users, 2509 Network Managed Devices, 457 Servers and the specific monitoring of 641 devices. SOC Infrastructure Services shall include the correlation of security events for all monitored devices and provide reporting capability through a web portal accessible to authorized TSA users.

C.4.2.3 Interoperability

The Contractor shall ensure that the ITMS network interfaces fully within the TSA enterprise and shall continue to support communications between users within TSA and other federal agencies. The Contractor shall provide system interoperability as directed by the Government. The Contractor shall also adhere to and comply with the TSA Enterprise Architecture model, as revised (See Attachment 16, Section J).

C.4.2.4 Service Level Agreements (SLAs)

The Contractor shall comply with specified SLAs in this Performance Work Statement and recommend SLAs/KPIs and incident linkages with management processes that improve service and reduce the Total Cost of Ownership. The Contractor shall regard SLA standards to be consistent with

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 15
-----------------	------------------------------------	--	--------------

private sector standards, i.e., for corporations with 40,000+ employees distributed nationwide unless higher standards are mandated by the Government.

C.4.2.5 DHSNet

The Contractor shall be aware of and assist in accommodating the requirements of DHSNet as defined in C.4.9, when those requirements become available. The Contractor shall implement the DHS ADEX in the test environment.

C.4.3 Global Managed Services

C.4.3.1 Capacity Management

The Contractor shall provide capacity monitoring, analysis, planning and reporting to the Government for the Managed Network and Managed servers for the ITMS Program. The Contractor shall ensure the ITMS IT enterprise is optimized and access to shared infrastructure resources is aligned with mission priority, user satisfaction, and productivity in order to provide a sustained level of operational readiness while facilitating TSA in meeting its business objectives. The Contractor shall establish key performance indicators of importance to TSA that specifically relate to the TOP and supporting network infrastructure (refer to the ODC and Travel requirements attachment listed in Section J). The server metrics shall include: CPU percent utilization; memory utilization (absolute amount and percent of total); disk I/O levels; network bandwidth utilized; unplanned downtime; local and shared disk utilization; and time to complete system backup activities.

The Contractor shall develop recommended system capacity thresholds. The Contractor shall monitor performance metrics against these thresholds and recommend actions to expand capacity when thresholds are approached. The Contractor shall establish lead times with TSA that are sufficient to enable remediation before capacity limits are forecast to be reached. At 90-day intervals, the Contractor shall update growth forecasts for TOP platform resource utilization and work with TSA to estimate costs needed to efficiently expand platform resources consistent with these forecasts in a timeframe consistent with the TSA budget cycle. When appropriate the Contractor shall recommend repurposing resources to apply them where demand is greater, which will permit optimization of resource utilization. The Contractor shall track and make available weekly platform capacity measures. The Contractor shall update quarterly the TOP capacity plan and forecast document.

The Contractor and the Government agree to develop a plan of action and processes regarding actions to be taken upon automated notification that a TSA appropriate network usage policy has been violated.

AMSS shall undertake capacity and performance planning within the standard out of the box capability of the Quest tools for the TOP environment. AMSS shall undertake capacity and performance planning within the 'out of the box' capabilities of the SiteScope tool set.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 16
-----------------	------------------------------------	--	--------------

C.4.3.1.1

Purpose

- 1) The purpose of Capacity Management is to ensure that IT processing, storage, and network capacity matches the evolving demands of the business in the most cost-effective and timely manner.
- 2) TSA estimates growth in network traffic, email, application servers, disk storage, and processing requirements, etc., to be in excess of 20% per year. A large number of projects now in development, plus the use of Internet browsers and tools for multi-media access, could result in even more rapid growth. The network is at the threshold of a major growth period as it becomes the primary information highway for new business and engineering applications. Therefore, accurate predictions must be made to determine adequate levels of equipment, and forward looking plans must be developed to introduce new technologies in a timely manner so as to be able to meet the needs of TSA.
- 3) Capacity management is the process of planning, monitoring, analyzing, modeling, sizing, optimizing, and initiating change to capacity to satisfy demand in a timely manner and at a reasonable cost to achieve the IT goals of TSA.
- 4) Capacity management focuses on procedures and systems, including specification, implementation, monitoring, analysis, and tuning of IT resources and their resulting service performance.
- 5) Capacity management provides guidance on how to plan, justify, and manage appropriate levels of resources needed for a given solution.
- 6) Capacity management is key to establishing the optimal capacity for a new service or component or to changing an existing service or component.
- 7) Correct management of capacity sizing results in:
 - a. Appropriate use of resources.
 - b. Sufficient capacity available in time to meet production workload needs.
 - c. Reduction of the frequency and duration of IT capacity failures.
 - d. Improved alignment between business needs and IT resources by deriving IT service and capacity requirements from specified business requirements.
- 8) Improper planning for capacity can lead to wasted resources resulting in unnecessary cost, or lack of resources resulting in poor performance or the unavailability of an IT service.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 17
-----------------	------------------------------------	--	--------------

C.4.3.1.2 Capacity Management Requirements

The Contractor shall comply with the following capacity management requirements:

- 1) Manage the Network to provide an infrastructure that ensures the optimal use of the resources needed to achieve the agreed upon levels of performance and be proactive and responsive to business needs.
- 2) Support TSA's long-range IT strategic planning with new technology analysis, consideration of TSA business needs as they relate to computer resources and the projection of future TSA growth against computer resource capacities.
- 3) Provide oversight and management to ensure optimal insight into the TSA operational environment. This includes:
 - a. Providing scalability, synchronization and anticipation of TSA's capacity needs
 - b. Assuring all groups are monitoring the correct entities
 - c. Perform trend analysis to determine adequate levels of equipment
 - d. Providing on-site monitoring capability including for the TSA management
 - e. Optimizing alert thresholds
 - f. Alert management
 - g. Collecting Performance data for SLA management
 - h. Performing event correlation both after an event and as a proactive management tool.
- 4) Establish a single point of responsibility for capacity planning in a Capacity Manager role.
- 5) Ensure agreement, measurement, and monitoring of capacity requirements in order to fully support service level management.
- 6) Recognize and correct shortfalls in the provision of the required levels of capacity and performance.
- 7) Provide problem and root cause analysis data through capacity management tools and techniques.
- 8) Monitor technology changes and make recommendations to TSA of new technologies to implement; and
- 9) "Optimal" in this context refers to resource usage at the best place, time, quantity, and price.
- 10) "Capacity" in this context, may imply resource capacity, such as storage, processor speed, network, or human resources, or an end-to-end IT service capacity, such as messaging, customer relationship management (CRM), or order processing.
- 11) Provide and implement the equipment and licenses required for server monitoring solutions.

C.4.3.2 Configuration Management

The Contractor shall conduct Configuration Management and develop a Configuration Management Plan in accordance with guidelines set forth in the TSA SDLC (Appendix C-7 Configuration Management Plan). The Contractor shall implement configuration management and provide access to ITMS practices, and provide access to Configuration Management data.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 18
-----------------	------------------------------------	--	--------------

The Contractor shall provide TSA with configuration management services that apply to IT systems, subsystems, and components used in support of the applications identified in Section J of the contract, unless specifically designated by the Government as optional or discretionary. The Contractor shall use only authorized components or configuration items in the production environment and will track and record changes throughout the component's life cycle.

The Contractor shall identify, control, and track versions of hardware, software, documentation, processes, procedures, and other components of the IT organization. The Contractor shall ensure that only authorized components, or configuration items, are used in the IT environment, and that changes to configuration items are recorded and tracked throughout the component's life cycle.

The Contractor shall provide configuration control support of those items to include, but not limited to, analyzing, tracking and reporting through an automated configuration tracking system. The Contractor shall provide support services for the identification and documentation of the characteristics of a configuration item, to control changes to a configuration item, and to record and report change processing and implementation status.

The Contractor shall afford the Government and its designees access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases. Site inspections may take place at any time during the term of this contract and may include the use of spot checks, scheduled inspections, random sampling, user reports, and periodic review of Contractor's quality and control programs.

The Contractor shall be responsible for configuration management standards, procedures, policies, administration of the configuration management tool; installation and maintenance of the configuration management software on the assigned servers and on users' workstations; user support and training. In addition, the configuration management service shall provide: reproducibility of delivered products; identification of assets released; and ability to identify and control baselines.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 19
-----------------	------------------------------------	--	--------------

C.4.3.3 Image Management

The Government will define the requirements for the software to be resident on the various devices to be deployed (Mobile seat, desktop, Personal Digital Assistant (PDA)) as well as for the following types of servers (file and print, email, Web, domain controller,). Image Management shall include the following:

- 1) Examining each commercial-off-the-shelf (COTS) product in the solution to determine the appropriate release level and configuration requirements for the image. COTS software refers only to the standard software installed as part of the TSA base image.
- 2) Developing and maintaining stable images for the configuration and integration process—Image Management and Certification
- 3) Performing interoperability testing of the workstation, server, and PDA images to identify settings, configuration, and compatibility issues to ensure images work with the TSA website.
- 4) Provide a development and test lab environment with established policies and procedures that support all project personnel including third-party vendors throughout the systems development life cycle. This will result in a higher quality product and reduce overall cost of development.
- 5) Maintaining the image under configuration control.
- 6) Insuring changes to the image will require approval of the appropriate Governance Board "build instructions" for developing the master image for each device to be deployed.
- 7) Maintaining copies of all standard configuration images.
- 8) Validating the image with a Quality and Test group, and further audited by TSA to be consistent with Federal and TSA requirements.
- 9) Developing automated load instructions for the mass loading of devices.
- 10) Validating and auditing these processes and place under the same SCCB process as the build instructions.
- 11) Examining new releases of the COTS products for consideration into future releases.
- 12) Testing recommended changes for interoperability with the rest of the ITMS solution, and reviewing with the SCCB prior to approval. This is a dynamic process that includes keeping the approved image up to date. The Contractor shall submit a quarterly new image release schedule.
- 13) Image Management shall include Security Management.

C.4.3.4 Change Management

The Contractor shall provide Change Management services to assess the impact of changes on existing capacity and identify additional resource requirements based on the change in demand. The Change Management services shall provide a disciplined process that can introduce required changes into the environment with minimal disruption to ongoing operations.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 20
-----------------	------------------------------------	--	--------------

The specific functions associated with Change Management are as follows:

- 1) Actively participate in the CM process by submitting their one-project Request For Change (RFC),
- 2) Providing peer review comments and reviewing all RFCs to minimize network outages and impact on users;
- 3) Review all RFCs weekly in two combined CM/RC meetings and verify that they meet RFC submission prerequisites before submission to TSA SCCB;
- 4) Forward RFC approval status spreadsheets and meeting and operations schedules to network infrastructure engineering managers, technical leads, and engineers to provide on-time approval and implementation;
- 5) Conduct a post-implementation process that reviews whether the change has achieved the goals that were established for it and determines whether to keep the change or back it out;
- 6) Provide coordination between development and operations;
- 7) Participate in weekly CM boards and meetings as presenters or members;
- 8) Coordinate the meetings and arrange for ITMS Infrastructure Engineering participants to support and attend;
- 9) Provide all CM process updates to Infrastructure Engineering group;
- 10) Participate as a voting member on CM boards;
- 11) Coordinate the RFC presentation or present the RFC in Technical Discussion Forum (TDF) or approval meetings.

The Contractor shall provide a change management process that shall include the following:

- 1) To formally initiate a change through the submission of a request for change (RFC).
- 2) To assign a priority and a category to the change after assessing its urgency and its impact on the infrastructure or end users.
- 3) This assignment affects the speed at which the change will be addressed and the route it takes for authorization.
- 4) To establish an efficient process for passing the RFC to a change manager and the change control board (SCCB) for approval or rejection of the change.
- 5) To plan the deployment of the change, a process that can vary immensely in scope and includes reviews at key interim milestones.
- 6) To work with the Release Management service that manages the release and deployment of changes into the production environment.
- 7) To conduct a post-implementation process that reviews whether the change has achieved the goals that were established for it and determines whether to keep the change or back it out.
- 8) To coordinate between development and operations.
- 9) To include the tracking of RFCs throughout a component's or system's life cycle and include notifications to appropriate individuals at specified life cycle stages.
- 10) To maintain control over break fix maintenance to maintain service availability and shall conduct break fix maintenance on an as needed basis.
- 11) To document break fix maintenance in an RFC and report that information to TSA.
- 12) In the context of change management, change is defined as anything—hardware, software, system components, services, documents, or processes—that is deliberately introduced into

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 21
-----------------	------------------------------------	--	--------------

the IT environment and may affect an IT service level agreement (SLA) or otherwise affect the functioning of the environment or one of its components.

- a. Changes can be either permanent or temporary.
- b. Changes can completely replace a current version of a component, either with a new component or a changed version of the component, or they can involve the installation of a completely different component or the removal of an outdated one.

AMSS shall perform this function for the TOP and ACS environments under the guidance of the TSA Release Manager, and shall be therefore subject to limitations based upon TSA RM's process and availability.

C.4.3.5 Configuration Reporting

The Contractor shall provide Configuration Reports as work products with supporting diagrams defining physical architecture characteristics. The Contractor shall update the diagrams as new capabilities or changes are introduced and allow Government staff access to TSA Engineering Architecture diagrams. The Contractor shall allow the reports to be extracted by the Government from the configuration tracking system and allow data to be viewed in logical structure and format.

The Contractor shall provide configuration reports as work products with supporting diagrams defining physical architecture characteristics and will update the diagrams as new capabilities or changes are introduced. The Contractor shall also provide a method to allow Government staff to access TSA Engineering Architecture diagrams. The Contractor shall provide the means for the reports to be extracted from the configuration tracking system and allow data to be viewed in logical structure and format. The Contractor shall make project configuration reports available via a central repository to TSA project personnel.

C.4.3.6 Review/Control Boards

The Contractor shall participate and follow the policies and procedures of the System Change Control Board to provide governance for a wide range of change management.

C.4.3.7 Software Management

C.4.3.7.1 Capability Maturity Model Integration (CMMI)

The Contractor shall develop software and systems engineering using the guiding principles of the Carnegie Mellon Software Engineering Institute, Capability Maturity Model Integration (CMMI). Upon request by the Government through the ordering process (see Section G.10), the Contractor shall provide a plan to achieve CMMI-SE/SW version 1.1 conformance for both TSA and TSA Contractor compliance. In the event the Contractor is requested through an individual task or delivery order to develop software and/or systems, it must demonstrate that processes being used are consistent with industry best practices and are repeatable.

The Contractor shall demonstrate process improvement efforts on developing and managing Contractor organizational standard processes for software and systems engineering based on the TSA Systems Development Lifecycle (SDLC) v.2.0.3, while keeping in mind the guiding principles of CMMI-SE/SW and other methodologies.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 22
-----------------	------------------------------------	--	--------------

C.4.3.7.2 Software Maintenance

The Contractor shall provide, within 90 days of release of any major system software upgrade, an Impact Statement of the release on the enterprise. AMSS shall test and implement maintenance releases and bundled patch sets. This implementation does not include major vendor version changes such as new software releases nor maintaining the approved image consistent with software currency for the TOPS and ACS environments, i.e. Oracle 9.x to Oracle 10.x etc. As part of this process, the Contractor shall implement version control and release management procedures integrated with the overall configuration management approach. AMSS shall implement patches based upon the Patch Impact Statement and appropriate risk/reward. Not all patches are applicable or appropriate based upon the TOP and ACS environments. Before implementation of a patch, the Contractor shall assess the impact of any hardware and software upgrades to system infrastructure, performance, security, and version compatibility, and shall test all new software releases approved by TSA. The Contractor shall be responsible for impact assessment of hardware and software upgrades to system infrastructure, performance, security, and version compatibility, as well as the requirement for TSA certification and approval before implementation. Software releases shall be subject to the SDLC guidance. New software versions must be certified and approved by TSA before implementation. Projects and project tasks will be separated from core and managed service tasks so that work directly related to the development and deployment of projects will be included in the scope of the work for the projects. This allows TSA to provide the project sponsor with the funding needs for the project. The Contractor shall also assess PMO projects to provide seamless integration with the current production infrastructure. The Contractor shall coordinate with TSA lines of business to see that the business requirements are met. The Contractor shall provide Earned Value metrics for non fixed price projects that meet the following criteria: Acquisition Category (ACAT) 4a or above, defined as equal to or greater than \$500,000 of acquisition cost, or projects with a period of performance equal to or greater than six months. The Contractor shall develop, implement, and maintain QA processes, activities, and procedures on PMO projects.

The following shall apply to the TOP environment. The Contractor shall perform up to 14 application standard builds per month. The Contractor shall perform a standard build Monday through Friday from 23:59 to 06:00 EST on scheduled work days. TSA will provide the Contractor with 48 hours notification prior to the build being performed unless build is an emergency patch or emergency build due to a production down situation. The Contractor shall perform up to 11 data loads per month Monday through Friday between the hours of 18:00 to 22:00 EST on scheduled work days. The Contractor shall perform up to 49 builds or build reviews per month in the Reston Integration and Test environment. The Contractor shall perform this activity between 08:00 until 18:00 Monday through Friday on scheduled work days. The Contractors AMSS DBA staff shall be on-site in Reston, VA from 07:00 through 19:00 EST Monday through Friday during scheduled work days. The ACS Engineering team shall perform up to two (2) application standard builds per month. A standard build shall be performed Monday through Friday from 23:59 to 06:00 EST on scheduled work days. Forty-eight (48) hours notification shall be required prior to the build being performed unless the build is an emergency patch or emergency build due to a production down situation.

C.4.3.7.3 Release Management

The Contractor shall develop a Release Management Plan in coordination with TSA that details how software patches, updates or upgrades are introduced in the production environment. The release

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 23
-----------------	---	---	---------------------

management plan shall include: release planning; release building; performance testing and evaluation; acceptance testing; release preparation; release deployment, backout and rollback; patch management; upgrades and other O&M activity or application interruptions e.g., UNIX or Oracle upgrades / recompiles and Storage Area Network reconfigurations. In support of TSA, the Contractor shall provide subject matter experts in support of AMSS in meeting the requirement to develop a release management plan. AMSS shall participate in Test Readiness Reviews (TRR) and Production Readiness Reviews (PRR) as conducted by TSA and acceptance of application builds and deliverables will be based upon TSA's SDLC.

The Contractor shall provide a release management process and system that provides control and tracking. The Release Management process shall address, at a minimum:

- 1) Release Planning
- 2) Release Building
- 3) Performance Testing/Evaluation
- 4) Acceptance Testing
- 5) Release Preparation
- 6) Release Deployment and Backout/Rollback
- 7) Patch Management
- 8) Upgrades

The Contractor shall work with the Government to coordinate future releases upon Government approval. Prior to release of the software, the Contractor shall conduct the appropriate testing and site preparation in accordance with the SDLC Guidance Section J.

C.4.3.7.4 Trouble Management

The Contractor shall provide trouble management to include:

- 1) Identifying, isolating, tracking, resolving, and documenting Contractor managed network hardware or enterprise applications software problems, failures, or faults which may impede the end-user's ability to communicate effectively with other users, servers or devices on the network.
- 2) Fault monitoring, fault isolation, fault resolution, ticket management, configuration management, and performance and capacity management for LAN infrastructure devices and server hardware
- 3) Performance monitoring, fault isolation, fault resolution, configuration management, and capacity planning for LAN server operating system software and e-mail applications.
- 4) Providing routine reports on system fault status and availability of network systems, services and components.
- 5) Providing an Incident Report, as a work product, for enterprise outages over one hour and a detailed remediation plan for significant outages when requested by the Government.
- 6) Developing and implementing an effective and efficient troubleshooting and problem resolution methodology.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 24
-----------------	------------------------------------	--	--------------

C.4.3.7.5 Monitoring and Data Collection

The Contractor shall monitor IT performance to include:

- 1) Error thresholds as a part of the fault management activity
- 2) Network performance and availability
- 3) End-user network response times and adjusting the network configuration and/or routing methods [as an option]
- 4) User and application causing peak load conditions, bandwidth use, etc. identification
- 5) Network statistical information gathering and analyzing
- 6) Overall network performance
- 7) Fault management provided using the latest techniques, tools, and current best practices

AMSS shall monitor and report on applications causing peak load conditions, however no user data will be collected as it is not available. User data, if available, shall be stored within the application however the TOPS and ACS applications do not store this information.

C.4.3.7.6 Software Support

The Contractor shall support software throughout the life of the contract. Upon installation, the Contractor shall provide training for contractor developed applications and help desk support to end users. The Contractor shall manage compliance of software licenses and register supported software with the vendors in order to receive notices and maintenance updates. The Contractor shall act as the agent to manage vendor licenses. For Contractor developed application features and functional capabilities, the Contractor shall develop user manuals, training materials and help desk documentation prior to production release of the application to assist system users, based on service order requests.

ACS team shall support bi-monthly staging, production deployment, and level III infrastructure support only: all development and end-user support services shall be provided by SM&A and the application developer for the PMIS application.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 25
-----------------	------------------------------------	--	--------------

C.4.3.7.7

E-Gov Service Level Agreement

The Contractor shall propose one or more SLAs to include at a minimum the following critical applications:

- 1) PIMS
- 2) TIBCO
- 3) ACS / Approved Foreign Flight Crew
- 4) Cockpit Crew Vetting
- 5) Contact List
- 6) TSA CM (supports the three TSA web sites)
- 7) Dialogic Alert Notification System
- 8) Documentum Rel 5 (eContent server, different from CM)
- 9) Enterprise Document Management Documentum Rel 5(EDM)
- 10) IACMS
- 11) IS (Integration Services, deployed on the two TIBCO servers)
- 12) PARIS
- 13) Registered Traveller
- 14) Tech Ideas (View Only)
- 15) No-Fly List
- 16) WebBoards (41 active boards for AvOps, MLS, HR, etc.)
- 17) Witness

For each of the critical applications, the Contractor shall define the Key Performance Indicators (KPIs) that will provide the basis to develop metrics for monitoring activities, communicating status, and taking corrective action. The Contractor shall make the metrics available to all stakeholders in a timely manner. The Contractor has a ninety (90) day stabilization period for all new performance measures to establish appropriate baseline thresholds.

AMSS shall work with TSA to define Kepi's for the following applications;

- 1) ACS / Approved Foreign Flight Crew;
- 2) Contact List;
- 3) TSA CM;
- 4) IACMS;
- 5) Paris;
- 6) Tech Ideas, view only;
- 7) No Fly List; and
- 8) WebBoards (41 active boards).

The KPIs shall be developed based upon out of the box functionality of the SiteScope Monitoring tool for the ACS environment and the Quest Monitoring Tool for the TOP environment.

C.4.3.8

Equipment Maintenance

The Contractor shall provide maintenance for contract managed components of the TSA infrastructure on Contractor maintained equipment. The Contractor shall perform both remedial and preventative maintenance. The Contractor shall provide maintenance services using on-site tier II and on call technicians to meet SLA requirements (see Section J). The Contractor shall provide maintenance that is consistent with the Original Equipment Manufacturer's (OEM) warranty (e.g., clean filters/fans

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 26
-----------------	------------------------------------	--	--------------

regularly, and coordinate with the OEM as necessary to address necessary repairs) and coordinate with the OEM as necessary for warranty covered repairs.

The Contractor shall not include OEM recommended consumable items and replacement of OEM recommended consumable items, to include ribbons, toner, printer maintenance kits, thumb drives, UPS batteries, laptop batteries in the per-seat CLIN prices.

The Contractor shall provide equipment maintenance services as defined in the following sections. Equipment maintenance services applies to the following areas: Managing equipment maintenance from a central location; maintaining ITMS infrastructure equipment; maintaining ITMS end user equipment; dispatching on-site Tier II and on-call technicians; providing a global reporting system; maintaining and updating maintenance records; maintaining service and repair logs on enterprise systems; developing a spare parts plan; providing critical incident support; providing non-warranty preventative and remedial maintenance activities; providing warranty support; and where applicable providing an equipment refresh. The Contractor shall provide general category Non-Warranty CLINs to allow the Government to order remedial maintenance on the desktop and infrastructure IT equipment. The Contractor shall provide preventive maintenance on the infrastructure IT equipment using Tier II support.

The Contractor shall propose a solution for global maintenance reporting to include providing the names for network equipment, i.e. servers, switches, routers and printers. The goal of this reporting is to provide the Government insight into equipment performance to enable better system performance and planning. The Contractor shall make maintenance records available to the Government upon request and provide the Equipment Maintenance Report on a monthly basis.

The Contractor shall maintain a repair log for contract managed equipment and shall ensure that such repair log information is maintained as part of the Asset Management system. The content of the Repair Log shall be defined based on the Contractor's global systems' capabilities after contract award.

Restoration SLAs shall not be applicable to the TSA OCONUS locations. The Contractor shall provide maintenance service on equipment outside of the contracted period of performance on a time and materials (T&M) basis.

C.4.3.8.1 Preventive Maintenance

The Contractor shall provide Preventive Maintenance on infrastructure equipment as follows:

- 1) Performing preventive maintenance including engineering changes, maintenance updates or releases, modifications, patches and upgrades.
- 2) Providing regular scheduled maintenance to meet system availability and performance requirements.
- 3) Installation service release hardware for installed systems.
- 4) Maintain service/repair logs for each supported hardware system and its components.

The Contractor shall perform preventive maintenance (hardware and software) in accordance with the OEM recommendations for network equipment.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 27
-----------------	------------------------------------	--	--------------

C.4.3.8.2 Remedial Maintenance

The Contractor shall perform remedial maintenance service on TSA's ITMS Contractor maintained malfunctioning equipment, hardware, and software, to return it to full operational status. The service shall be performed in collaboration with the help desk policies and procedures and is subject to the Government's review.

The Contractor shall comply with the following Remedial Maintenance requirements:

- 1) Use Help Desk policies and procedures, subject to initial Government review, to resolve customer problems or questions, whenever possible.
- 2) Schedule and coordinate a visit to the end-user location.
- 3) Provide accessible knowledge base, troubleshooting, and diagnostic support in response to a SPOC task or delivery order to resolve problems and questions that cannot be resolved over the telephone or remotely.
- 4) Provide On-site or desk side remedial maintenance to support the repair or replacement of ITMS Contractor maintained malfunctioning hardware or software, during and after the equipment OEM's warranty period based on TSA ordering the appropriate CLINs. Remedial maintenance service includes transportation, labor, and parts to return the malfunctioning component to operating condition.
- 5) Arrange for maintenance agreements and support from hardware and software providers to maintain service levels and performance expectations based on TSA ordering the appropriate CLINs. Non-Warranty desk side Maintenance Support Services shall meet the restore-time SLA. This shall apply to desk side service support, i.e., work stations, laptops, and printers.
- 6) Record observations and conclusions in the ticketing system. Non-warranty server Maintenance Support Services shall meet the SLA restore-time. This shall cover central shared components including servers (Unix, Wintel), workstations, storage devices, backup units.
- 7) Update applicable configuration and inventory systems.

C.4.3.8.3 Critical Incident Support

The Contractor may provide Critical Incident Support, also referred to as Quick Response, Quick Turnaround, Heightened Response, as requested through an individual delivery or task order. For such critical incident support, a fixed team of Contractor personnel dedicated to TSA, and located on-site may report to the Contractor and be deployed at the guidance of TSA management in support of TSA operations.

C.4.3.9 Spare Parts

The Contractor shall store, inventory and maintain spare parts and components to support the repair of ITMS managed hardware and software after the OEM warranty period. The Contractor shall propose a Spare Parts Support Plan with recommendations for maintaining levels of spares equipment inventories. The costs associated with the execution of the Plan, and spare parts, excluding the cost for the loaner program, for non-warranty equipment are covered under the applicable managed services CLIN. A Spare Parts Support Plan shall be submitted by the Contractor for Government review and approval within 60 days of contract award, and shall include the

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 28
-----------------	------------------------------------	--	--------------

Contractor's plan and cost to maintain a pool of equivalent "loaners" to provide for the end user when user equipment must be shipped back to the OEM for warranty repairs.

The Contractor shall provide and maintain spare parts at necessary levels to meet contracted service performance levels. During implementation, the Contractor shall have material planners review the equipment to be serviced at TSA sites. The Contractor shall match the equipment history to the specific service levels, and material planners shall build a list of the parts for TSA locations; the Contractor shall manage the entire process of providing the parts from inventory to the TSA location including packing, shipping, and tracking via a spare parts inventory information system. The system shall monitor parts usage and automatically replenish parts based on the reorder point in accordance with the reporting requirements.

C.4.3.10 Warranty

The Contractor shall maintain the equipment in accordance with manufacturer's warranty restrictions and software licensing agreements. The Contractor shall track warranty repairs in the repair log. TSA shall provide the Contractor with OEM Letters of Agency so that the Contractor can register the products on behalf of TSA with OEMs, as necessary, in order to receive maintenance updates.

The Contractor shall perform warranty services in accordance with the OEM's terms and conditions for entitlement. The Contractor shall certify their technicians' skill to repair the Dell and Cisco equipment. The Contractor shall scan the PCs and servers that are connected to the contractor managed TSA network and account for the TSA software, if the Software Distribution system is accepted and ordered by TSA. The Contractor shall provide TSA with notification so that the appropriate service orders can be replaced for software license renewal. The Contractor shall deploy their service technicians nationwide and on-site Tier II to provide three (standard, premium and premier) grades of field services as appropriate on network equipment, PCs and printers. The Contractor shall leverage their relationship with other maintenance suppliers to provide support on copiers, fax machines, TVs, secure safes, secure shredders, and personal wireless devices (PDA and PED). The Contractor shall register Cisco products with the manufacturer to receive SMARTNET proprietary support that includes obtaining patches and spare parts that will allow the Contractor to meet the accepted SLAs. The Contractor shall register Dell products with the manufacturer to receive support that includes obtaining patches and spare parts that will allow the Contractor to meet accepted SLAs.

The warranty period commences on the date of delivery of the product from the manufacturer and ends based on term length purchased. The Contractor shall track the warranty period in the asset management system.

When individual equipment items are no longer covered under the original contracted warranty, the Government will select from the following:

1. Order a non-warranty managed services CLIN.
2. Execute a technical refresh by ordering an appropriate seat CLIN from Section B.2 of the Contract B-Tables.
3. Execute a technical refresh by acquiring equipment that meets the government property standardization requirements stated herein and order the appropriate government property inspection CLIN.
4. Elect not to enroll the equipment under non-warranty maintenance.

The warranty periods will vary and are based upon the OEM's warranty policies.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 29
-----------------	------------------------------------	--	--------------

C.4.3.11 Equipment Refresh

The Contractor shall refresh equipment, as authorized by TSA service order, for software and hardware to ensure that seat services are in compliance with SLAs. The Contractor shall provide planning for equipment refreshment in order to not disrupt the daily operations of the end user. Equipment refresh is at TSA's discretion based on specific service order.

The Contractor shall be constantly evaluating the supportability of the TSA-installed equipment. As equipment becomes obsolete and the Contractor determines the OEM's intention to drop support on equipment and spare parts will no longer be available, the Contractor shall notify TSA and make recommendations for replacement products. The Contractor shall provide TSA with dates when the Contractor would be unable to perform remedial maintenance and meet the SLA. These dates shall be commensurate with the Contractor's inability to provide non-warranty maintenance for the specified equipment.

TSA will then have the option to place service orders to either replace all of the affected equipment as a project prior to them malfunctioning or replace them when they malfunction. Out of warranty equipment and unapproved third party procured equipment shall not be included in the calculation towards Break Fix SLAs or Equipment Delivery.

C.4.3.12 Asset Management

Asset management is the systematic planning and control of a physical resource throughout its life. Managing agency assets and associated services will involve a variety of business processes that support mission readiness and accountability, including work management, inventory management, service management, security, business effectiveness, contract management, and procurement. IT asset are a common denominator. The Contractor shall track assets under managed services and leased equipment, recording moves, adds and changes.

The Contractor shall provide TSA a comprehensive Asset Management lifecycle solution that compliments their proposed business solution. TSA will work with the Contractor to devise a solution that ensures asset data is shared mutually.

The Contractor shall propose a comprehensive asset management lifecycle solution. The proposed lifecycle solution shall: create asset-level visibility and help TSA understand where assets are located, who has access to the asset, and the value of the asset; facilitate control of the infrastructure from both an asset utilization and budget perspective, minimizing both over-and under-provisioning; ensure software license compliance resulting in reduced risk and optimized software spending; support formalized change management and streamlined procurement efforts; and drive better IT investment return decisions through ongoing monitoring and reporting.

The Contractor shall manage assets associated with this acquisition where managed services have been ordered. The Contractor is required to be knowledgeable of Government regulations and user needs, and to establish, implement, and maintain an asset management solution that lays the groundwork for process enablement, compliance, and governance.

The Contractor shall provide a comprehensive asset management system to track all inventory covered by this contract. This system shall enable the Government to extract information needed to effectively manage all assets. The asset management system shall be integrated with the

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 30
-----------------	------------------------------------	--	--------------

provisioning and ordering, invoicing, and help desk ticketing systems and other Government systems dependent upon the input of asset management data, as ordered. The system shall track all managed equipment by location, user, type, network connection information, and equipment ID. Updates to the IT Asset Management system shall be made as the Government's needs change, and be available electronically as part of the applicable management report to the Government.

The Contractor shall conduct an initial assessment of TSA's IT current assets. The Contractor shall provide an Asset Report to the Government on a monthly basis that includes all ITMS-leased seat assets and ITMS Government property.

The Contractor shall be responsible for, as a minimum, the following services:

- 1) Ensure that all moves, additions, and deletions of equipment are current on a daily basis
- 2) Provide role-based by site, password protected, read access to property custodians and other TSA personnel
- 3) Create and maintain a table for active and inactive users with roles and locations of personnel from data provided by TSA
- 4) Deploy TSA inventory database and Engineering Architecture repository; the Contractor shall be responsible for providing the following monthly data feed information:
 - a. Managed Services provider asset tag
 - b. TSA asset tag
 - c. Manufacturer's service tag number
 - d. Serial number
 - e. Category
 - f. Class
 - g. Manufacturer
 - h. Make
 - i. Model
 - j. Description
 - k. Cost
 - l. Vendor
 - m. ESN (cellular)
 - n. Status
 - o. AA
 - p. Office
 - q. Branch
 - r. Division
 - s. Airport site
 - t. Code
 - u. Building
 - v. Floor
 - w. Room
 - x. User_first_name, User_last_name
 - y. CLIN
 - z. Purchase Order or Service Order number
 - aa. DD-250 date or in-service date
 - bb. Warranty end date (Warranty End Date shall be 36 Months from the DD250 Signing Date.)
 - cc. Government owned/leased
 - dd. Disposal method
 - ee. Disposal date
 - ff. IP and MAC address

Contract	Document No.	Document Title	Page #
	HSTS03-06-D-CIO500	ITMS Bridge Contract	31

- 5) Verify and provide accountability of all managed equipment to TSA through physical audit
- 6) Report: By site, real-time, standard, and ad hoc
 - a. Standard field reporting shall be able to sort by user, CLIN, type, site category, and class accessing only their area's data
 - b. Standard HQ reporting shall be able to sort by user, CLIN, type, site, category, and class
 - c. Administration reporting shall include above standard capabilities for reporting as well as ad hoc reporting
 - d. Reporting shall include TTO/TTR
- 7) Ensure all managed equipment has been labeled/tagged with appropriate identification asset tags/stickers
- 8) Maintain the hardware inventory database
- 9) Provide monthly data feed to TSA inventory database
- 10) Accept data feeds from HR including duty station addresses for all employees and/or Contractors assigned TSA assets
- 11) Assist in establishing and maintaining a software inventory database
- 12) Lead the annual and semi-annual physical inventory sweeps
- 13) Document policy and procedures for maintaining asset tracking accountability
- 14) Maintain a searchable listing which includes leased/Government Property procurement request/service order for individual equipment items
- 15) Assist in annual inventories and assist in establishing and maintaining a software inventory database (include data elements for software database: type of software, name of software, license number, user name (first and last), license expiration date, classification (enterprise or individual)), and documentation of policy and procedures for maintaining accountability
- 16) Serve as the central point of contact for information relative to the IT inventory database
- 17) Be responsible for tracking, monitoring, and reporting on a baseline quantity of 65,000 assets.

Scope and Limitation of Authority. The TSA Acquisition Office will provide the successful Offeror a letter of appointment designating a person(s) the Authorized Order Agent (AOA) designation. The AOA Letter of Authority will specifically set forth dollar limitations (not to exceed \$150,000.00 for single purchases) and the general category of items authorized for purchase. Items not falling within the scope and limitations stated in the letter of appointment are not authorized and shall not be purchased by the Ordering Agent. The aggregate amount of a purchase transaction shall not exceed the monetary limitations specified in the letter of appointment. Purchases may not be split to avoid this monetary limitation. Items must be immediately available and one delivery and one payment made. Purchase requirements exceeding the Ordering Officer's authority must be submitted to the TSA Contracting Officer for purchase approval

Delegation of Authority. The AOA is the only person(s) authorized to purchase items set forth in their letter of appointment. They are solely responsible for obtaining prices and placing orders. This authority CANNOT be re-delegated.

C.4.3.13 Contingency Planning

Contingency Planning is the process for making sure that the Government can recover from processing disruptions in the event of localized emergencies or large-scale disasters, and is essential to the continuing accomplishment of the Government's mission.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 32
-----------------	------------------------------------	--	--------------

The Contractor shall conduct contingency planning for the ITMS program. Contingency Planning is essential to ensure that the Government is able to recover from processing disruptions in the event of localized emergencies or large scale disasters. The Contractor shall develop a Contingency Plan consistent with OMB, DHS and TSA guidelines for the Continuity of Operations Plan and the Disaster Recovery Plan. Once approved by the Government, the Contractor shall implement the Contingency Plan and conduct annual drills of the plan, as directed by the Government.

The Contractor shall develop the TSA ITMS Contingency Plan and update it periodically as required. The Contractor shall develop a comprehensive disaster and disruption contingency plan for ITMS-managed resources employed by TSA. To do this, the Contractor shall work closely with TSA OCIO representatives to understand DHS and TSA policies for service reconstitution and to define the range of primary disruptive scenarios to include in the plan. The scope of ITMS resources includes but is not limited to TSA core network, Exchange email system, file and print services, Active Directory and user management, IP telephony, messaging and conferencing services, user support (SPOC functions), TSOC functions, Legacy applications (TSA HQ), and TOP applications (Hosting Center). The Contractor shall base the contingency plan on TSA-provided prioritization for restoration of the ITMS systems and services in the event of disruption. The plan shall identify the relevant systems and network components that constitute each service and document the range of disruptive scenarios that are applicable to each service, ranging from local outages to large scale emergencies.

The Contingency Plan shall include a comprehensive Network Recovery Plan that clearly articulates the Contractor plan to recover the network in the event of failure. This plan shall include, at a minimum:

- 1) Telecommunications network;
- 2) Front and back office systems;
- 3) Remote offices;
- 4) Network Operations Center (NOC); and
- 5) Call center operations.

The Contingency Plan shall be based on TSA-provided prioritization for restoration of the ITMS systems and services in the event of disruption. The Plan shall identify the relevant systems and network components that constitute each service and document the range of disruptive scenarios that are applicable to each service, ranging from local outages to large scale emergencies. For each group of related ITMS services and systems, the Contractor shall develop in the Plan restorative responses to each disruptive scenario. The restorative response shall include but is not limited to: identifying required alternative equipment needed to restore service, and determining to what degree it is available to TSA; assigning responsible persons or organizational components and reporting channels; determine procedures to transfer operational data and/or services; determining changes to network operations needed to support service transfer; determining procedures needed in advance of disruptions to enable rapid recovery of capability; and developing appropriate tests to verify readiness to react to disruption and to exercise the recovery measures.

The Contingency Plan shall identify scenarios for which full or partial recovery can be accommodated using current resources, as well as cases where gaps exist that require additional systems or network equipment in order to recover. Following acceptance of the contingency plan by TSA, the Contractor shall prepare cost and technical proposals to include WBS, implementation plan, test, and acceptance plan for implementation of the disaster recovery plan at one or more to-be-determined Alternate Operations Facilities (AOF). The contingency plan shall prepare TSA to exercise recovery measures as needed to respond to disruptions. The plan shall also identify needed improvements in system

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 33
-----------------	------------------------------------	--	--------------

capability that will enable better agency preparedness and help estimate resources needed to fill the gaps that are identified.

C.4.3.14 Online Catalog of Services

The Contractor shall provide a plan for an E-Procurement provisioning solution within 45 days of contract award to TSA that supports a single procurement lifecycle (product acquisition through transition/disposal) of the TSA equipment and peripheral product environment, including service and support. The system shall be comprised of a supplier-hosted catalog, order acceptance and audit capabilities, fulfillment tracking, and delivery completion notification of the ordered product or service to TSA.

The provisioning system shall include a variety of flexible solutions that seamlessly integrates into customer environments and allow order generation from all TSA sites with permission given to designated officials the visibility and control over the order approval process. The system shall also implement security that limits and restricts viewing of orders by departments. The system shall streamline the process of purchasing assets through workflow and routing process and established business rules to allow Managers located in various TSA facilities the ability to approve and submit an order request to an authorized TSA business unit that has contract authority to enter the Government into a purchaser's agreement with a single-source vendor. The streamlined solution should allow each order requests to be submitted by site specific personnel, received, reviewed, approved, tracked and monitored by the user or site manger.

The catalog shall include pictures or graphical representations, descriptions, and prices of all ITMS approved products and services, as applicable. The Contractor shall be responsible for keeping the catalog up to date with CLIN information and new CLINs and updates should be performed within one (1) business day following acceptance of a new CLIN or contract modification. The Contractor shall submit written technical and cost proposals in accordance with Section G.11. The Government will be responsible for periodic validation of the E-Procurement provisioning system and catalog information therein, and may rely on third-party independent verification and validation of the process and system in place by the Contractor.

The E- Procurement system shall seamlessly integrate with the Contractor's Asset Management system and shall provide support TSA basic asset information such as: make, model, serial number, date of purchase or date of lease, and warranty information, etc.

In addition, the system shall:

- 1) Provide expenditure data to analyze purchasing trends and spares requirements
- 2) Capture the complete audit trail of transaction activity
- 3) Include processes to ensure purchases comply with internal Government policies and contract terms
- 4) Provide Email notification of order status change, requisition approval or denials.
- 5) Track serial information of deployed units to the original order
- 6) Perform Ad-hoc reporting capabilities

The Contractor shall provide complete whitepaper documentation of the system and any changes made to the system. A training manual shall be developed that provides step-by-step instruction to utilize all system capabilities. The training manual should be updated periodically to reflect system changes. This documentation and training manual shall be provided to the Government upon deployment of the E-Procurement system.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 34
-----------------	------------------------------------	--	--------------

C.4.3.14.1 Electronic Order Forms and Electronic Reports

The Contractor shall provide a Web-based online ordering feature that allows a TSA authorized requestor to view and select items, services and reports. The requestor shall also be allowed to review, modify, or add to an order and be able to provide delivery requirements and obtain pricing while placing an electronic order. Requestors shall receive immediate electronic confirmation of orders.

C.4.3.15 Deployment of Products and/or Services

The Contractor is responsible for the deployment of the requested product or service ordered through this contract. The Contractor shall configure and integrate the asset with TSA's images and shall ship the asset to the end user location, install and connect the asset to the network, and test the asset per the approved test and acceptance plan in Section E.4.

C.4.3.15.1 Grades of Service

The Contractor shall provide global managed services consistent with the assigned Grade of Service.

Premier Service

The Contractor shall provide Premier Service to designated TSA HQ, TSOC and other on-site Tier II locations listed in section C.5.4, and TSA executives in the designated on-site Tier II locations who are identified on the VIP list. Premier Service requests shall be given the Contractor's senior leadership attention. Service representatives or technicians shall respond within 30 minutes from when the call is logged where there is on-site Tier II service available and during standard site support hours.

Service and trouble tickets shall be resolved within 24 business hours for equipment that is under contracted ITMS maintenance services, from when the call is logged.

Premium Service

The Contractor shall provide Premium Service to TSA designated VIP users. Service technicians shall respond within 4 hours from when the call is logged, receipt of a trouble call. Service or trouble tickets shall be resolved or escalated within 24 business hours from when the call is logged. A call is considered resolved when confirmed by appropriate TSA personnel.

Standard Service

The Contractor shall provide standard service to those seats not designated as premier or premium seats. Service or technicians shall respond to trouble calls within 24 business hours from the call being logged (receipt of a troubled call). Service or trouble tickets shall be resolved or escalated within 24 business hours from when the call is logged. A call is considered resolved when authorized by appropriate TSA personnel.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 35
-----------------	------------------------------------	--	--------------

C.4.3.16 Help Desk Services

The Contractor shall provide and support end-user Help Desk services. The Help Desk shall be manned with live telephone coverage 365 days per year including all Federal holidays. The Help Desk shall be available to all TSA authorized users through the phone at all times. The Contractor shall provide a toll free number for all TSA users throughout the United States. On call support is for Application Outages or System not available outages only.

Aviation Operations WebBoards end-users shall be supported by designated WebBoards managers within the Aviation Operations organization. ACS Team shall provide level III application and infrastructure support.

Remediation for errors found within the 60 days following a new application deployment or application upgrade shall be performed by the Contractor or application developer.

The objective of this section is to provide all TSA with Tier 0/I, Tier II, and Tier III service. TSA recognizes that engaging an external service provider is a mature business practice used by many companies ensuring responsive and competitive operations. The TSA wishes to implement an IT infrastructure that is consistent with industry best practices and expects the Contractor to provide a comprehensive, best value solution.

The central service desk shall be the single point of contact for the end user for related problem reporting and service requests including but not limited to desktop and laptop hardware, LAN/WAN connectivity for the personal computer (PC)/ laptop, PDAs, IMAC activity, shrink-wrap off-the shelf and business applications. Any TSA confidential information that has been input into a service center database, knowledge databases and end-user databases that are used in connection with any services provided to TSA shall be protected in accordance with the policies of TSA.

The TSA requires a single point of contact (SPOC) to act as the primary interface to the thousands of end users that use various COTS and custom developed applications from recording of the incident through its ultimate closure. The Contractor shall make available an End User IT portal for use by the general user population. This portal shall allow real-time access to submit a service request electronically, or to view the current status of an open service desk request. The Contractor shall track and reports performance on a monthly basis against the agreed upon service levels. Such reports will show service desk performance, and highlight exceptions listing those tasks and metrics that do not meet the established service levels. The exception report will indicate Contractor corrective action plan for any services not meeting the established service levels. This service can take the form of, but is not limited to, answering questions concerning problem resolution for TSA standard COTS and some specialized applications for its end users. Additionally, the Contractor shall coordinate the transfer of information from Tier 0/I to Tier II and Tier III services, some of which shall be provided by the Contractor, the TSA and various 3rd party vendors and Original Equipment Manufactures (OEMs). Supporting TSA user requires the ability, on the part of the Contractor, to take customer calls, log the call into the helpdesk database, analyze the call, resolve the problem or assign the problem to another helpdesk technician and log the resolution in the helpdesk's knowledge base. The TSA expects timely, courteous and competent responses to its end users' problems by the Contractor.

ACS shall provide support for Fingerprints and CITS investigation processing and shall coordinate with OPM on resolution of investigation download issues. ACS shall also provide Break-Fix support for issues related to Daily Processing of Fingerprints and CITS records.

Contract	Document No. HSTS03-06-D-C10500	Document Title ITMS Bridge Contract	Page # 36
-----------------	------------------------------------	--	--------------

Users requesting service or support will telephone a central service center by dialing a Contractor provided toll free number. When answering a call, the Contractor's analyst shall use the standard greeting script developed in conjunction with TSA. The Contractor shall respond with similar service requirements to web initiated tickets. Tickets submitted via the web will be queued in the order of arrival and the end user shall receive a call back from a Contractor agent in order of receipt to discuss the problem in the event that the incident requires additional detail. The Contractor's analyst shall define, prioritize, refer, track, and escalate end users' problems and requests to meet agreed upon service levels. The Contractor shall randomly conduct end-user telephone surveys to measure end-user satisfaction on closed tickets. The standard Contractor format shall be at minimum a seven-question survey and shall be used to contact (1 phone call placed and a message left) up to 10% of the end-user population. These questions are answered on a 1 – 5 scale by the end users. There is an additional question to solicit feedback and comments from the end user. The Contractor and TSA shall mutually agree to incorporate up to three additional questions if required. The results of such survey will be reported monthly, commencing in the second month after the six-month Transition Period.

The Contractor shall provide basic helpdesk operations that include Tier 0/I call center support, Tier II support including remote desktop management for some COTS/GOTS applications and operate and maintain the interface with other Tier II and Tier III support organizations. Issues outside the Service Desk capability to resolve are either dispatched to desk-side support technicians or escalated to Level 2 or 3 support providers as defined in the agreed upon call scripts. The Contractor shall deliver Level 2 or 3 support through other Contractor support components such as LAN NOC, WAN NOC, Data Center and SOC, TSA internal and third party support providers. Voice and data network, wireless, LAN administration, WAN, mainframe and proprietary application issues will be referred to Level 2-3 support providers. The central service desk is 24x7 including Government holidays. Central service desk Level 1 Agents shall possess at minimum technical experience with PC COTS software and hardware as well as effective end user service demeanor. Agents are the first point of contact and primary telephone support for end users calling the service desk. The Contractor's AMSS Application Help Desk Engineers staff shall be available for remote help desk services on Monday through Friday from 08:30 until 17:00 EST during scheduled work days.

The Contractor's end user desk support service (outside of TSA HQ and TSOC sites) shall be sized to address the following:

- 1) Actual dispatched DSS calls (2,924) for the dispatched environment.
- 2) The device quantity (15,845) for the dispatch environment (again excludes dedicated support at TSA HQ and TSOC).

The Contractor shall:

- 1) Provide enhanced technologies that speed resolution times or proactively eliminate end-user problems, thus improving the TSA employee's productivity.
- 2) Provide 24x7 support for an outage to a TOP application in the production environment.
- 3) Provide AMSS helpdesk support by Application Help Desk Engineers on Monday through Friday from 07:00 until 22:00 EST during scheduled work days and shall provide TOP help desk support for upwards of 700 tickets per month.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 37
-----------------	------------------------------------	--	--------------

- 4) The Contractor's solution shall provide the following features:
 - a. A single point of contact for problem and service requests
 - b. Ownership of problems from identification to solution/resolution
 - c. Seamless call distribution and call management support

The Contractor's service desk support shall be sized to address the following:

- 1) Primary Hours of Coverage: 24x7
- 2) Abandon Rate: 6.0%
- 3) Speed to Answer (Sec): 45
- 4) First Call Fix Rate (Fixable Calls): 85.0%
- 5) First Call Fix Rate (All Calls): 21.3%
- 6) Cycle Time: 0.8 (excluding TSA positive call closure time)
- 7) Number of Client Referral Points: 25 (COTS/GOTS resolvers are not included)
- 8) Includes: End to End Problem Mgmt, Smarthands
- 9) Average of 1.05 Incidents per Seat per Month
- 10) Average of 18.4 Minutes Handle Time per Call (Average of In-Bound and Out-Bound calls)
- 11) Limited to 50,000 Screeners
- 12) 20,000 calls / month

In addition, upon SR issuance, the Contractor shall provide incremental SPOC services for ITMS applications. The Help Desk interface shall be responsible for operations, problem resolution and facilitation of the Contractor's activities to ensure that the end users are operational as quickly as possible.

The services provided by the Contractor shall be as follows:

- 1) Helpdesk support for Tier 0/I
- 2) Tier II support for COTS/GOTS/ACS applications
- 3) Interfacing with Tier II and Tier III support organizations.
- 4) Remote Desktop Management
- 5) Reporting trouble call metrics

The Contractors AMSS ACS Application Help Desk Engineers staff shall:

- 1) Be available for remote help desk services on Monday through Friday from 08:30 until 17:00 EST during scheduled work days;
- 2) Provide AMSS TOP helpdesk support by the Application Help Desk Engineers on Monday through Friday from 07:00 until 22:00 EST during scheduled work days.

The Contractors service desk support shall be sized to address the following:

- 1) TOP help desk support of up to 700 tickets per month;
- 2) ACS help desk support of up to 375 tickets per month.

The helpdesk interface shall be responsible for operations, problem resolution and facilitation of the Contractor's activities to ensure that the end users are operational as quickly as possible.

As necessary, the Contractor shall apply automated tools and methodologies in support of these efforts. The Contractor is expected to use the established Network Management System (NMS) enterprise framework for providing diagnostic, inventory and status information.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 38
-----------------	------------------------------------	--	--------------

The definitized requirements for the COOP/DR/Contingency Plans will be mutually agreed, based on final definitions and provision by the government of the requirements. The COOP/DR/Contingency Plans will be developed and provided after the establishment of the requirements, as follows:

ITMS COOPS Plan 120 days
TSOC COOP Plan 120 days
ITMS DR Plan 90 days
TSOC DR Plan 90 days

The COOP/DR/Contingency requirements provided in this contract are based on a initial assessment and will be finalized as the COOP/DR/Contingency requirements are provided by the government.

TIER 0/I Roles and Responsibilities:

- 1) The Contractor shall be responsible for providing Tier 0/I helpdesk support to all the users within the TSA.
- 2) Helpdesk services may be provided at the Contractor's facilities, at the Government's discretions and will include a SPOC for desktop support and coordination of computer service needs for all TSA users.
- 3) A single toll-free phone number, supported with Automatic Call Distributor (ACD) capabilities, will be provided for all IT problems.
- 4) Provide SPOC to end user.
- 5) Staff and maintain helpdesk.
- 6) Setup and maintenance a ticket management system; this will include logging of all trouble tickets into a Contractor provisioned, configured, and managed automated trouble-ticket management system that is electronically accessible to TSA staff via the internal LAN or the Internet.
- 7) Thoroughly document all trouble ticket problems and the steps taken to resolve these problems.
- 8) Log all trouble ticket resolutions into the help desk's knowledge database.
- 9) Monitor and document all trouble ticket hand-offs and resolutions.
- 10) Receive and answer calls.
- 11) Allow trouble ticket generation via 1) phone, 2) e-mail and 3) world wide web (WWW).
- 12) Interface with the asset management database.
- 13) Determine inquiry/problem resolution requirements.
- 14) Resolve inquiry/problem within 15 minutes, if possible, otherwise escalate to appropriate Tier II resource.
- 15) Interface and monitor the enterprise management system.
- 16) Track calls at Tier II and Tier III until resolution, in case of a delay inform the appropriate TSA personnel.
- 17) Technology Refresh of all software used to run and manage the helpdesk.
- 18) Answering the TSA end users' calls from a Contractor provisioned, configured and managed ACD system. The logging of all trouble tickets into a Contractor provisioned, configured and managed automated trouble-ticket management system that is electronically accessible to TSA staff via the internal LAN or the Internet.
- 19) Resolve issues over the phone or through the use of remote control software.
- 20) Perform hardware diagnostic procedures on PCs and printers, place hardware trouble calls to the appropriate support organization and coordinate the replacement of any defective parts.
- 21) Perform basic Network and Systems monitoring using Network Systems Monitoring software.
- 22) Perform any required daily routines such as database backups, database initialization, etc. on Contractor or TSA provided systems.
- 23) Dispatch and arrange for on-site support as required for problem diagnosis and/or resolution.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 39
-----------------	------------------------------------	--	--------------

- 24) Coordinate with OEM regarding utilization of warranty services, as needed.
- 25) Provision of monthly management and usage reports.
- 26) Perform root cause analysis on systemic issues, recommending solutions or elevating unresolved issues to the appropriate support personnel.
- 27) Track each call received, even if the call was elevated or routed to another support organization (i.e., Tier II or III), to ensure the customer's needs were met.
- 28) Monitor and documenting all trouble ticket hand off and resolutions.
- 29) Maintain superior service during fluctuations in the call volumes.

TIER II Responsibilities:

The Government requires on-site Tier II support that is comprised of cleared Secret technical specialists who shall resolve complex technical problems to include the reconfiguration of laptops, desktops, and troubleshooting various software and hardware related issues. In addition to other support duties, there shall be a sufficient staff of individuals assigned to the TSA HQ Support Team, TSOC, and TSA specified field locations with the function of performing Installs, Moves, Add, and Changes (See Paragraph on IMACs). This team shall work on-site at Headquarters' during normal business hours 7a-7p. Field locations hours of operations will be designated by site. Contractor support shall be provided after hours on a short-term basis if required to address emergency situations within the constraints of available resources/funding, tasking, and skill requirements. The team duties shall include the following:

- 1) All knowledge of the Tier I technicians.
- 2) Use of the Knowledgebase.
- 3) Microsoft Desktop and application configuration
- 4) Network accessory maintenance (printers, file storage, CD burners, etc)
- 5) Minor cable repair as required
- 6) Analog technology support (fax, modems, etc)
- 7) Network user support
- 8) Performing Installs, Moves, Adds and Changes
- 9) Blackberry Support
- 10) Asset Tracking
- 11) VOIP Support
- 12) Identify problem characteristics and, if possible, root cause
- 13) Resolve inquiry/problem within prescribed time limits, if possible, otherwise escalate to appropriate resource
- 14) Notify the appropriate TSA managers/designees, as required
- 15) Notify Tier 0/I personnel about call status/resolution
- 16) Assist Tier 0/I personnel in logging the resolution in knowledge database
- 17) COTS/GOTS Applications support
- 18) Trained on journeyman TOP/ACS application functionality

Outline the current hardware configuration of the desktops and laptops being used at TSA. The TSA has standardized its desktop and laptops making it a nearly homogeneous desktop environment. The Contractor shall provide support for these COTS applications in addition to all in-house developed HRM applications, including but not limited to e.g., IPPS, CUPS, USCG-FPD, etc. The Contractor's service desk support shall be sized to address the following: Top help desk support of up to 800 tickets per month. ACS help desk support of up to 375 tickets per month. The Contractor shall provide information on the automated trouble ticket management.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 40
-----------------	------------------------------------	--	--------------

C.4.3.16.1 Administration and Support

The Contractor shall provide staff to answer questions pertaining to services, products, delivery times, prices and other contract specifics via Web, telephone, facsimile, and email. The Help Desk shall have access to, and be able to understand and interpret diagnostic information for problem solving. The Help Desk shall have familiarity with the current hardware and software in order to provide usage and feature information, as well as troubleshooting capabilities. The Help Desk shall be responsible for handling and clearing Trouble Tickets and IMACs.

C.4.3.16.2 Self-Help System

In addition to its primary role as the SPOC for resolving IT problems, the end user will contribute to the knowledge management activities of the TSA by logging helpdesk problem solutions in a resolution knowledge database. This knowledge database shall be readily available for queries by end users for self-help. The self-help concept is an important part of the TSA overall end-user support strategy. A key performance metric for this contract is tracking the usage of this self-help database and its effectiveness in answering end-user queries. Within 45 days of acceptance the Contractor shall propose a system that shall be accessible to TSA employees and shall assist them in searching for answers to common problems and previously resolved technical issues.

The Contractor shall provide the detailed functionality of their proposed self-help system. Additionally, the self-help system must provide the following functionality at a minimum:

- Integration with the Contractor's trouble ticket tracking system
- Ability to measure the usage of the system

All data collected by the helpdesk personnel is the intellectual property of the TSA. Upon request by the Government, the Contractor must provide the data from the system in an easy to read and portable format, including an electronic version.

The Contractor shall propose the technical and cost requirements to develop this system.

C.4.3.16.3 Communication Initiatives

The Contractor shall perform many customer support functions. In this capacity, the Contractor shall act as the customer advocate and information focal point for the end user community.

To effectively perform this role, the Contractor shall establish a proactive and interactive communications process that educates the end user community as to the availability of services and the access to these resources. The Contractor shall work with the TSA to publish documents, send e-mails, hold conference calls, etc. to reach out across the agency and educate TSA employees. These communication pieces will include, but not be limited to, the contact number, email and Web addresses to initiate trouble tickets, hours of operation and the scope and level of services being offered by the end user.

AMSS shall assist with the management of 3rd Party Vendor provided software for infrastructure or COTS software packages. This support shall include problem escalation and tracking of package 'bugs' through the AMSS assigned tickets. TSA will be responsible for resolution of software defects or performance issues for TSA contracted Application Providers for custom applications or modified COTS/GOTS applications.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 41
-----------------	------------------------------------	--	--------------

Through the period of performance the Contractor shall continue to raise the awareness of the services offered to the end user. This process will also provide a means for the Contractor to obtain information from users regarding their IT needs.

As part of the response to this Performance Work Statement, the Contractor shall describe the process they plan to put in place for effectively communicating with the end-user community.

System owners who are primarily responsible for providing software or hardware to TSA shall provide Tier III support except for those applications listed in the software application addendum of ACS and TOPS applications or as otherwise agreed upon by TSA. TSA will make available to the helpdesk the appropriate contact information and the level of support that has been purchased from these vendors. The Contractor shall be responsible for escalating and tracking the status of these calls until they are resolved. The warranty information of the hardware shall also be provided to the helpdesk personnel to arrange the necessary warranty support from the hardware vendors.

The Contractor shall have end-to-end ownership of the trouble ticket. Even if the service or problem is referred to a Tier II or Tier III support group or TSA in-house application development and support areas for resolution, the Contractor, as the owner of the issue, shall be responsible for ensuring that the problem is resolved. Any process or management issues regarding the hand-off or delays resulting due to Tier II or Tier III responsiveness will be brought to the attention of TSA management during the weekly Status Reports.

As part of the response, the Contractor shall provide, within 45 days a detailed plan, to include processes regarding the processes it plans to implement for effective Tier II and Tier III interface management including its interfaces with the warranty service vendors.

Remediation for errors found within the 60 days following a new application deployment or application upgrade shall be performed by the vendor or application developer.

C.4.3.16.4 Remote Desktop Management and Systems Monitoring

Remote Control and Network Systems Monitoring software shall be provided by the Contractor; the Contractor must also provide system integration, adequate connectivity and bandwidth. It is the expectation of TSA that the Remote Control and Network Systems Monitoring software will be used to diagnose and remedy helpdesk support issues where appropriate.

C.4.3.16.5 Remote Seat Management Policy for Contractor

Remote management of desktop seats and servers shall be performed by the Contractor in accordance with TSA security policy. Remote access will require coordination with TSA Security Manager to ensure the firewall or other IT Security devices/tools rule sets are configured to allow such access. Additionally, the Contractor shall use TSA provided security products if they are appropriate for the type of session security required. If the TSA provided products are not applicable for the type of security needed, the Contractor shall use only TSA approved products or technologies incorporating strong authentication and encryption. No remote seat management shall be performed without the use of TSA provided or TSA approved session security products.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 42
-----------------	------------------------------------	--	--------------

C.4.3.17 Installation, Moves, Adds, Changes (IMAC)

The Contractor shall manage service for priority diagnostics, dispatching technicians, escalations, and interfacing with other service providers for IMAC requests and resolutions to TSA locations. IMACs shall allow reconfiguration of hardware and software to meet daily business needs and requirements. There shall be (three) types of IMACs, software IMACs, physical IMACs, (and special project IMACS). Software IMACs shall be administered remotely, where possible, by qualified personnel without dispatching a technician. Physical IMACs shall involve dispatching a technician to TSA locations. Special project IMACS involve moves of more than 25 users, and moves that involve special scheduling, shipping, or other additional logistics. The Contractor shall provide technicians who meet skill sets and security requirements.

The Contractor shall provide Order Processing / IMAC Sustainment personnel to perform the management and coordination of IMAC activities. Supervision of the on-site installation teams will be performed by the contractor's Regional Management staff.

The Contractor shall centralize and perform the IMAC management and reporting functions. The Contractor shall propose fixed-price CLINs that sustain a drawdown structure based upon a predetermined quantity of received requests per year. In addition, the Contractor shall provide a CLIN that contains 100 simple IMACs that TSA can order to add to the annual draw down fund. The simple IMACs in the draw down fund can be ordered by Government as needed for TSA CONUS locations by TSA calling the central service desk. TSA and the Contractor shall establish a monthly payment plan based on the number of IMACs that the Contractor completes out of the CLIN that contains 100 simple IMACs in the annual draw down fund. After award the Contractor shall collaborate with TSA to modify the established IMAC processes to facilitate the TSA approval and the Contractor execution processes.

IMACS range from simple (moving a work station from one location to another to complex (moving a group of people from one location to another)). CLINs will include individual, 10, and 25 IMAC bundles. More than 25 should be treated and priced as a special project, as will moves that involve special scheduling, shipping, or other additional logistics. Large desktop and networking rollouts shall be treated and priced as a special project. For IMACs that are considered a special project, the Contractor shall provide a plan that determines the priority and scheduling of the installation.

The Contractor shall provide efficiencies in travel time for combination IMACS (for example, simultaneous performance of a physical and software IMAC).

It is the Government's intention that IMACs will be performed by the Tier II onsite staff wherever applicable. Therefore an IMAC will not be charged. The Contractor shall manage service for priority diagnostics, dispatching technicians, escalations, and interfacing with other services providers for IMAC requests and resolutions.

The Contractor shall decrement an annual draw down fund by the numbers and types of IMACs that are performed and notify TSA when the annual draw down fund is depleted to a level of 80%. At that time TSA may add IMAC CLINs in quantities to re-refresh the annual draw down fund based on projections for the remainder of the year. Wherever applicable, the Contractor shall utilize the dedicated Tier II onsite staff to perform IMACs.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 43
-----------------	------------------------------------	--	--------------

C.4.3.17.1 Definition

Installation – Setup and configuration of TSA managed equipment.

Move – Deployment of TSA equipment to a different physical location

Add – The modification to TSA equipment that involves the addition of hardware or software components.

Change – The modification of hardware or software configuration of TSA equipment without changing the component.

The Contractor shall propose a planned schedule and costs for special project IMACs within 48 business hours of receipt of project-related IMAC requests. The plan shall designate the priority and scheduling of the installation. Special projects are: more than 25 individual IMACs in a single location that must be completed at the same time; moves that involve special scheduling, shipping, or other additional logistics and; large desktop and networking moves. TSA will provide the Contractor with sufficient requirement details to include the detailed list of equipment involved in the IMACs, the location where the equipment resides, the location where the equipment is being moved, the site preparation (power, cabling, HVAC, circuits, and telephone) tasks that are assigned to the Contractor, scheduled completion dates for the IMACs, Contractor interdependencies on other TSA entities, and the TM and COTR contact information to allow proposal responses within 48 business hours. In cases where the Contractor and suppliers requires site visits and surveys along with a Rough Order of Magnitude (ROM) and a schedule for submitting the final proposal.

The Contractor shall dispatch service technicians support personnel to perform simple IMACs. The Contractor shall also dispatch service technicians to perform special projects and simple IMACs in locations where there is no Tier II support coverage for the site requesting service.

C.4.3.17.2 Service Description

The Contractor shall perform physical IMACs (C.4.3.17.4) by dispatching technicians to TSA locations to move TSA equipment. The Contractor shall provide technicians who meet skill sets and security requirements. The Contractor shall verify that the requests for a move have been approved by a TSA order. The Contractor shall provide a center service desk to receive IMAC requests. Work orders, to include the annual draw down fund and special project IMACs shall be issued through the TSA procurement system to ensure proper authorization. Once approved, the individual IMACs shall be ordered by TSA by placing a ticket in the Help Desk. The Contractor shall provide dedicated on-site Tier II and service technicians to complete the effort.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 44
-----------------	------------------------------------	--	--------------

C.4.3.17.3 Software IMACs

- TSA will order the Software Distribution and engineering support CLINS to allow the Contractor to remotely administer software IMACs by qualified personnel without dispatching a technician.
- The Contractor shall perform software IMACS using the dedicated on-site Tier II support and from the drawdown funds until the Software Distribution system is operational.
- Software shall be installed using the default options of standard out-of-the-box installation instructions for applications, except where the Contractor and TSA mutually agree to a custom install.
- TSA will provide software Client Access Licenses (CAL) and other software licenses.
- The Contractor shall ensure requests meet the approved TSA software list. Non approved requests will be directed back to the appropriate TSA officials for requirements collection.
- TSA will order the Software Distribution and engineering support CLINS to allow the Contractor to maintain a software library to ensure sufficient license exists to support the software request prior to installation. The Contractor shall update the software library accordingly. (See Asset Management).
- The Contractor shall administer support remotely, where possible, by qualified personnel without dispatching a technician. Remote distribution and software library requirements shall be completed via the Software Distribution system.
- The Contractor shall verify that the requests meet the approved TSA software list.
- The Contractor shall forward requests for software IMACs that are not on the approved TSA hardware list to the appropriate TSA officials for requirements collection.

C.4.3.17.4 Physical IMACs

- The Contractor shall utilize dedicated on-site qualified IT personnel to perform individual IMAC requests.
- TSA will provide network infrastructure connections prior to the Contractor performing physical IMACs.
- The Contractor shall propose a solution to receive IMAC requests, obtain approval from authorized TSA personnel, and execute.

C.4.3.17.5 Data Migration

The Contractor shall support data migration service requests on TSA desktop clients up to 1 gigabyte of data. TSA desktop client data migration requests will fit within the preview of the Tier II structure where applicable and/or the Project IMAC drawdown structure when necessary. TSA will provide an operational device (CD R/W drive, tape storage, etc) and media for the contractor to perform data migration.

C.4.3.17.5.1 Email Migration

The Contractor shall support email migration service requests on TSA desktop clients up to 75 megabytes of data. TSA desktop client data migration requests will fit within the preview of the Tier II structure where applicable and/or the Project IMAC drawdown structure when necessary.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 45
-----------------	------------------------------------	--	--------------

C.4.3.17.6 System Re-imaging

The Contractor shall perform re-imaging service on deployed and re-deployed TSA seat clients. Re-imaging service must fit within purview of the Tier II structure where applicable and/or the Project IMAC drawdown structure when necessary. Re-imaging does not include: data (local and on the network) and email migration, user profile migration, reloading application, re-applying rights to distribution lists or other accesses. It is limited to installing an approved TSA image.

C.4.3.17.7 Asset Management Data Updates

Upon completion of the IMAC service the Contractor shall update the Asset Management database by updating the data in the asset tracking tool directly or electronically. Asset updates shall include the user (first and last name, email address, contact information); physical location change (site, room, and cubicle); entitlements; and configuration updates. The Government will provide appropriate HR feeds to identify new and departed staff including Contractors.

Tiered Support Reporting Requirements

The Weekly Activity Report shall consist of an itemization of each ticket worked that includes, at a minimum,

- Date and time
- Individual user
- Source of activity (SPOC/Local phone call/observation)
- System malfunctioning
- Short descriptor of activity
- Work/fix performed
- Impact to the mission

The Monthly Status Report shall include:

- Description of work accomplished during the period (the report will cover the previous month)
- Status of activities in progress
- Planned activities for the upcoming period and associated schedule information, including dependencies with other activities/projects
- Trouble ticket status for tickets that were opened during a specific reporting period, including aging report for open tickets that exceed defined closure thresholds. VIP tickets will be identified separately in the same report. In addition, Headquarters ticket reports will not include non-headquarters related tickets.

Government Property

TSA will provide administrative supplies and onsite office facilities for Contractor support personnel, to include, but not limited to, a workspace, workstation, desk and phone. Dedicated TSA laptop(s) and telephone(s) will be provided for the HQ and Airport Contractor support personnel.

C.4.3.18 Software Support

The Contractor shall provide support, management, control, and maintain all supported software running on ITMS assets (See Attachment 15, Section J). Sabre deployment and production support shall be limited to the 33 domestic sites currently in production. OLC supports TSA personnel training

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 46
-----------------	------------------------------------	--	--------------

at domestic airport only. The Fingerprints/Lems system is currently not supported by AMSS and is considered to be outside the scope of this ITMS Bridge contract. This shall be part of the transition project. The Contractor shall configure, install, test, and integrate various new software and hardware required for test-beds, proof of concept, infrastructure design, or pilot systems under evaluation. The Contractor shall install workstation software, and creating customized standard loads for distribution to multiple workstations. The Contractor shall coordinate software issues and licenses with DHS enterprise agreements, image requirements, and non-ITMS operational assets to assure continued availability.

The Contractor shall install patches and updates to the software. The Contractor shall ensure compliance with all supported software licenses and warranty restrictions. The Contractor shall identify to the Government any breach in software license and warranty. The Contractor shall maintain warranty and repair records and advise the Government of warranty expiration.

The Contractor shall provide software diagnostics as appropriate to maintain software in accordance with the SDLC and other ITMS policies and procedures, and service level agreements. The Contractor shall be responsible for distribution of software applications and patches remotely, where applicable, up to five days per week, 16 hours per day from 0800 to 2400 Monday through Friday. At a minimum, Contractor responsibilities shall include software license management, IMAC asset management and reporting, and end user support during the remote distributions.

The Contractor shall develop the TSA Operating Platform Reference Architecture document. The Contractor shall update and reissue the Reference Architecture document when significant technological changes are implemented on the platform. The Contractor shall participate with TSA in an application architecture review process for each new or changed application that includes but is not limited to: mapping the application to the architecture; assessing conformance with the architecture; determining gaps, exceptions, and required changes to the platform standards to accommodate the application; where changes are required in the platform, and agreed to by TSA, developing an implementation and test plan to validate the changes in the Integration Lab in Reston; providing the application integration strategy required to assist with the development of a COOP Plan in concert with the TSA Office of the CIO and the TSA Office of Emergency Preparedness; and maintaining consistency with TSA's "Office of Emergency Preparedness TSA Headquarters Plan – Assistant Administrator for Information Technology/Chief Information Officer and Information Technology/Chief Information Officer and Information Technology and Telecommunications Support.

The Contractor shall conduct contingency planning for the ITMS program and specifically for the enterprise applications represented in Section J, of the contract and manage the integration strategy for TSA applications.

The Contractor shall support TSA's Enterprise Data Model (EDM) in order to more effectively maintain software in accordance with the SDLC and other ITMS policies and procedures and service level agreements. The Contractor shall provide assistance to the EDM maintainers to define and document any custom extensions that are added to the TOP Oracle data model in conjunction with Contractor applications development or system maintenance to make sure that all such data elements are consistent with the EDM and are properly defined and documented and that the EDM is updated to reflect new data elements that arise from such modifications. The Contractor shall also work with other application providers as part of the application architecture integration assessment process to verify that they are aware of the applicable data standards in the EDM and to request that they document the data model used within their application for use by the EDM maintainers. The Contractor shall monitor periodic revisions to the EDM and provide documented additions to the TOP applications for the EDM.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 47
-----------------	------------------------------------	--	--------------

C.4.3.19 Operational Infrastructure Security

The Contractor shall provide IT security for equipment, networks and architecture of the ITMS in accordance with the SDLC and TSA security regulations and the approved Managed Services Provider Security Program Plan. The Contractor shall ensure highly reliable, secure, compliant transmission of data on the TSA infrastructure needed to support TSA goals and objectives. The Contractor shall monitor all elements of security through the Security Operations Center (note: SOC functions can be consolidated with NOC functions).

The Contractor shall provide general security services in addition to specific services that include the requirements to establish and maintain key relationships with vendors in order to expeditiously and efficiently support the TSA; to document outages and restoration activities; to apply patches, or operating system upgrades, as approved by TSA and to apply configuration changes to rules, signatures, or other specified components of the device or software, as approved by TSA.

The Contractor shall:

- 1) Assist in Publishing Office of Chief Information Officer (OCIO) security policy and procedures by providing recommendations.
- 2) Contribute to the TSA Systems Development Life Cycle (SDLC) Handbook and associated guidelines as they relate to security activities and issues.
- 3) Participate in and provide oversight of in-house security tests and evaluations conducted by the Contractor. The Contractor shall provide support for up to five (5) 3rd party security tests per year, upon Government request.
- 4) Evaluate Accreditation Packages and make recommendations regarding approval-to-operate/Interim Authority to Operate to the TSA OCIO, OIT Package.
- 5) Support the implementation of a TSA education, training, and awareness program for users and personnel in accordance with the developed/established TSA IT Security (ITSEC) Education, Training and Awareness Program (ETAP). The Contractor is responsible for training its own employees and sub-Contractors. (Any course, in all forms, developed as result of this particular task shall become the property of the Government.)
- 6) Maintain the TSA-wide Computer Security Incident Response Capability (CSIRC).
- 7) Operate and maintain the TSA OIT Internet Firewall infrastructure to protect TSA assets against external and internal threats.
- 8) Provide oversight for the TSA OIT disaster recovery program.
- 9) Perform operational management of Intrusion Detection System (IDS) equipment, rule sets, and log files; and conducting audits of logs from Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS).
- 10) Perform vulnerability scanning, reporting, and remediation for TSA operational equipment. TSA requires that the scanning tools used be COTS based. TSA requires that the tools meet existing enterprise architecture technical reference model, as revised, and at a minimum, pending NIAP certification. Security Vulnerability Scanning shall be sized, at minimum, for the existing ITMS environment with 18,188 workstations. Vulnerability Scanning shall cover a minimum of 20,000 IP Addresses.
- 11) Provide a vulnerability management service and use a tool to track the identified threats and their current disposition. The Contractor shall use a tool to track remediation actions undertaken to reduce risk. The Contractor shall provide TSA with a monthly report of vulnerabilities and their current disposition. The Contractor shall track all known and

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 48
-----------------	------------------------------------	--	--------------

identified IT vulnerabilities within the ITMS Bridge infrastructure. The Contractor shall report back to TSA known vulnerabilities on a monthly basis. The Contractor shall consolidate identified threats and their assessed threat levels against the environment.

- 12) Participate in TSA Executive Boards as requested.
- 13) Escalate and resolve issues to verify SLA compliance and customer satisfaction.
- 14) Provide specific recommendations for improving IT security.
- 15) Provide guidance on IT security related industry best practices.
- 16) Assist project teams in improving documentation standards.
- 17) Deploy and maintain anti-virus software on Contractor managed servers. Pricing for non-Wintel antivirus licensing shall be provided under individual task or delivery orders.
- 18) Provide administration, monitoring, and day to day support for security.
- 19) Limit OCISO (Security) policy change review/revision requests to two (2) per week.
- 20) Limit OCISO requests to review other material for OCISO impact to two (2) per week.
- 21) Store diagrams on a central portal with a report of changes up to 14 days after the change.
- 22) Assure that internet traffic shall be capable of being authenticated to the domain account of the user.
- 23) Accommodate 5 3rd party test efforts per year. Should the Government want a 3rd party to test equipment, the Contractor shall provide full support to that 3rd party.
- 24) Internet access shall be logged and accessible via a reporting server in a format that shall allow TSA to track internet access per user.
- 25) Enable content filtering of Internet traffic with rule sets that can be modified by TSA.
- 26) Provide TSA a reporting server with the ability to pull reports on an as-needed basis.
- 27) Provide updated network diagrams including IP addresses to OCISO 14 days after updating. The network diagrams and documentation shall include the date of the change, and a listing of all previous changes to explain the difference between previous changes and the current diagram and documentation.
- 28) Implement a commercially available anti-SPAM solution to monitor all inbound and outbound TSA email upon TSA making product available as Government property.
- 29) Provide personal firewall support that addresses the management and administration of Symantec Client Firewall (SCF) on ITMS Bridge Windows workstations. This support shall include the distribution of Intrusion Detection System (IDS) signatures, software patch management, and applications monitoring. The administration of SCF shall include continued administration of application version, IDS signature, and product configuration. The monitoring and use of management consoles and reporting systems shall aid in virus protection.
- 30) Support a SOC Infrastructure designed to support 524 sites, 39 Firewalls, 54 NIDS, 382 HIDS, 375 ESM, 18,000 Seats, 55,000 users, 2509 Network Managed Devices, 457 Servers, and the specific monitoring of 641 devices. SOC Infrastructure Services shall provide correlations of security events for all monitored devices and provide reporting capability through a web portal accessible by TSA authorized users.
- 31) Deliver the overall ITMS Security Program Plan within sixty (60) days of contract award (see Section F, Deliverables).
- 32) Provide TSA with a threat assessment service based on information provided by the following processes and documents, for example: change control documents; threat reports; individual system security scans; firewall threat reports and system logs. In addition, the service will follow the TSA Risk Management policy in terms of how threat assessments are categorized.
- 33) Provide information on critical patch testing and implementation concept.
- 34) The Contractor management service center shall provide skilled network analysts on a 24x7x365 basis in support of the 802.1x port authentication requirements. The Contractor shall administer the VLAN and port reconfigurations as required based on incidents or

Contract	Document No.	Document Title	Page #
	HSTS03-06-D-CIO500	ITMS Bridge Contract	49

reports to the service desk. For example, this may include such requests as password resets and other authentication parameters that may result in no user network connectivity.

35) Enable 802.1x on all Contractor managed access devices capable of supporting this function. The Contractor shall determine the resources necessary to produce an 802.1x solution. In the end state the solution shall allow TSA the ability to require network authentication before nodes receive an IP address and are allowed to connect to the network. The Contractor shall provide the following deliverables at the completion of this effort:

- 1.) Cost Proposal for implementation and maintenance of the proposed solution. This should be separated into two areas: HQ and the rest of the TSA Contractor managed environment.
- 2.) System Design Document of the end-state of the end solution.
- 3.) WBS for the labor hours for specific work components required for the proposed solution.
- 4.) Labor Hours necessary for the ongoing maintenance of the solution.
- 5.) BOM (Bill of Materials) for the proposed solution. This shall include all hardware and software with cost prices to purchase and any other fees (management, support) required to make the solution viable. This solution shall leverage as much equipment as possible to include testing equipment.
- 6.) Implementation Plan and schedule. While exact dates are not expected, TSA does expect the Contractor to propose timeframes to complete each stage of the solution.

TSA does not expect the above mentioned required actions to take the lifetime of the Bridge Contract to complete.

- 36) Deliver admin passwords for Local Admin accounts, Enterprise admin accounts, and Service accounts for all Contractor managed domains whenever an admin password is changed.
- 37) Provide a local administrator password management service. This service shall provide the Government with management, change control, and administration of the local administrator account and password on Contractor managed workstations. This service shall also include administration of Web and database applications supporting the service. The Contractor shall change default local administrator account username and password every ninety (90) days in accordance with TSA policy. The new account username and password information will be provided to TSA upon change.
- 38) Enable commercially available pop-up blocking and Anti-Spyware software on all applicable end-user devices.
- 39) Provide monthly reporting of all Firewall changes to TSA.
- 40) Separately aggregate security related trouble tickets by the SPOC and maintained by ITMS. Access to this list shall be restricted to authorized users.
- 41) Provide an analysis with a business justification for deploying vs. not deploying as critical patches are released by the manufacturer.
- 42) Provide monthly report on perimeter Firewall activity to include threat analysis.
- 43) The Contractor shall provide Firewall management and monitoring support for a total baseline of 32 Cisco PIX Firewalls (12 HA Pairs / 9 Standalone), a Cyberguard Firewall High-Availability Pair (HA), and a Sidewinder Firewall - 2 High-Availability Pairs (HA).

This service shall support assets under Managed Services by the Contractor. Remediation activity shall vary depending on the nature and scope of the IT products introduced into the environment and

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 50
-----------------	------------------------------------	--	--------------

incident response activities may fluctuate according to customer request for specific instances, yet this service shall be dependant on customer guidance and policy.

For example, if systems managed by a third party do not have proper anti-virus and/or patch levels, these systems may pose an elevated risk to other managed TSA IT assets. The Contractor processes shall work as designed to identify, contain, remediate, and report known vulnerabilities and exploits against TSA managed assets. The difference is that the Contractor process shall work to protect TSA assets from exploitation, however, the Government will not have knowledge of specific threats posed by unmanaged systems, nor will the Government have the information needed to remediate vulnerabilities to unmanaged systems. This shall be the Contractor's responsibility to manage per the TSA Incident Response Process.

The Contractor shall bear the cost of restoration if the Contractor personnel or their subordinates are responsible for the incident. In cases where the Contractor provides management and maintenance support for the impacted element, the Contractor shall perform the restoration of the impacted element as appropriate to the work breakdown structure (i.e., OS and Exchange level restoration within the SMC; TOPS applications within AMSS; etc.). Specifically, the Contractor shall perform restoration services only to the extent that the Contractor shall provide the management and maintenance of the impacted element. The Contractor shall perform restoration services only to the extent that the Contractor shall provide the management and maintenance of the impacted element or to the extent that the Contractor caused the incident directly. The Contractor shall provide restoration services at an additional charge as directed by the Government Contracting Officer.

The Contractor shall be responsible for the following:

- 1) DHS minor 4300A revision are limited to 1 per month;
- 2) DHS major 4300A version releases are limited to 2 per year;
- 3) OCISO policy change review/revision requests are limited to 2 per week;
- 4) OCISO request to review other material for OCISO impact are limited to 2 per week;
- 5) TSA SDLC contribution request are limited to 1 per quarter and any meetings are within 30 miles of TSA HQ;
- 6) Contractor ITMS IS Operations Manual shall consist of five (5) major IS process areas with 30 supporting procedures and 20 artifact templates.

The Contractor shall provide Operational Infrastructure Security services to include desktop, network, data center, and applications for both hardware and software elements. Operational Infrastructure Security shall include:

- 1) Provide oversight and operational support of daily operations from the operational security perspective.
- 2) Work to maintain the integrity of security across all operational domains, and work in close coordination with other security personnel (e.g., at the SOC) to manage security incidents to maintain security across the ITMS enterprise.
- 3) Provide Security reviews for operational changes and COTS products.
- 4) Scans and Tests shall be included as part Security Operations Center services; therefore, it is not included in this section.
- 5) Security SLA Management shall be covered as part of Operational services.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 51
-----------------	------------------------------------	--	--------------

- 6) Risk Management, as a part of Operational Infrastructure services, shall include the following:
- a. Certification and Accreditation Management
 - b. Risk Identification
 - c. Risk Remediation
 - d. Incident Management
 - e. Intrusion Detection Monitoring
 - f. Incident Handling
 - g. Network Security Management
 - h. Firewall Support
 - i. Physical Security Monitoring
 - j. VPN Security
 - k. Ongoing Risk Assessment Activities for ITMS Security

The Contractor's risk management team shall participate in up to five (5) security product evaluations per year. The Contractor shall have personnel supporting the threat assessment service and shall follow the TSA risk management policy in terms of how threat assessments are categorized.

In circumstances where a system managed by a third party does not have proper anti-virus and/or patch levels, those systems may pose an elevated risk to other managed TSA IT assets. The Contractor shall identify, contain, remediate, and report known vulnerabilities and exploits against TSA managed assets. The Contractor shall work to protect TSA assets from exploitation.

The Contractor is not responsible for remediation of classified computer security incidents unless caused by the Contractor and/or their sub-contractors. In cases where the Contractor provides management and maintenance support for the impacted element, the Contractor shall perform the restoration of the impacted element as appropriate (i.e. OS and Exchange level restoration within the SMC; TOPS applications within AMSS; etc.). The Contractor shall perform restoration services only to the extent that the Contractor provides the management and maintenance of the impacted elements or to the extent that the Contractor caused the incident directly.

Operational Infrastructure Security shall include the following Regulatory Compliance:

- 1) Provide the required assistance to TSA in order for ITMS to be compliant with Government regulations, to include the following:
 - a. Federal Information Security Management Act
 - b. Computer Security Act of 1987
 - c. The Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)), also known as the Information Technology Management Reform Act
 - d. OMB Circular A-130
 - e. NIST FIPS-199
 - f. OMB Circular A-123, "Internal Control Systems"

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 52
-----------------	------------------------------------	--	--------------

- g. OMB Circular A-130, "Management of Federal Information Resources"
- 2) According to FISMA, the Contractor managed network and applications are not considered a National Security System; therefore the Contractor shall assist TSA in following the National Institute of Standards and Technology (NIST) guidelines as defined within the NIST Special Publication 800 series.
 - a. NIST SP 800-18 "Guide to developing Security Plans for Information Technology Systems"
 - i. Create a System Security Plan for new systems in coordination with the Government in accordance with NIST SP 800-18
 - ii. Update the System Security Plan as major changes to each system occur
 - b. NIST 800-26 "Self-Assessments Guide for Information Technology Systems"
 - c. NIST SP 800-37
 - i. Assist the Government in preparing the Certification Package, required for TSA to conduct the Certification & Accreditation phases of the process.
- 3) Assist TSA in its compliance effort with Department of Homeland Security regulations.
 - a. Verify that ITMS components are compliant with TSA regulations.
 - b. Verify that industry standard principles and practices are followed.
- 4) Comply with the following HSAR 3052.204-70 Security requirements for unclassified information-technology resources.

Security Requirements for Unclassified Information Technology Resources (Dec. 2003)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a TSA network or operated by the Contractor for TSA, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in TSA unclassified systems that directly support the agency's mission. The security requirements include, but are not limited to, how the TSA's sensitive information is to be handled and protected at the Contractor's and TSA sites, (including any information stored, processed, or transmitted using the Contractor's computer systems), the background investigation and/or clearances required, and the facility security required. This requirement includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include-

- (1) Acquisition, transmission or analysis of data owned by TSA with significant replacement cost should the Contractor's copy be corrupted; and
- (2) Access to TSA networks or computers at a level beyond that granted the general public, (e.g. such as bypassing a firewall).

(b) At the expiration of the contract, the Contractor shall return all sensitive TSA information and IT resources provided to the Contractor during the contract, and a certification that all TSA information has been purged from any Contractor-owned system used to process TSA information. TSA shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 53
-----------------	------------------------------------	--	--------------

C.4.3.19.1 Security Management

The Contractor shall be responsible for Information Technology (IT) security for all managed systems connected to a TSA network or operated by the Contractor for TSA, regardless of location in compliance with OCIO Policy Directive No. 2005-1. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in TSA unclassified systems that directly support the agency's mission. The security requirements include, but are not limited to, how the Transportation Security Agency's sensitive information is to be handled and protected at the Contractor's site, (including any information stored, processed, or transmitted using the Contractor's IT systems), the background investigation and/or clearances required and the facility security required. This requirement includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

The Desktop Security Management for the Contractor managed environment shall be sized to address TSA's 18,188 workstations. Desktop security management shall include: Personal Firewall RuleSet Development, Local Administrator Password Management, System Anti-Virus Management, System Anti-Virus Monitoring, and Anti-Spyware Management/Monitoring for 18,188 desktops/laptops.

C. 4.3.19.2 Virus Management

The Contractor shall provide virus management for Contractor managed client, server, and network services in accordance with all TSA/ Federal Security Standards.

C. 4.3.19.3 Security Program Plan

The Contractor shall provide, implement, and maintain an IT Security Program Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Program Plan shall be compliant with Federal laws that include, but are not limited to, the Computer Security Act of 1987, and the Federal Information Security Management Act of 2002, as amended by the E-Gov Act of 2002. The plan shall meet IT security requirements in accordance with Federal policies and procedures that include, but are not limited to OMB Circular A-130, Management of Federal Information Resources, Appendix III, DHS Sensitive Systems Policy Directive 4300A, TSA Management Directive 1400.3, current DHS Secure Baseline Configuration Guides and section 4.3.20 of this document.

Within 60 working days after contract award, the Contractor shall submit for approval an IT Security Program Plan. This plan shall be consistent with and further detail the approach contained in the Contractor's proposal or quote that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as approved by the Contracting Officer and OCISO, shall be incorporated into the contract as a compliance document. This plan shall describe the processes and procedures that will be followed to provide appropriate security of IT resources that are developed, processed, or used under this contract. The Contractor shall conduct a Technical Interchange Meeting within 10 working days after contract award.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 54
-----------------	------------------------------------	--	--------------

C.4.3.19.4 Certification & Accreditation

The Federal Information Security Management Act (FISMA) requires agencies to provide information security for the information and information systems that support the operations and assets of the agency. The primary way for ensuring that agency information and information systems are adequately protected is by following the ongoing Risk Management process known as Security Certification & Accreditation.

Security Certification & Accreditation (C&A) is a four-phased, dynamic risk management process focused on two distinct procedures: certification and accreditation. The Contractor shall utilize National Institute of Science and Technology (NIST) publications and templates and Government mandated automation tools, such as the Department of Homeland Security mandated RMS and TAF tools.

The Contractor shall support Certification and Accreditation activities conducted by TSA. The Contractor shall provide compliance services to ensure C&A documents are compliant with federal standards. The Contractor shall present and the Government will approve the methodology used to ensure compliance. The Contractor may be asked to prepare the following artifacts as part of the Certification and Accreditation package:

- Risk Assessment Report (RA)
- Up-to-date System Security Plan (SSP)
- Tested Contingency Plan (CP)
- Security Assessment (formerly ST&E) Procedures
- Certification Package
- Security Assessment Report
- Up-to-date Plans of Action & Milestones (POA&Ms)
- Self-Assessment (SASMT)

Risk Assessments shall use the above artifacts, but not limited to, as a basis for identifying risk. The duration of Risk Assessment activities performed by the Contractor shall require a minimum of two weeks.

These documents are expected to be provided in accordance with ongoing TSA System Development Life Cycle Management (SDLC) and Capital Planning and Investment Control guidelines. Any methodology used by the Contractor shall be presented and agreed to by the Government. Updates and changes to SDLC artifacts such as system security plans, risk assessments, contingency plans, and self assessments will be performed for those systems under managed services. For those changes not included in managed services, or in Contractor proposal, updates and changes will be included as a part of an individual task or delivery order.. System owners will be appointed by TSA.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 55
-----------------	------------------------------------	--	--------------

C.4.3.20 Work Breakdown Structure (WBS)

For each PWS task, the Contractor shall develop and use a Work Breakdown Structure (WBS) to segregate the work scope requirements for each task provided into definable product elements and related services and data. The WBS shall be a direct representation of the work scope into appropriate elements for cost accounting and work authorization the WBS shows how program costs are summarized for the lower elements to the total program level.

C.4.3.20.1 WBS Dictionary

The Contractor shall prepare a WBS dictionary for each task which requires the development of a WBS. This dictionary shall define the work scope represented in each element of the WBS. This shall include summary work scope descriptions and/or references to the applicable sections of the performance work statement in order to provide a logical cross reference.

C.4.3.21 Compliance with SDLC

The Contractor shall use the TSA System Development Life Cycle (SDLC) methodology as a guideline for all program and project activities. Due to the over-riding cost concerns of following the TSA SDLC in its entirety, the Contractor shall comply with the TSA System Development Life Cycle (SDLC) methodology, including the production of Documents/Artifacts, when those individual artifacts are called out specifically and listed individually in a SR. The additional costs associated incurred by the Contractor by providing all the specific documentation and/or project artifacts, as those costs shall be incurred to that specific project/SR. TSA will work to ensure that SDLC artifacts are listed in the SR request at the time of submittal to the Contractor. The Government reserves the right to tailor required SDLC documentations and processes via specific references in the SR. The Contractor shall be expected to understand the SDLC guidelines, value and advise TSA of potential work product documentation that may not have been requested by TSA.

C.4.3.22 Subject Matter Expert (SME) Support Services

The Government may require subject matter experts (SMEs) to support emerging or unique requirements across a broad range of disciplines and transportation modes, e.g., engineering, security, analysis, logistics, etc. that are not definable at contract award. These SME support services will be purchased on a case-specific basis.

C.4.4 Desktop Managed Services

The Contractor shall provide Core Managed Desktop Services to the user. The Contractor shall assume responsibility for existing desktop hardware and will assure the equipment remains operational. Desktop services shall include the provisioning and managing services necessary to enable end-users throughout TSA to access the data required to perform their jobs effectively.

The duties of field service support shall include but not be limited to the following: possess all knowledge of the Tier I technicians; Use of the Knowledgebase; be knowledgeable in Microsoft

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 56
-----------------	------------------------------------	--	--------------

desktop and application configuration; perform network accessory maintenance (e.g., printers, file storage, CD burners); be knowledgeable in analog technology support (e.g., fax, modems); perform network user support; performing installs, moves, adds, and changes; perform Blackberry support; perform asset tracking; perform VOIP Support; Identify problem characteristics and root cause analysis; resolve inquiry/problem within prescribed time limits, if possible; otherwise, escalate to appropriate resource; notify the appropriate TSA managers/designees, as required; notify Tier 0/I personnel about call status/resolution; assist Tier 0/I personnel in logging the resolution in knowledge database; provide COTS/GOTS applications support.

The Contractor shall provide a Single Point of Contact (SPOC) service center through a Help Desk that will provide all aspects of desktop support services to include, at a minimum:

- Hardware and Software Maintenance
- Moves, Adds, Changes
- Trouble Ticketing
- Technician deployment

The Contractor shall include, within the non-warranty managed services CLINs, ongoing hardware and/or software maintenance prices for the following product technology types:

- 1) WINTEL desktop and laptop workstations;
- 2) WINTEL servers;
- 3) Cisco networking products; and
- 4) Workgroup and local printers.

The Contractor shall include, as an estimate, if necessary, any additional cost for third party, ongoing hardware and/or software maintenance costs not covered in the above mention list that are required beyond the TTO period.

C.4.4.1 Seat Management

This ITMS contract is a managed services contract with varying levels of support to be provided for different types of "Seats". A seat may consist of services (with or without equipment) ranging from an end-user seat (desktop, laptop, etc.) to an infrastructure seat (router, switch, server, etc.). The level of seat managed service support requirements will vary dependent upon seat functionality which may include maintenance, COTS software, help desk services, trouble resolution, asset management, security management, network maintenance, planning, system engineering, provisioning and billing. All services seats, as defined in this Performance Work Statement, shall be provided by the Contractor and included in the managed services seat CLIN price for each seat type. The seat CLIN price shall be distinct from any corresponding Product CLIN price. Seat Management services may be acquired via four (4) options:

- 1) Product/managed services "leased" over specified period, e.g., 36-months with any additional Transition to Ownership (TTO) and Transition to Removal (TTR) costs which are *not* included in monthly price
- 2) Product/managed services "leased" over specified period, e.g., 36-months with any additional TTO costs included in monthly product CLIN price

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 57
-----------------	------------------------------------	--	--------------

- 3) Managed services for Government Property (GP) within original "warranty" period, e.g., first 36-months
- 4) Managed services for GP beyond original warranty period

The Government will acquire its own products, as required, to support the environment and users. In order to meet the Service Level Agreements provided in the Performance Management Incentive Plan, the Government will provide equipment in sufficient quantities and in a timely, standardized fashion. The Government will provide the types and makes of equipment, meeting the agreed upon standardization requirements in sufficient quantities to allow a minimum of a three week stock. The Contractor in perspective of their support obligation shall advise the Government of the minimum inventories required. The Contractor shall stock inventory for a period of 60 days without additional cost to cover support obligations.

The Contractor may opt to inspect Government property outside the standardized Government equipment list prior to taking it into managed services. In cases where the equipment is still under warranty, the Contractor shall accept the equipment under managed services and oversee the warranty repair. In cases where the equipment is out of warranty or ill-configured to meet SLAs, the Government, with guidance from the Contractor may choose to acquire the parts to rectify the deficiencies. Here, the Government will acquire the parts, the Contractor shall accept the unit under managed services and the Contractor shall rectify the deficiencies with the new parts. If the Government, under advisement from the Contractor, determines that repairs to the equipment are so extensive that the cost would likely exceed of 1/3 of the value of the system, the parties shall agree that equipment should not be put in service.

The Government will order types and makes of equipment that meet the following standardization requirements:

- 1) Desktops/Laptops: Dell,
- 2) Wintel Servers: Dell, Unisys,
- 3) Unix Servers: Sun,
- 4) Network Routers: Cisco,
- 5) LAN Switches: Cisco,
- 6) Printers: Lexmark, Hewlett Packard or Unisys,
- 7) Firewalls: Cisco, Securer Computing or Cyberguard.
- 8) (Linux servers make and model will be determined at the time the Government anticipates a requirement.)

The Contractor shall evaluate the impact of the Government providing equipment outside the stated standardized list. Once the equipment is evaluated, the equipment shall be added to the standardized list and any subsequent introduction of the same equipment shall not require the Contractor to review. The Government will acquire its own products as required to support the environment and users. In order to meet the Service Level Agreements provided in the Performance Management Incentive Plan (PMIP), the Government will provide equipment in sufficient quantities and in a timely, standardized fashion. The Government will provide the types and makes of equipment, meeting the agreed upon standardization requirements in sufficient quantities to allow a minimum of a three (3) week stock.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 58
-----------------	------------------------------------	--	--------------

The Contractor, in perspective of their support obligation, shall advise the Government of the minimum inventories required. The Contractor shall stock inventory for a period of sixty (60) days without additional cost to cover support obligations. The Government will not pay across the board integration charges. These costs shall be appropriated in individual SR charges or in the general managed services costs, unless otherwise authorized by the Government.

The Contractor shall assist the Government in developing a forecasted ordering activity list. The Contractor shall advise the Government of the minimum inventories required. The Contractor shall stock inventory for a period of 60 days without additional cost. The Contractor shall use Government resources for transportation of equipment, or in other cases, the Contractor shall negotiate transportation costs on a case by case basis with authorized Government officials. In cases where the equipment is still under warranty, the Contractor shall accept the equipment under managed services and oversee the warranty repair. In cases where the equipment is out of warranty or so ill-configured to meet SLAs, the Government with guidance from the Contractor may choose to acquire the parts to rectify the deficiencies. Here, the Government will acquire the parts, the Contractor shall accept the unit under managed services and the Contractor shall rectify the deficiencies with the new parts. If the Government under advisement from the Contractor determined that repairs to the equipment are so extensive that the cost would likely exceed of 1/3 of the value of the system, the parties will agree that equipment should not be put in service.

Performance evaluation standards shall be used to measure delivery of seat management services, per the defined service levels (Attachment 5, See Section J). Performance evaluation factors will be used to assess quality of service.

The Government requires the Contractor to propose new technologies as they become available for Government consideration, and may expand services to include inter-modal user requirements, e.g., seaports, land border crossings, highways, etc. Also, the Contractor shall propose the deletion/retirement of obsolete and/or non-used technology.

The Contractor shall provide these services at the request of the Government in accordance with the procedures outlined in Section G.

C.4.4.2 Peripheral Devices

The Contractor shall provide managed services (help desk, asset management, trouble resolution, corrective maintenance, moves, adds, changes) for peripheral devices to include, at a minimum, printers, copiers and facsimile machines.

Printers

The Contractor shall support all TSA managed printers to include group, color, large, and multi-function copier/printers as ordered. The Contractor shall work with the Printer's OEM whenever maintenance is necessary.

Copiers

The Contractor shall support TSA copier machines as ordered. The Contractor shall provide routine maintenance including changing toner and clearing paper jams at TSA locations with on-site Tier II support. The Contractor shall work with the copier machine's OEM as necessary.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 59
-----------------	------------------------------------	--	--------------

Facsimile

The Contractor shall support TSA facsimile machines as ordered. The Contractor shall provide routine maintenance including changing ribbons or toner cartridges, installing fonts, and clearing paper jams at TSA locations with on-site Tier II support. The Contractor shall work with the Facsimile's OEM whenever necessary.

TV

The Contractor shall provide and support Televisions and video monitors as ordered.

Secure Safe

The Contractor shall support and maintain secure safes. The current safes are Hamilton two-drawer, single lock security safes which are capable of housing legal-size documents.

Secure Shredder

The Contractor shall support and maintain secure shredders. The current shredders are Model 233/1 which is a high security/light volume/cross cut paper shredder. The shredder can handle up to 4 sheets of paper at a time and produce a small 1/32" x 1/2" particle.

C.4.4.3 Personal Wireless (PDA and PED)

The Contractor shall support and provide Personal Digital Assistants (PDA) and Personal Electronic Devices (PED), for devices not covered in this contract, as a future requirement as defined on the ordering process (see Section G.10). PEDs are devices oriented toward a particular user that leverages wireless communication such as cellular or PCS services. Examples of these devices include RIMs BlackBerry product line. The Contractor shall support the core functionality (scheduling, contacts, time management, email), and individual operating systems. PDA's may be combined with Cellular/PCS services.

The Contractor shall provide these services at the request of the Government in accordance with the procedures outlined in Section G.

C.4.4.4 Service Provisioning

The Contractor shall provide and maintain an accurate, user-friendly, Web-based Provisioning System that enables the Government to order, track, and review the status of all ITMS Service Requirement Activities. Any systems, tools, processes, and resources needed to support the provisioning system for managing the provisioning of client and network assets shall comply with ISO 9000 and CMMI standards. Provisioning activities shall include, at a minimum:

- 1) Coordination
- 2) Procurement
- 3) Staging
- 4) Imaging assets
- 5) Deployment
 - a. Shipping the asset to the end-user location
 - b. Installing the asset

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 60
-----------------	------------------------------------	--	--------------

- c. Connecting the asset to the Network
 - d. Testing the asset
 - e. Obtaining final end-user acceptance of the asset
 - f. Completing a satisfaction level survey
- 6) Disposal of equipment based upon Government direction

The Contractor shall notify the requestor when an order has been received. The Government's preferred methodology is that the Contractor shall respond to the requestor with an email notification indicating receipt of the order and the tracking number; however, the Contractor may propose an alternative solution, but this solution must be approved by the Government before it is implemented by the Contractor. This notification shall also contain the name and telephone number of the assigned Contractor representative.

The Contractor shall provide real time updates to the status of the order in the provisioning system. The requestor shall be able to enter a tracking number and retrieve status information quickly and easily through the Website.

The following types of services shall be supported by the provisioning system:

- 1) IMAC and disconnect orders;
- 2) Information requests/service requests;
- 3) CLIN orders;
- 4) Special projects.

The Government requires access to the Web Order System on a real-time, periodic basis to a Government owned data repository under development. The Government requires access and support to establish periodic downloads of transaction data from the service provisioning system to a Government database.

C.4.4.4.1 Web-Based Capabilities

The service provisioning Website shall be accessible by the Government and shall contain all necessary provisioning information, and provide IMAC and Trouble Ticket request forms online for downloading and uploading. The Website shall have security features to protect information and must incorporate the capability to allow access to all authorized TSA requestors based on their need and role.

The Contractor shall be responsible for providing, implementing, and maintaining Web-based solutions to meet Performance Work Statement requirements. The Contractor provided Web-based solutions shall be compatible with Internet Explorer, and shall be available via Government Intranet. These applications shall be Java enabled and compatible with Internet Explorer greater than or equal to 6.0. All Web-based applications shall be accessible through one Web-based home page. The Contractor shall provide all necessary hardware to host the appropriate Web applications. The status of all Web-based applications shall be updated in real time. The Government shall provide the Government the capability to download or print information from the Web-based system. The Government shall have the capability to access the Web-based system through dial-up modems. The Contractor shall develop a web-based capabilities plan as a part of the E-Procurement plan (See C.4.3.14).

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 61
-----------------	------------------------------------	--	--------------

C.4.4.5 Grades of Service

The Contractor shall provide Desktop services consistent with the assigned Grade of Service of the seat.

Premier Service

The Contractor shall provide Premier Service to designated TSA HQ, TSOC and other on-site Tier II locations listed in section C.5.4 and TSA executives in the designated on-site Tier II locations who are identified on the VIP list. Premier Service requests shall be given the Contract's senior leadership attention. Service representatives or technicians shall respond within 30 minutes from when the call is logged where there is on-site Tier II service available and during standard site support hours.

Service and trouble tickets shall be resolved within 24 business hours for equipment that is under contracted, orderable CLINs from when the call is logged.

Premium Service

The Contractor shall provide Premium Service to TSA designated VIP users. Service or technicians shall respond within 4 hours from when the call is logged, or upon receipt of a troubled. Service or trouble tickets shall be resolved or escalated within 24 business hours from when the call is logged. A call is considered resolved when confirmed by appropriate TSA personnel.

Standard Service

The Contractor shall provide standard service to those seats designated as such. Service or technicians shall respond to trouble calls within 24 business hours from the call being logged, receipt of a troubled call or an authorized CLIN order. Service or trouble tickets shall be resolved or escalated within 24 business hours from when the call is logged. A call is considered resolved when authorized by appropriate TSA personnel.

New service requests for authorized CLINs shall be completed within five (5) business days after receipt of an authorized request.

C.4.5 Managed Network Services

The Contractor shall provide network management services to ensure highly reliably communications among networked ITMS users. Network services include resource planning, network design, configuration, performance monitoring, security, operations and maintenance, continuity of operations, fault isolation, and reporting. The Contractor shall provide a secured Network Operations Center. The Contractor shall support 24x7 operations, and provide tools and processes that comply with industry best practices and relevant SLAs.

The Contractor shall support component systems that include: hubs, switches, routers, communication links, regional links, and all other supporting data communications for ITMS's Network operations. Also included are systems that primarily support the Network infrastructure (refer to the ODC and Travel requirements attachment listed in Section J), including: network servers, VPN servers, application servers, file servers, message (e-mail) servers, gateway servers, web servers, bastion hosts, and firewall systems. The Contractor shall configure Remote Network Monitoring services to monitor 2,509 Network Devices at a level of service of 7x24x365.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 62
-----------------	------------------------------------	--	--------------

The Contractor shall serve as the focal point of expertise, or subject matter expert(s), for all aspects of the Local Area Network (LAN), the Wide Area Network (WAN), the computer systems and the software applications (e.g. Windows, routers, Exchange email, TCP/IP, and servers).

The Contractor shall closely couple Local Area Network (LAN) deployment with overall seat and Wide Area Network (WAN) deployment activities, and coordinated with a variety of TSA employees, stakeholders, partners, Federal agencies, and commercial entities to assure on-time operational capability.

The Contractor shall:

- 1) Resolve network-related issues through fault management, provide a single point of contact by phone or email, and help desk/trouble ticketing system to manage call placement and problem resolution.
- 2) Provide LAN and WAN subject matter experts.
- 3) Recover from disasters, prevent unauthorized access and alerts LAN administrators of security-related issues through security management.
- 4) Manage network assets, circuit utilization, Domain Name Services and IP address use through configuration management.
- 5) Produce and manage real-time performance statistics to address performance-related issues, and recommend performance improvements, when appropriate.
- 6) Provide Tier II and Tier III expertise to the Help Desk
- 7) Provide the network managed services, owns, operates, and maintains all associated hardware to provide the Government a fully network managed system. Upon expiration of the product 36-month lease, the Government will assume ownership of any associated software and licenses.

The Contractor's network management service shall include the following activities:

- 1) Base Ticket Notification;
- 2) Base Ticket Reporting;
- 3) MIB II Ticket Notification;
- 4) MIB II Ticket Reporting;
- 5) Proprietary MIB Ticket Notification;
- 6) Proprietary MIB Ticket Reporting
- 7) Fault and performance monitoring;
- 8) Client Notification and Coordination;
- 9) Problem Isolation
- 10) Problem Resolution;
- 11) Dispatching;
- 12) Carrier Problem Notification;
- 13) Carrier Problem Management
- 14) Managed Communications;
- 15) Performance Analysis and Management;
- 16) Traffic Shaping – QOS;
- 17) Configuration Management; Configuration Backup;
- 18) VLAN Configuration Administrations and Management;
- 19) Port Security Administration and Management (802.1x).

The Contractor's network management service shall be sized to handle, at minimum, the following remote network management types of device requirements:

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 63
-----------------	------------------------------------	--	--------------

- 1) Enterprise Routers - 27 ;
- 2) Mid-Range Routers – 126;
- 3) Small Routers – 110;
- 4) Enterprise Switches – 194;
- 5) Large Switches - 418 ;
- 6) Workgroup Switches – 1;
- 7) Rack Botz – 724;
- 8) VPN Concentrators - 2
- 9) Load Balancers - 6 ;
- 10) UPS – 444;
- 11) Windows Servers – 433;
- 12) UNIX Servers – 24.
- 13) (These numbers exclude 241 Data Circuits).

The Contractor shall use the following additional information in developing their response:

- 1) 500 Logical MACs per Month;
- 2) 1500 Incidents per Month;
- 3) Estimated Annual Service Calls: 6,864.

C.4.5.1 Performance Management

Performance Management applies a set of proven methodologies for managing business application performance over the TSA enterprise infrastructure. Such capabilities are required to provide quality business services management, as they relate to the support of the IT infrastructure. Without the ability to measure and control the delivery of information in support of specific business processes, IT can never achieve its ultimate mission. To meet this strategic goal, traffic management solutions perform the following major functions:

- 1) Application and network performance monitoring
- 2) Traffic shaping and performance trend analysis
- 3) Data compression
- 4) Load balancing
- 5) Infrastructure resource management
- 6) Global usage policy enforcement/measurement

The Contractor shall:

- 1) Establish and monitor service-level agreements for critical applications or sites, confirming the value of the delivered service
- 2) Identify and control the impact of undesirable or suspicious usage patterns, to ensure network resources are used only for their intended purpose
- 3) Provide detailed performance diagnostics that include connection profiling, server responses (TCP Health), forensic—traffic history, and round trip delays based on real traffic

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 64
-----------------	------------------------------------	--	--------------

- 4) Tune network resource allocation to improve the ability to deliver high quality services efficiently
- 5) Provide data export of KPIs for correlation with higher layer dashboards while enabling real-time, executive level views of network health to Government authorized staff
- 6) Provide a per-site view that shows all KPI metrics—all views should include navigation to higher-level views, drill-down to lower-level views, and provide the ability to navigate KPIs chronologically as histograms. Histogram metrics shall utilize bar graphs to reflect reporting data.

The Contractor shall provide the service and tools to continuously evaluate systems within the enterprise to ensure the delivery of end-to-end Quality of Service (QoS). The Contractor shall develop a Performance Management Plan and apply policy enforcement differentiated by mission-critical, recreational, malicious traffic patterns and numerous additional filters, resulting in strong assurance that traffic most important to the mission is given the highest priority as it relates to the use of network resources. The plan shall also detail how service-degrading anomalies and issues are escalated to enable quick and efficient resolution. This shall occur within 90 days of contract award.

The Contractor shall provide the service and tools to continuously evaluate the ITMS contract to ensure the required Quality of Service is delivered. The Contractor shall develop a Performance Management Plan which details the procedures, measures, monitoring and analysis tools, and performance parameters to ensure an efficient and consistent operation. The plan shall include details as to how service-degrading anomalies are escalated to ensure quick and efficient resolution. The plan shall address the Contractor's recommendations for applications reporting metrics on a daily, weekly and monthly basis after implementation of the Quest Application Management tool. The plan shall also detail how issues are escalated to ensure quick and efficient resolution.

The Contractor shall submit performance improvement plans in writing to the TSA engineering staff. TSA will return comments within one month. The plan(s) shall include procedures to measure, monitor and report network performance parameters to provide an efficient and consistent network operation along with recommended performance measurements.

C.4.5.1.1 Performance Management Requirements

The Contractor shall comply with the following performance management requirements:

- 1) Provide a solution delivering ongoing performance analysis
- 2) Develop a Performance Management Plan, and update it annually thereafter.
 - a. Include procedures to measure, monitor and report network performance parameters to promote an efficient and consistent network operation.
 - b. Significant parameters of performance measurement include, but are not limited to: end-user network response time.
- 3) Define and document ITMS performance requirements.
 - a. Service mappings
 - b. Thresholds
 - c. Alert Management
 - d. Reporting requirements
- 4) Provide oversight and management to promote optimal TSA insight into the operations environment. This includes, but is not limited to:

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 65
-----------------	------------------------------------	--	--------------

- a. Verifying that metrics that are incorporated into the contract are being monitored.
 - b. Providing on-site monitoring capability
 - c. Optimizing thresholds
 - d. Providing Alert management
 - e. Collecting Performance data for SLA management
 - f. Performing event correlation after an event and as a proactive management tool.
- 5) Promote continuous improvement towards ITMS service metrics.

C.4.5.1.2 Monitoring Tools

- 1) The Contractor shall identify, evaluate, develop, and implement performance management using automated tools from an operational support perspective for all network components, systems, and services.
- 2) The Contractor shall identify and implement metrics and thresholds to measure and manage network performance using automated tools with review and approval by the Government.
- 3) The Contractor shall use network tools to remotely identify and diagnose network problems.
- 4) The Contractor shall ensure performance monitoring tools integrate with existing tool suite.
- 5) The Contractor shall implement comprehensive event correlation across monitoring platforms.
- 6) The Contractor shall improve Enterprise Operations Views on operator consoles.
- 7) The Contractor shall develop and implement new capabilities to provide performance management functionality for new technologies as they are introduced into the production environment.

C.4.5.1.3 Service Level Agreements (SLAs) and Key Performance Indicators (KPIs)

- 1) The Contractor shall manage business requirements by developing SLAs that place a "business value" on particular services.
 - a. An SLA is an agreed-upon, measurable service metric "target" between the Contractor and TSA, and is applied to the services provided.
- 2) The Contractor shall define SLAs and KPIs for ITMS Services that directly reflect business requirements, IT capabilities, and appropriate levels of cost.
 - a. The Contractor, working with IT must be rigorous in determining what levels of service it can reasonably agree to deliver within capability and budget.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 66
-----------------	------------------------------------	--	--------------

- b. The Contractor, working with IT, must then create and maintain SLA metrics to measure the services provided.
- c. Services that cannot be measured must not be included in an SLA.
- 3) The Contractor shall provide TSA-tailored thresholds to monitor usage, throughput, errors, and congestion on the managed network with review and approval by the Government.
- 4) The Contractor shall provide operational support requirements for network and desktop performance during the development of new technology to ensure optimal performance in the production environment.
- 5) The Contractor shall thoroughly and carefully evaluate the impact on SLAs and the overall delivery of service of the following categories:
 - a. Services
 - b. Applications
 - c. Middleware (including databases)
 - d. Operating Systems
 - e. Hardware
 - f. Networks (Local and Wide Area)
 - g. Facilities

C.4.5.1.4 Map to Industry Standards

The Contractor shall map ITMS SLA metrics to comparable industry standard of 40,000 people distributed nation-wide, unless otherwise mandated by Government. The Contractor shall also ensure understanding of service dependencies and map these to respective infrastructure components.

C.4.5.1.5 Monitor Performance

- 1) The Contractor shall continuously and proactively monitor, record, and report network statistics that will optimize network performance, response times, and availability.
- 2) The Contractor shall monitor utilization and performance by site, application, and/or users with alarms and adaptive responsiveness to ensure mission critical performance.
- 3) The Contractor shall measure performance of network components for compliance with manufacturer's published performance specifications for network hardware and software.
- 4) The Contractor shall perform other performance measurements as required to meet service level requirements.
- 5) The Contractor shall monitor and manage, in real-time, the availability of network components, systems, and services for optimum performance, response time, and availability.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 67
-----------------	------------------------------------	--	--------------

- 6) The Contractor shall monitor and manage network traffic patterns and identify issues such as "bottlenecks" that may reduce performance.
- 7) The Contractor shall gather and analyze network and desktop statistical information and provide recommendations to improve network performance.
- 8) The Contractor shall provide routine reports on system status, availability and performance of network systems, services and components.
- 9) The Contractor shall provide recommendations to optimize and operate the network with predictable levels of performance to the Government.

C.4.5.1.6 Perform Trend Analysis

- 1) The Contractor shall perform detailed trend analysis of performance metrics and KPIs
 - a. Analyze baseline anomalies and issues,
 - b. Tune thresholds, and
 - c. Analyze historical information to identify trends.
- 2) The Contractor shall diagnose, identify, and correct failing network components or failure of interfaces between and among network components and other systems, operating environments, and/or applications.

C.4.5.1.7 Performance Reporting

- 1) The Contractor shall provide a comprehensive suite of reports to be available on a daily and monthly basis that describes and explains network performance.
- 2) Upon the Government's request the Contractor shall provide reports that include Root Cause Analysis of LAN performance and fault activity during the previous reporting period and recommend corrective actions for critical areas of the managed network.
- 3) The Contractor shall assess the impact of new applications/capabilities upon the network, and report any significant issues associated with impacts to these applications/capabilities.
- 4) The Contractor shall provide immediate written notification of conditions that have the potential to cause future network problems.
- 5) The Contractor shall provide the Government with: performance, exception, and trouble ticket reports on a daily and monthly basis.
- 6) The Contractor shall provide reports in a format that is easily accessible via Web-based format.
- 7) The Contractor shall provide the SPOC, PMO and TSA alert notification and recommendations when network elements exceed mutually agreed upon performance thresholds.
 - a. Provide the PMO and TSA with explanations and observations on alarms and their ramifications.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 68
-----------------	------------------------------------	--	--------------

- 8) The Contractor shall provide Periodic Network Reviews to provide NOC analysis and recommendations on identified LAN and server issues.
- 9) The Contractor shall recommend changes in the network needed to improve availability and response time.
- 10) The Contractor shall recommend, and, upon TSA approval, purchase, install and operate new tools that will assist in identifying, monitoring, and resolving actual and potential problems.
- 11) The Contractor shall optimize network efficiency by relocating servers, adding new LANs, when needed, and using load balancing and traffic routing techniques.

C.4.5.2 Monitor Network Performance

The Contractor shall continuously monitor and record network statistics to ensure acceptable network performance. The Contractor shall monitor network components, systems and services for optimum performance, response time and availability. The Contractor shall monitor and manage network traffic and identify surges and bottlenecks that may reduce performance. The Contractor shall gather and analyze network performance statistical information and submit performance reports in accordance with Section C.4.2. The Contractor shall provide recommendations to improve network performance to the Government.

C.4.5.3 Operations and Maintenance

The Contractor shall provide Network operations and maintenance support through the NOC. The Contractor shall monitor operations and performance of network systems. The Contractor shall provide system administration support for end users. The Contractor shall provide network monitoring pricing. The Contractor shall provide a network monitoring system that will enable the Government to monitor the performance and availability of the Contractor provided services and equipment on a real-time, read-only basis.

The Contractor shall provide support for Production Engineering to be included in the Enterprise Operations and Maintenance function. These tasks shall include: acting as a lead technical expert for the enterprise in the areas of network infrastructure (refer to the ODC and Travel requirements attachment listed in Section J) and management, server infrastructure and management, and support of systems in the production environment to include servers, operating systems, and network devices; providing leadership for production support projects and processes with business impacts; ensuring repeatable processes that will provide the highest levels of availability and stability to include insertion of system upgrades in both the OS and device level, implementation of new technologies, and oversight of the production environment; providing strategic direction and developing tactical plans composed of WBS and milestones that will further ensure that TSA successfully meets its mission objectives. Providing support for Production Engineering shall include completing complex tasks to ensure optimal operations in all aspects of the TSA infrastructure.

The Contractor shall:

- 1) Operate and monitor the availability and performance of the Network
- 2) Monitor and support all network systems
- 3) Provide reports of network outages including planned outages

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 69
-----------------	------------------------------------	--	--------------

- 4) Provide operational support for all server application administration, systems programming support, database administration, hardware/software configuration, and inter-system communications.
- 5) Provide systems and application administration for end user rights, including access, and e-mail
- 6) Identify, evaluate, develop and implement network management from an operational support perspective to perform proactive fault management, performance management, growth management, security management, asset management, accounting management, and desktop management for all network components, systems, and service
- 7) Identify and implement metrics and thresholds to measure and manage fault, growth, performance, security, and accounting for the network and desktop using automated network tools
- 8) Consolidate network tools into an integrated network management system
- 9) Review the current network tools and make recommendations for enhancement or replacement
- 10) Develop and implement new capabilities to perform the required network management functions based on the implementation of new technology
- 11) Provide operational support requirements for network tools during the development of new technology to ensure maintainability and supportability of new technology
- 12) Identify and resolve problems proactively before they affect users in order to ensure high network availability and reliability
- 13) Plan and manage network growth by predicting future trends based on historical network trends and business information.
- 14) Monitor and manage network traffic patterns and identify issues such as "bottlenecks" that may reduce performance
- 15) Provide routine reports on system status and availability of network components, systems, and services

C.4.5.4 LAN

The Contractor shall provide secure Local Area Network (LAN) infrastructure and server management services to ensure data access and communications at TSA locations for mission requirements is provided. The Contractor shall manage, design, procure, integrate, configure, install and conduct testing for the deployment of LAN devices and servers in coordination with WAN and seat rollout, in support of TSA requirements.

C.4.5.5 WAN

The Contractor shall provide Wide Area Network (WAN) infrastructure and services to interconnect all TSA and DHS HQ locations. Nationwide WAN services shall carry data, voice, and video with full management and quality control in support of TSA missions. Covered: All CONUS locations with WAN Connectivity.

Refer to Attachment 5, Section J for SLA details.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 70
-----------------	------------------------------------	--	--------------

The Contractor shall provide these services at the request of the Government in accordance with the procedures outlined in Section G.

C.4.5.6 VPN Services

VPN capability, servers, applications, and support for TSA personnel without LAN/WAN access, including personnel working from off-site locations shall be required. The Contractor shall:

- 1) Provide VPN support and services for TSA personnel without LAN/WAN access to include:
 - a. Design, develop, procure and install synchronous and asynchronous VPN communications capabilities. This includes supporting asynchronous communications servers, statistical multiplexers, modem pools, gateways and any other communications support hardware and software needed by TSA.
 - b. Develop practical and effective approaches to enhance external access to the network by TSA end-users, employees traveling or working at home, or other approved remote users.
 - c. The approach shall include, but not be limited to, identification of alternative remote access methods, the development and implementation of an additional level of security for VPN (Dial-In) users to protect TSA sensitive resources, and increasing the data rate over currently available modem pools.
 - d. Improve the gateway and enhance the Dial-Out capabilities for users accessing information from external information providers.
 - e. Remote TSA end users shall be able to access all network resources within prescribed security limits. The functionality of their access should only be limited by the performance implications of their slower speed connection from the remote site to the network. Therefore, they should have all the network functionality their user ID would permit if directly on the network, the only penalty being the slower speed imposed by the remote connection.

The Contractor shall provide these services at the request of the Government in accordance with the procedures outlined in Section G.

C.4.6 Telecommunications Services—CONUS/OCONUS

The Contractor shall provide mobile technologies and services for employees who need immediate access to mobile communications services for both nationwide and internationally use. Cellular service to be provided should include, but are not limited to, voice calls and related features such as voice mail, call forwarding, three way calling and caller ID as well as short messaging services (SMS). The Contractor shall make available under this contract a range of instruments and devices (analog, digital, secure) that shall deliver Cellular/Personal Communications Service (CPCS). The Contractor shall provide Internet Protocol Telephone (IPT) or Voice over Internet Protocol (VoIP) and mobile technologies and services. Support is considered part of a Seat concept and shall include instruments, services, and cabling along with other bundles services. The existing cellular services vary in availability, reliability and cost depending on location and provider.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 71
-----------------	------------------------------------	--	--------------

Additional Program Requirements:

- 1) Required in-stock devices to meet expedited deployment. Stock should be sufficient to meet high demand and emergency escalations. There should be no corresponding cost to retain in stock. Cost will be incurred upon deployment to end-user. This shall be included in the Contractor's other bundled services proposal.
- 2) Asset Management Services management shall include a plan to include Government Property and maintenance of devices on the monthly inventory report.
- 3) The Contractor shall propose seamless customer service support (i.e., helpdesk, 800).
- 4) The Contractor shall provide all services and features as described in the Contractor's proposal for the life of the contract. Features to be provided hereunder are described in Contractor's proposal. The Contractor shall identify new services and features as they are made available to the general public during the life of the contract(s). Pricing for new services and features shall be negotiated at the time of acceptance, and will be added to the contract(s) via contract modification before they become effective.

The Telecommunications services provided shall comply with the TSA Management Directive No. 1400.3, Security Policy Handbook – Chapter 4.

C.4.6.1 Personal Wireless (PDA and PED)

The Contractor shall provide commercial PDA and PED technology that will meet CONUS and OCONUS requirements as a future requirement as defined in the ordering process (see Section G.10). The proposed solution shall provide equipment that is portable in size and weight providing comfort and convenience to all user.

PDA and PED technology shall comply with current security standards. Please refer to section C.4.6 Telecommunication Services (Wireless) – CONUS/OCONUS for security standards and policies.

Additional Requirements:

General

- 1) Support PDA related desktop software
- 2) Support compatible installation of numerous applications
- 3) Recommend the use of the Palm OS software or Pocket PC
- 4) Synchronization conduit for Microsoft Outlook
- 5) Provide USB and serial connection for phone and PDA interfaces
- 6) Provide GPS Locator
- 7) Support encrypted HTML browsers for secure online transactions

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 72
-----------------	------------------------------------	--	--------------

Communication Features

- 1) Email capable – Must be capable of synchronizing email wirelessly through the user of a client on the machine or other means.
- 2) Text messaging capable
- 3) Speakerphone
- 4) Voice memo (desired, not required)
- 5) Voice-activated dialing (desired, not required)
- 6) Web access

Productivity Features

- 1) Calculator
- 2) Contact directory
- 3) Headset jack – capability to use a hands free set is required
- 4) Memo pad (desired, not required)
- 5) Palm OS or Pocket PC features
- 6) Scheduler – Must have the ability to synchronize contacts as well as calendar
- 7) Speed dialing
- 8) To do list (desired, not required)

The Contractor shall provide these services at the request of the Government in accordance with the procedures outlined in Section G.

C.4.6.2 Wireless Data

The Contractor shall provide wireless data as a future requirement as defined in the ordering process (see Section G.10). The Contractor shall provide wireless data technology for the ITMS Program as ordered. This includes conversion devices from a wired environment into a wireless environment. The technology used to push this wireless data over a large area.

Wireless technology shall comply with current security standards. Please refer to section C.4.6 Telecommunication Services (Wireless) – CONUS/OCONUS for security standards and policies.

The Contractor shall provide these services at the request of the Government in accordance with the procedures outlined in Section G.

C.4.6.3 Blackberry Services

The Contractor shall provide Blackberry technology for the ITMS Program as ordered. This includes data only as well as voice and data-capable devices. The Contractor shall provide support for existing devices deployed as well as meet additional device requirements. The Contractor shall upgrade to the latest version of the BlackBerry server software and remain current with new service packs and versions. The installed base of Blackberry handsets is already capable of supporting the upgrade to the latest version of the server software.

The Contractor shall provide a cost-effective Wireless data and voice solution that has the capability to:

- 1) Wirelessly send and receive email via Push-like technology.
- 2) Provide voice services as applicable.
- 3) Transfer current cellular phone numbers to integrated Blackberry device.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 73
-----------------	------------------------------------	--	--------------

- 4) Provides minimum of Triple DES end-to-end encryption of data; this requirement shall be met by the Contractor.
- 5) Meet or exceed, or in the process thereof, NIST FIPS certification.
- 6) Provide enterprise class service and scalability from an "in-house" infrastructure.
- 7) Be expandable to secure content delivery in addition to email.
- 8) Multiple Tiers of handhelds available for different levels of users, both with and without voice capabilities.
- 9) Provide roadmap or overview for legacy domain migration specific to Blackberry.
- 10) Present pricing in a subscription/seat-based format.
- 11) Provide standard Blackberry accessories.
- 12) Factor in growth capacity and utilize a solutions provider with a proven track record in secure wireless data and voice solutions.
- 13) Stock Government property devices. Stock should be sufficient to meet high demand and emergency escalations. There shall be no corresponding cost to retain in stock. Cost shall be incurred upon deployment to end-user. This shall be included in Contractor other bundles services proposal.
- 14) Provide Asset Management Services management shall include a plan to include Government furnished equipment and maintenance of devices on the monthly inventory report.
- 15) The Contractor shall propose seamless customer service support (i.e., helpdesk, 800).

TSA Customer Requirements

The following customer requirements are specified and shall be met by the Contractor:

- 1) Infrastructure: The infrastructure for the Blackberry Wireless Solution shall be contained "in-house" – all encryption and non-transmission tasks are handled behind the firewall.
- 2) Functionality (ease of use): The Blackberry system must be easy to use and trainable for the end user.
- 3) Security: The solution must be FIPS certified or in progress thereof and provide no less than Triple DES end-to-end encryption of data.
- 4) Expansion capability: The solution must be scalable to be able to expand to possibly thousands of users.
- 5) Best Practices/Open Standards: The system should use industry and Government best practices.

TSA IT Requirements

The following IT requirements are specified and shall be met by the Contractor:

- 1) The port will be configured for TCP outbound only.
- 2) The solution will in no way change the functionality of the current Exchange mail infrastructure.
- 3) RIM tag line is removed from outgoing email.
- 4) A centralized management console is required to manage the overall solution. Access to the console will be provided to Managed Services Administrator and Monitoring Agent. Physical location of console is on each instance of BES

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 74
-----------------	------------------------------------	--	--------------

TSA Security Requirements

Wireless technology shall comply with current security standards. Please refer to section C.4.6 Telecommunication Services (Wireless) – CONUS/OCONUS for security standards and policies.

The following security performance requirements are specified and shall be met by the Contractor:

- 1) All data will be protected by no less than Triple DES encryption for wireless transfers.
- 2) The device and overall solution must comply with the DHS Security Policy for Wireless devices/services.
- 3) The solution will meet or exceed FIPS certification or be in process thereof.
- 4) Handheld policy controls will be available to maintain security protocols (password policies, encryption key updates, etc.).
- 5) Power on password protection with enforcement, to include password length, complexity, frequency of change, history, and disabling of user overrides.
- 6) No inbound firewall ports will be opened.
- 7) Blackberry Enterprise Server administration is restricted to authorized personnel only.
- 8) Enable an email confidentiality statement with deployment of 'white package'.

Performance Requirements

The following performance requirements are specified:

- For the white package network, a redundant server will exist to provide service in the event of failure of primary server.
- Four (4) business days replacement of handheld devices diagnosed as 'dead' by SPOC (once sparing requirements are confirmed).

Managed Services Requirements

Site preventative maintenance, installations, emergency repair/replacement, ongoing support provided by the Contractor.

TSA Training Requirements

The following indicates user and equipment training on Blackberry devices:

- Create user package and collateral to be made available at implementation or during formal training.
- Provide formal end-user training.
- Provide FAQ via the TSA intranet.

System Requirements

- Support users on all active domains
- Disposition and migration plan for users on legacy domain – tsa.dot.gov
- Send and receive data from the BES in accordance with performance measures outlined in Section J attachments.

The Contractor shall provide these services at the request of the Government in accordance with the procedures outlined in Section G.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 75
-----------------	------------------------------------	--	--------------

C.4.6.4 Land Mobile Radio

The Contractor shall support Land Mobile Radio (LMR) communications to include basic RF Engineering in support of deployed LMR solutions as ordered. TSA's LMR utilizes frequencies authorized for use by the National Telecommunications Information Agency (NTIA). The frequency band utilized is based on the Federal Law Enforcement Very High Frequency (VHF) allocation in the 162MHz – 174MHz range. TSA currently has LMR equipment deployed to 429 sites throughout the United States and Provinces. Currently, these locations are supported by 7,400 LMRs, with 88 repeaters enhancing the LMR communications at over 80 of the locations. The Contractor shall provide coordination of ITMS frequency management activities. The Contractor shall manage the Land Mobile Radio (LMR) communications facilities for 429 TSA locations in the United States and its Provinces. Currently, these locations are supported by 7,400 LMRs, with 88 repeaters enhancing the LMR communications at over 80 of the locations. The Contractor shall also provide coordination of ITMS frequency management activities.

Technology Requirements shall be met by the Contractor:

Project 25 compliant VHF narrow-band digital system operating range of 162MHz – 174MHz with backward compatibility to wideband analog that is capable of the following:

- 1) Meets NTIA spectrum standards specified in NTIA Manual, Chapter 5, Section 5.3.5.2
- 2) Supports AES encryption standard and is FIPS certified
- 3) Non-proprietary modulation that allows for interoperability with Federal, State and Local Enforcement/First Responders
- 4) Over-The-Air-Re-key (OTAR) capable
- 5) Supports advanced data applications
- 6) Subscriber equipment (mobile/portable) be capable of a minimum of 16 individual channels

Program Support Requirements shall be met by the Contractor:

- 1) Personnel resources for Frequency Management, Interoperability and RF Engineering. Frequency Management services to include – coordination of frequency assignment requests and documentation, license modifications and updates, spectrum management functions and interagency frequency coordination.
- 2) Program Management resources necessary to plan for and manage the design, development, procurement, configuration, integration, deployment and operations of the program
- 3) Program Management Office resources for program, procurement and deployment management, systems architecture, systems design, systems integration, testing and quality assurance
- 4) Management and control of all LMR assets.
- 5) PMO reporting the LMR program to include regular program status communications regarding schedules, current status, design baseline and approvals, policy, issues and escalations

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 76
-----------------	------------------------------------	--	--------------

The Contractor shall provide these services at the request of the Government in accordance with the procedures outlined in Section G.

C.4.6.5 IPT/VoIP

See Infrastructure Engineering Section C.4.9.

The Contractor shall provide these services at the request of the Government in accordance with the procedures outlined in Section G.

Telephony

The Contractor shall provide commercially available telephony services such as, as ordered, to include dial plans, call forwarding, speed dial, call transfer, and call set up. The Contractor shall provide voice mail service and maintain the phone number records.

Telephony shall comply with the current security standards in the TSA Management Directive No. 1400.3, Security Policy Handbook – Chapter 4, Section 11.

Call Accounting System

The Contractor shall provide a Call Accounting System to track traffic flow within the ITMS-Voice over Internet Protocol (VoIP) system and external systems (e.g., the local PSTN, FTS2001, WITS). The Contractor shall provide all hardware, software, and integration support necessary for the Government to interface with the Call Accounting System. All data contained and used in the Call Accounting System shall be the property of the Government, and shall be formatted in a way that it can be transferred from that system into another system using available non-proprietary standard electronic format.

The Contractor provided Call Accounting System shall provide for ad hoc reporting as it relates to station and traffic records. Reports generated on station specific information shall be restricted to the appropriate law enforcement entities and DHS officials with the required written authorization. The Contractor shall support traffic and station ad hoc reporting for any specified period of time over the life of the contract.

Call Detail Records

The Contractor provided Call Accounting System shall retain all call detail records, for a minimum of sixty (60) days, of any call activity originating from or terminating to an ITMS station, interfaced equipment, or service. The Contractor shall provide the Government the ability to access the current month's and the previous month's call detail records for all calls that involve an ITMS provided voice station. The Contractor shall provide the Government the ability to access all archived call detail records within two business days of receiving notice from the Government.

The Contractor shall provide and maintain a call detail record database containing at a minimum, the following fields, for each call:

- 1) Site
- 2) Telephone number
- 3) User

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 77
-----------------	------------------------------------	--	--------------

- 4) Called number for outgoing calls
- 5) Calling number for incoming calls
- 6) Date
- 7) Duration
- 8) Trunk access
- 9) Cost

C.4.7 Special Services/Systems

C.4.7.1 Electronic Surveillance

The Contractor shall provide electronic surveillance technology as a future requirement as defined in the ordering process (see Section G.10). The Contractor shall provide electronic surveillance technology and services. Surveillance cameras shall be installed in several locations within an airport. The Contractor shall provide the capability for the video viewing from either a desktop or laptop as well as LAN viewing. The Contractor shall connect all TSA checkpoints into a TSA LAN backbone at the airport, FSD office (if on-site), training rooms, FSD operations center, and any other fixed location where TSA has equipment.

The Contractor shall support the legacy Electronic Surveillance System implemented for Aviation Operations for monitoring checkpoints and baggage screening. When directed by the Government the Contractor shall provide a new digital video surveillance system that will operate within the ITMS network, and shall provide the ability to link other non-TSA cameras to the video servers as requested by the Government. The Contractor shall also support a web based interface for viewing over the WAN by authorized parties; bandwidth limitations taken into consideration.

The Contractor shall provide these services at the request of the Government in accordance with the procedures outlined in Section G.

C.4.7.2 Managed Applications Services

The Contractor shall provide managed applications services to ITMS users. The Contractor shall maintain legacy applications (See Section J, Attachment 15, TSA ITMS Application List).

The Contractor shall provide and maintain file, print, and application servers for ITMS operations. The Contractor shall upgrade service space as appropriate and in accordance to findings during capacity planning.

It is anticipated that over the life of this contract, DHS will consolidate select managed applications services. The Contractor shall coordinate with these DHS activities as required.

AMSS shall manage the applications as referenced in Section J Attachment 15 with the exception of: all applications located at TSOC, Known Shipper, Registered Traveler, Documentum Upgrade, US Visit Air Exit, and Fingerprints & Lems. AMSS shall support Utility Items as they exist currently in the TOP and ACS environments.

The Contractor shall monitor, manage administer and deliver second and third level support for key TSA applications, as referenced in Section J, Attachment 15. The Contractor's support shall focus on enterprise application packages with an emphasis on TSA technical support management and end-

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 78
-----------------	------------------------------------	--	--------------

user satisfaction. The Contractor shall deliver application support and services throughout TSA's various software applications' operational lifecycles. Significant elements of the Contractor's support and management solution shall include but not be limited to providing: integrated call center support and Help Desk services; application and database monitoring; technical and functional application support; applications and database management. The Contractor shall remain at the forefront of presenting and managing change via the TSA Review Board process. Once an application is promoted into production, the Contractor shall provide operations and maintenance functions.

The Contractor's AMSS staff shall implement patches and upgrades for TOP and ACS environment based upon an Impact Statement and appropriate risk/reward analysis. The Contractor's AMSS staff shall perform an impact analysis of critical patches within 48 hours. The Contractor shall perform interim mitigation for applicable patches as available. The Contractor's AMSS staff shall coordinate efforts with security staff and other appropriate Contractor personnel. The Contractor's AMSS staff shall support builds in the ITE environment, testing efforts, TSA Review Boards, and promotion to production. Performance testing results for AMSS Managed Applications shall be provided by Quest Standard 'out of the box' reports and functionality. Additional performance reporting shall be considered to be out of scope of this ITMS effort. AMSS shall continue to perform DBA functions for the Documentum application. Documentum enhancements are outside the scope of this effort. The Contractor's AMSS staff shall support upgrades based upon mutual agreement within mutually agreed upon timeframes. AMSS DBA staff shall be on-site in Reston, VA from 07:00 through 19:00 EST Monday through Friday during scheduled work days for the TOP environment. The Contractor's AMSS Technical Support Engineers shall be on-site at TSA Headquarters from 07:00 through 18:00 EST Monday through Friday during scheduled work days.

The Contractor shall manage the applications as referenced in Section J Attachment 15 with the exception of: applications located at TSOC, Known Shipper, Registered Traveler, Documentum Upgrade, US Visit Air Exit, and Fingerprints & Lems. The Contractor shall support utility items as they exist currently in the TOP and ACS environments.

C.4.7.3 Email Services

The Contractor shall provide Email to ITMS users. The Contractor shall ensure the Exchange Server maintains an operational status in compliance with the appropriate SLA(s), Section J, Attachment 5. The Contractor shall manage the mailbox space within the server. The Contractor shall ensure the service is maintained and scheduled maintenance is not performed during business hours. The Contractor shall coordinate all such scheduled maintenance with authorized ITMS TSA officials.

Five CLINs have been created to comply with the Government's request for Classified "Spillage: Email Message Support services. These are summarized as follows:

1. Infrastructure Spillage Hardware & Software Environment
2. Classified Spillage Email Support for 1-25 Active Accounts
3. Classified Spillage Email Support for 26-50 Active Accounts
4. Classified Spillage Email Support for 51-100 Active Accounts
5. Classified Spillage Email Support for Restoring from Tape of 1-5 Active Accounts

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 79
-----------------	------------------------------------	--	--------------

The Infrastructure Spillage Hardware & Software Environment CLIN represents hardware and software for the establishment of a non-production or private environment which investigation by Government Security will be conducted concerning a security incident that has occurred for 1 to 5 active email accounts on a specific day. The Classified Spillage Email Support for Restoring from Tape of 1-5 Active Accounts CLIN is dependent on the Infrastructure Spillage Hardware & Software Environment CLIN being ordered and implemented. The remaining three CLINs, Classified Spillage Email Support for 1-25 Active Accounts 1-25, 26-50 and 51-100 provide services for the deletion of a single inappropriate / classified message within the specified range number of active email accounts in a Microsoft Exchange environment, but limited to data store, in the event of a classified "spillage". The Government requires that this support only provides for "deletion only" for an inappropriate / classified email message regardless of level of security classification.

C.4.7.4 Internet Services

The Contractor shall provide internet access over the LAN/WAN. The Contractor shall ensure security firewalls are in place such that the integrity of the system and the data are maintained with web content filtering. The Contractor shall continue current operating level. The Contractor shall support a service equivalent to approximately 25Mps of TSA internet traffic flowing through the hosting center.

C.4.7.5 Intranet Services

The Contractor shall provide Intranet Services for all TSA authorized users.

C.4.7.6 Extranet Services

The Contractor shall provide extranet services and interfaces necessary to communicate with external law enforcement/intelligence, affiliated Government, industry partners, and public community organizations through secure Internet connections in accordance with TSA approved standards. Communications between the following parties, as a minimum, includes: DHS, FAA, DOT, FBI, CIA, NSA, Airlines and shipping companies.

C.4.7.7 Proxy Services

The Contractor shall provide Proxy Services and address translation services to enable TSA personnel access to the internet on a per user basis to include:

- 1) Update of security attributes
- 2) Backup of configuration logs
- 3) Report usage
- 4) Web content filtering

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 80
-----------------	------------------------------------	--	--------------

C.4.7.8 Satellite Communications

The Contractor shall provide satellite communications as a future requirement as defined in the ordering process (see Section G.10). The Contractor shall provide commercial satellite communications that will meet mobile CONUS and OCONUS requirements, if requested by the Government. The proposed solution shall provide equipment that is portable in size and weight providing comfort and convenience to all users.

The Contractor shall provide these services at the request of the Government in accordance with the procedures outlined in Section G.

C.4.7.9 Service Provisioning

The Contractor shall provide support to include, at a minimum, the following: ITMS-WOS PC/LAN/WAN Services; Wireless Services; and POTS/Telecom Services. The objective of this CLIN is to provide day-to-day support for the TSA staff to encompass the management of existing/new equipment and services for voice and data seat services, communication services and network services used at TSA Headquarters, FSD locations, airports, and other TSA locations worldwide. The range of equipment and services may include, at a minimum, office automation equipment, personal computers, desktop voice and data, virtual private networks (VPNs), land mobile radio (LMR), LANs/WANs, cellular voice/data, wireless devices, PDAs and pagers. The Contractor shall provide day-to-day support for the TSA staff in managing of existing service and acquiring /new equipment and services for voice and data seat services, communication services, and network services used at TSA Headquarters, FSD locations, airports, and other TSA locations worldwide. The range of equipment and services shall include, but is not limited to: office automation equipment, personal computers, desktop voice and data, virtual private networks (VPNs), land mobile radio, LANs/WANs, cellular voice/data, wireless devices, PDAs, and pagers. The service provisioning support shall include, at a minimum: ITMS-WOS PC/LAN/WAN Services; Wireless Services; and POTS/Telecom Services.

The following is representative of the typical range of duties but not necessarily all-inclusive of the support the Contractor shall provide:

- Receive, process and submit "draft" service orders for subsequent TSA authorization to the appropriate service provider, e.g., ITMS-WOS, ITMS-FedCell, GSA-FTS, NCS-GETS, NCS-TSP, etc.
- Service Orders may encompass full SDLC/life-cycle processes from initiation through disposition phase for both product and labor services.
- Service provisioning will apply to both CONUS and OCONUS TSA users.
- Coordinate authorized user requirements with service provider(s) as necessary to meet ordering-installation due dates.
- Assist end-users with ordering/authorization procedures and service status/availability inquiries as required.
- Interface with TSA oversight/program managers and end-users as necessary to install/remove/relocate/convert telecommunication services at TSA Aviation Operations (AVOP) field locations, TSA Headquarters and other authorized TSA locations. Telecom services include both switched/ non-switched wireline and wireless services for satellite TV, cable TV, telephone, DSL, internet service and digital data circuits.
- Provide TSA with research and documentation support on all FAA telecom circuit reconciliations and cancellations.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 81
-----------------	---	---	---------------------

- Assist TSA with technical research and recommendations in response to user inquiries regarding service enhancements, additions and processes.
- Assist TSA with implementation, management, and support for Continuity of Operations (COOP) and Government Emergency Telecommunication Service (GETS) Cards/MCI WorldCom Calling cards for domestic and international access.
- Provide management and response to service requests submitted to TSA Equipment mailbox(es) for the Headquarters IT POCs for issuance, status, and information as needed concerning the request. Initiate internal trouble tickets for various departments within TSA to ensure install, move, add, and changes (IMACs) are processed in a timely manner. Develop necessary policies and procedures as appropriate.
- Assist TSA with ensuring payments of outstanding debts and balances incurred prior to transfer of telecom services from FAA to TSA. Coordinate the review and reconciliation of TSA billing invoices and orders using automated electronic billing system and hard copy files. Develop analytical reports outlining monthly I.T. service allocations and expenditures for review by senior management officials within TSA – OIT.
- Assist TSA with ITMS – WOS order-entry training for new Service Provisioning staff as requested.
- Provide Service Provisioning support coverage for core business hours of Monday through Friday, 8:00a.m. to 5:00p.m.

C.4.8 Data Center Operations Management

The Contractor shall manage the TSA production server environments. Currently, TSA utilizes production server environments in St. Louis, MO and in Arlington, VA. The Contractor shall:

- 1) Coordinate with hardware and maintenance vendors as required.
- 2) Coordinate with facility related maintenance work to maintain optimal continuity.
- 3) Support TSA and it's subContractors in accomplishing its mission.
- 4) Perform periodic checks/walkthroughs on the infrastructure equipment to ensure that operational status is within manufacturer's specifications.
- 5) Ensure that any planned equipment installations will not adversely affect the operation of the existing equipment.
- 6) Maintain the load balancing of the critical loads and distribution equipment to ensure that the installation provides power without overloading cables or equipment.
- 7) Serve as the primary contact regarding any emergency situations that may arise within the data center.
- 8) Maintain familiarization with OSHA regulations that would pertain to data center operation.
- 9) Continually review systems and infrastructure to ensure compliance with configuration controls and enterprise architecture.

The Contractor shall provide a Systems Management Center (SMC) with qualified technical subject matter personnel for TSA Headquarters facility in Arlington, VA, that will operate 7x24x365 in support of TSA's critical server production processing environments. The Contractor's SMC shall provide real-

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 82
-----------------	------------------------------------	--	--------------

time services as indicated in Section C.4.8.6. The SMC shall provide account management and operational services required to provide day-to-day distributed processing services from a centralized environment(s)."

C.4.8.1 Maintenance Records

The Contractor shall maintain and provide maintenance records for all Contractor supported equipment, See C.4.3.8.

C.4.8.2 Audits

The Contractor shall conduct audits of all the systems on a quarterly basis. The Contractor shall provide the Government with a working product audit report within fifteen (15) days at the end of each quarter.

C.4.8.3 Data Center Disaster Recovery

The Contractor shall create a draft TSA Disaster Recovery plan within 90 days of contract award. A final TSA Disaster Recovery Plan shall be delivered to the Government within 180 days of contract award. Within 30 days of the Government's acceptance of the final Disaster Recovery Plan the Contractor shall provide cost and technical proposals to include a WBS, implementation plan, test and acceptance plan for implementation of TSA's Disaster Recovery plan.

The Disaster Recovery plan shall focus on the restoration of services in the event of catastrophic failure of TSA HQ 6th floor data center and the Hosting Center. The plan must include restoration of all hosted systems and applications, as prioritized by the Government. The Contractor shall archive all Government data at off site locations apart from the TSA HQ and the Hosting Center. The Contractor must demonstrate to the Government that the Disaster Recovery plan is implementable in conjunction with the Contingency Plan (Section C.4.3.13) and Continuity of Operations exercises on an annual basis or as otherwise directed.

C.4.8.3.1 COOP – Continuity of Operations

The Contractor shall plan for ITMS Continuity of Operations. The Contractor shall work with the TSA Office of the CIO and TSA Office of Emergency Preparedness in providing all necessary IT services for continued operation of the TSA facilities as documented in TSA's Office of Emergency Preparedness "TSA Headquarters Plan – Assistant Administrator for Information Technology / Chief Information Officer and Information Technology and Provisioning Support."

The Contractor shall develop an ITMS COOP plan that documents the Contractor's roles and responsibilities as they apply to ITMS COOP operations. The Contractors must demonstrate their ability to compliment and facilitate Government activities in the event of a COOP activation or exercise.

The Contractor's COOP plan must be delivered to the Government within 120 days of contact award.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 83
-----------------	------------------------------------	--	--------------

C.4.8.4 Operations Process and Planning

The Contractor shall assess all PMO projects to ensure seamless integration with the current production infrastructure. The Contractor shall coordinate with all Lines of Business to ensure all business requirements are met. The Contractor shall escalate issues that may impact the program. The Contractor shall be proactive with TSA users to resolve the problems which arise from the daily operations and to work with them on opportunities for systems improvement.

C.4.8.5 Operations Support

The Contractor shall manage the TSA server production environments and equipment. The Contractor shall provide 24x7 coverage. The Contractor shall provide a single screen view of the TSA production environment's overall health. The Government does not anticipate an increase in the core enterprise systems; however, growth in high speed circuits and refresh enterprise support system is anticipated which may affect the size of SAN storage and backup.

The Contractor shall use the current level of data (6.6TB) being backed up in the Windows environment at the hosting center. No growth of data volume has been projected in the evaluation quantities. The Contractor shall continue current operating level for tape backup and recovery. The Contractor shall base sizing estimates at the current level of data (6.6TB) for Window environment and for the Unix environment being backed up in the TOP environment at the hosting center. No growth of data volume has been projected in the evaluation quantities.

The Contractor shall perform all tasks required to deliver daily production support of all applications, as identified in Section J, and perform Database Management functions. This includes supporting the Contractor managed COTS software. The Operations and Support (System Administration) shall include:

- 1) **Production Environment Management** – the Contractor shall manage the change control requests for production systems, migrate changes of all new releases of enterprise application software into production and maintain version control of the software.
- 2) **System Monitoring** – The Contractor shall monitor and analyze system parameters and interpret System monitoring, as identified in Section C.4.3.7.5 Monitoring and Data Collection.
- 3) **General Backup and Recovery** – Ensure that backup/recovery of Contractor server installed enterprise application software, user files, and datasets are done correctly; write backup/restore procedures/scripts as needed. This will include interfacing with backup software and the tape backup system.
- 4) **Maintain system software** – Install new releases and patches.
- 5) **Problem Resolution** – Diagnose and resolve problems related to the server and Contractor managed COTS software. The activity may include interfacing with users, application developers, and NT systems administrators to resolve bugs and error messages.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 84
-----------------	------------------------------------	--	--------------

The Contractor shall also provide other operations support and system administrative functions as follows:

- 1) Integrate and test Contractor managed TSA application related software with other Contractor managed packages on servers.
- 2) Write and implement server scripts if needed for such things as backup, cron jobs, product outputs or any other function.
- 3) Define printers needed for server output.
- 4) Develop and maintain interface software for file transfer to other agencies.
- 5) Interface with front-end (first line of contact); Help Desk/Hotlines, NOC and other support groups; coordinate applicable activities with hardware and software maintenance contract personnel.
- 6) Ensure that the operating system and systems software in production are at a supportable release; assist with testing of new releases of the systems software with the application and operating systems personnel.
- 7) Maintain current versions on the TSA operating platform, standard office automation services, and other services approved by the Government.
- 8) Allocate disk space and reformat disk space as needed to ensure optimum performance of the application.
- 9) Provide operator training and/or documentation for any production scripts, and establish/maintain a CD-ROM library of installed software.
- 10) Maintain and document installation information, trouble shooting techniques, problems encountered, configurations information and default settings.
- 11) Make recommendations for new servers and hardware to existing servers which will increase performance and uptime. Recommend new hardware and solutions as they become available for technology refresh.
- 12) Evaluate the solutions with relation to infrastructure production environment.
- 13) Maintain/document information, such as production configuration, default settings and installation information, trouble shooting performed, problems encountered, etc.

C.4.8.6 Server Management

The Contractor shall provide Server Management support services including:

- 1) Deployment
- 2) Image and Certification
- 3) Installation
- 4) Warranty

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 85
-----------------	------------------------------------	--	--------------

- 5) Asset Management Services
- 6) Single Point of Contact (SPOC)/Help Desk Services
- 7) Remote Network Management
- 8) Infrastructure Maintenance
- 9) Security
- 10) Systems Management Services
- 11) Service Delivery Management
- 12) System Software Support
- 13) Problem and Change Management
- 14) Capacity Management
- 15) Operations Support
- 16) Database Management

The Contractor's server management service shall include the following activities:

- 1) Problem Management;
- 2) Directory Services Management (Active Directory & LDAP);
- 3) User/Group Account Administration;
- 4) File Server Administration and Management;
- 5) Print Server Administration and Management;
- 6) Network Print Server Device Administration and Management;
- 7) Virtual Private Network (VPN) Server Support;
- 8) DNS/WINS Administration and Management;
- 9) Messaging Administration and Management (Microsoft Exchange);
- 10) Blackberry Server Administration and Management;
- 11) Trouble Management (Server);
- 12) Interactive Intelligence Information (I3) Server Support;
- 13) Outlook Web Access (OWA) Administration and Management;
- 14) Threat Management and Intrusion Detection Server Support;
- 15) Internet/Intranet/Extranet Administration and Management;
- 16) Proxy Services;
- 17) Server Performance Management;
- 18) Human Resource Management and Administration;
- 19) Configuration Management (Documentation);
- 20) Backup, Restore, and Tape Archive Management; Server Release Management;
- 21) Storage Management
- 22) Data Center Management;
- 23) Operations Support;
- 24) Tape Operations;
- 25) Server System Management ODCs.

C.4.8.7 Storage Management

The Contractor shall provide management of TSA's Storage Area Network (SAN) environments.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 86
-----------------	------------------------------------	--	--------------

C.4.8.8 Database Management

The Contractor shall provide data base management services. Database management services shall include security, integrity, privacy, backup, recovery, tracking, control monitoring and reporting. Through database management, the Contractor shall ensure optimal performance.

TSA understands that a database may be perfectly tuned, but the application using the database may still perform at unacceptable levels because of the application. The Contractor, at a minimum, shall still assist in an effort to achieve sustained performance of an application through monitoring, measuring, and tuning the database parameters to reduce bottlenecks. In addition, the Contractor shall be responsible for problem resolution and daily maintenance of AMSS Managed Applications and appropriate infrastructure.

The Contractor shall provide logical and physical database support. The Contractor shall provide problem resolution and daily maintenance. For Unisys developed application features and functional capabilities delivered under the Bridge Contract the Contractor shall maintain data dictionaries according to approved TSA standards, data tables and system's models. Database management services shall include, at a minimum:

- 1) Participation in future database design process and database schema.
- 2) Providing guidance and support to application developers to improve application performance, debug application problems, and providing guidance on database security.
- 3) Maintaining all production replication server databases.

C.4.8.9 Backup and Recovery

The Contractor shall provide backup and recovery services throughout the life of the contract for Contractor managed server systems. The Contractor shall identify policies and procedures in a Backup and Recovery Plan. The Contractor shall backup data and server system hard drives for Contractor managed server systems and data. The Contractor shall validate the integrity of the back up copies and provide security of server system backups. The Contractor shall back up server data on a nightly basis. The Contractor shall maintain records on backup and recovery server data and provide reporting to the Government. The Contractor shall provide a plan in 60 days for server data storage backup that is consistent with the federal NIST guidelines and requirements.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 87
-----------------	------------------------------------	--	--------------

C.4.8.10 Tape Operations

The Contractor shall provide tape operation services. The Contractor shall maintain the TSA tape library. The Contractor shall monitor and maintain tape media to provide clean, certified media. The Contractor shall provide the Tape Operations consumables to include tape media and bar code labels. The Contractor shall manage the shipment of tapes to an off site storage facility and conduct annual verification of tape backup inventories. Retention of the media should be consistent with the Backup and Recovery Plan referenced in Section C.4.8.9 Backup and Recovery.

C.4.8.11 Participation on Boards

In the capacity as Security Advisor, the Contractor shall participate in other ITMS and TSA boards to include, at a minimum, the System Configuration Control Board.

C.4.8.12 Network Security Operations

The Contractor shall provide enterprise security operations. The Contractor shall provide oversight and operational support on a daily basis. The Contractor shall maintain the integrity of the security across the enterprise and closely coordinate with other security personnel. The Contractor shall provide security reviews of changes to COTS hardware and software. The Contractor shall monitor SOC security and identify breaches and incidents. In the event of a security compromise, the Contractor shall report on the identification and resolution and what steps are to be taken to ensure such breach does not occur again. Scans and tests shall be conducted by the SOC as directed by the TSA IT Security MD 1400.3 Policy Handbook. The pre-deployment scans shall be limited to each individual device build or configured as ordered by task or delivery order. The Contractor shall conduct only one scan when multiple devices of identical builds or configurations are deployed. Monthly scan reports shall be stored on a report sever for retrieval by approved personnel. Monthly Scans shall be conducted over a period of weeks based on the duration necessary to complete the scan. The Contractor staff responsible for threat identification shall monitor a maximum of 10 external threat report sources (assumption does not specify per week, per month, or per year), review up to 5 related change requests per week and review up to 2 risk assessments per week.

The Contractor shall be responsible for the management, administration, maintenance and configuration of an anti-spam solution. This shall include any Government authorized changes in configuration in accordance with the TSA Information Technology Security Office (ITSO).

The Contractor shall be responsible for vulnerability scanning on a monthly basis for all managed devices in the environment. The scope of the Monthly Vulnerability Scans shall include every managed and networked device in the ITMS Bridge infrastructure with an IP address accessible and responsive to the scanning consoles. The results of these scans shall be analyzed for duplicates and reports will be provided monthly. The Contractor shall work with TSA to identify items of concern that should be addressed and shall track these efforts to remediation. In addition the Contractor shall identify non-responsive possibly non-managed devices in the environment. The Contractor shall track these devices as a threat to, at minimum, the stability of the environment. The Contractor shall work with TSA to determine appropriate corrective action. The Contractor shall provide security services monitoring of security logs shall include but shall not be limited to: NIDS, HIDS, firewalls, server event logs, e-mail AV, system AV, spyware, and proxy. This service shall include, but is not limited to, correlation of alerts between the security devices listed above. Upon detection of security events,

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 88
-----------------	------------------------------------	--	--------------

centralized security personnel shall evaluate the event, prioritize it, and inform the Computer Security Incident Response Center (CSIRC) about critical situations for elevation to TSA.

C.4.8.13 Security Audits/Audit Log

The Contractor shall support periodic security audits conducted by TSA. Government sponsored audits may include all TSA managed system user accounts. The Government retains the authority to determine the selection of a specific operating system. Raw data of the audit and any associated reports will be made available to the Government upon request. The Contractor shall assist by setting up the auditing environment and running through simulations and activities directed by the lead for the Security Audit. The Contractor shall maintain a log of each audit. The Contractor shall coordinate auditing efforts with TSA staff and, where appropriate, incorporate Government methodologies.

C.4.8.14 Network Intrusion Devices/Host Intrusion Devices

The Contractor shall provide both NIDs and HIDs for monitoring the operational environment as directed by TSA.

Host based intrusion detection shall include, at minimum, HIDS Management/Monitoring and supporting 25 HIDS Policies. NIDS service shall include, at minimum, the Management and Monitoring of different manufacturers in order to provide Defense-in-Depth.

C.4.8.15 Firewall support

The Contractor shall provide firewall support. The Contractor shall provide firewall support for web hosting, data centers, and networks.

Firewall service shall include, at minimum, the Management and Monitoring of 38 devices including:

- 1) Cisco PIX Firewalls – 32 Total (12 HA Pairs / 9 Standalone);
- 2) Cyberguard Firewall – 1 High-Availability Pair (HA); and
- 3) Sidewinder Firewall – 2 High-Availability Pairs (HA).

C.4.9 Infrastructure Engineering

The Contractor shall provide infrastructure engineering to include the LAN, WAN, Data Center, HQ and remote site operational environments. The Contractor shall plan, design, and develop current and future operational IT infrastructure solutions in accordance with the SDLC. The Contractor shall coordinate infrastructure engineering efforts with the OCIO's office to ensure that infrastructure engineering meets the TSA and DHS enterprise architecture and common solutions engineering designs. The Government and the Contractor shall mutually agree on requests for engineering based on complexity, priority, time, and effort required and shall balance the Government's right to timely response with the Contractor's limited resources and fixed costs under this contract.

TSA Architecture

The services described herein apply only to equipment and users connected to the TSA NETWORK domain. The Contractor shall provide "Legacy" users and systems in the TSA domain with the same

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 89
-----------------	------------------------------------	--	--------------

levels of service that they receive in the ITMS contract and/or the same levels of service that they are currently receiving.

Data Items

The Contractor shall deliver data items per the agreed schedule. Examples of data items include: engineering schematics, network architecture drawings, IP configuration tables. Data items shall be provided via softcopy with additional hard copies as requested. The engineering diagrams and associated underlying data shall be made available to the Government via a shared drive, per Section C.4.14. The Contractor shall provide updated network drawings within 30 days of award. Requests for unscheduled items and data calls will be accommodated when requiring minimal effort. Requests for complex items shall be negotiated for priority, time and effort required and shall balance the Government's right to accurate and timely information with the Contractor's limited resources and fixed costs under this contract.

Interoperability

The Contractor shall understand that the Government is faced with periodic demands to integrate their technologies with other external organizations' support systems. The Contractor shall fully cooperate with these efforts within the given resources, by providing data items and attending meetings as requested by the Government and dependent upon available resources. The Contractor shall respond to specific requirements ordered via the ordering process (see Section G.10).

Electronic Surveillance System

The Contractor shall provide ongoing engineering support for the Electronic Surveillance Systems currently implemented at 8 airports.

802.1X

TSA will furnish hardware and software upgrades required to enable 802.1X at the appropriate time in the implementation schedule.

Wireless

Wireless technology will be implemented on a limited basis at TSA locations when wired infrastructure is deemed not cost effective. The Contractor shall provide infrastructure engineering support for the development, design and implementation of wireless solutions.

Workstation Configurations

The Government plans one refresh of the Dell laptop and Dell desktop models during the base period of the contract, however, additional configuration changes may be required based on OEM model availability. The Government and Contractor shall mutually agree on future hardware or software configuration changes to desktop and laptop systems. The current OEM (Dell) shall remain the standard. Images for these new configurations shall be completed on a quarterly basis or as agreed.

DHS ADEX

Any integrated DHS ADEX design, development and implementation will be performed as a future delivery or task order. The Contractor shall attend discussions and provide data items for this effort as described above.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 90
-----------------	------------------------------------	--	--------------

Server Image

No refresh of the Dell servers (beyond the 1850, 2850 and 6850) is planned during the base period of the contract, however, additional changes may be required based on OEM model availability.

TSA Infrastructure

The Government shall order types and makes of equipment that meet the following standardization requirements or as agreed to by both parties for specific projects:

- Desktops/Laptops: Dell
- Wintel Servers: Dell, Unisys
- Unix Servers: Sun
- Linux Servers: Unisys
- Network Routers: Cisco
- LAN Switches: Cisco
- Printers: Lexmark, Hewlett Packard or Unisys
- Firewalls: Cisco, Securer Computing or Cyberguard

The Contractor shall provide engineering support and implement upgrades to Microsoft Windows Server 2003 and AD/Exchange/OWA 2003 in the Production environment. This upgrade may include additional GFE hardware and GFE software to replace some or all of the Active Directory, Exchange and Outlook Web Access (OWA) servers. In the event that Microsoft releases a new Server Operating System and the Government desires to implement the upgrade, the Government will order the implementation via a future delivery or task order..

OS Support – Unix

Unix support is limited to the existing Sun Solaris environment. TSA does not anticipate any major expansion of, or technical refresh of, the existing Sun Solaris environment.

C.4.9.1 Tier III support

The Government requires Tier III support (i.e., engineering/fix support for issues that cannot be fixed at Tier 0/I or Tier II support levels) that is comprised of engineering technical specialists who will resolve complex technical problems. There shall be a sufficient staff of individuals assigned to the TSA Engineering Support Team with the primary functions described below:

- 1) Document existing infrastructure/operational systems.
- 2) Solve complex, high impact design/development/support problems, deploy TSA approved contract solutions.
- 3) Provide quality improvements and root-cause analysis.
- 4) Produce documentation and communication of user requirements for new systems and additional IT support to Engineering Support Team management.
- 5) Analyze requirements, develop test data, scripts and test cases, execute testing, analyze and document test results.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 91
-----------------	------------------------------------	--	--------------

- 6) Trouble-shoot, maintain, and install approved upgrades.
- 7) Analyze the existing network and recommend solutions.
- 8) Ensure and coordinate the timely handoff of engineering specific requirements.
- 9) Cooperate and coordinate with external vendors and organizations to solve complex interface issues.

C.4.9.2 Software Upgrades/Patch Implementation

Upon notification by OEM or other official source, the Contractor shall provide the following levels of service for software upgrades and software patch management as defined below:

- 1) The Contractor shall test and provide an impact analysis within 48 hours of Contractor receipt/notification of availability from the OEM or other alert source, on software patches that repair security vulnerabilities assessed as critical and/or restore critical system to full functionality. Upon approval of the test and impact analysis by the Government, the Contractor shall immediately begin implementation of the patch/update following an agreed to prioritization and schedule. This applies to the following:
 - a) Microsoft Software
 - b) Cisco Networking Equipment
 - c) Symantec Software
- 2) The Contractor shall test and implement within 45 days of release, all patches, bug-fixes, service packs that provide extra protection, provide additional functionality or that are classified as important by the OEM vendor. The Contractor shall provide the Government with the ability to view port usage along with source destination networks. The Contractor shall submit a System Software Upgrade implementation plan to the Government for approval.
- 3) The Contractor shall test and implement within 180 days of release, any major system software upgrade. The Contractor shall submit a System Software Upgrade implementation plan to the Government for approval.
- 4) The Contractor shall perform an impact analysis of the TOP and ACS critical patches within 48 hours of release by a third party vendor.
- 5) The Contractor shall be responsible for version changes and upgrades into ITE and production environment. Version upgrades are infrastructure upgrades only and do not include major vendor version changes such as from Oracle 9.x to Oracle 10.x.

(Where did this come from) The Contractor shall perform the following functions as they relate to the test and implementation of required critical software patches that repair security vulnerabilities and/or allow the intended system to full functionality by the OEM: The Contractor shall perform an impact analysis of Critical Patches within 48 hours. However, there is recognition that there shall be a requirement for some critical security patches that must be installed within 48 hours. Under normal conditions the Contractor shall coordinate with Security and other appropriate Unisys and TSA personnel. The Contractor shall support builds in the ITE environment, testing efforts, TSA Review Boards, and promotion to production. The Contractor shall support upgrades based upon mutual agreement within mutually agreed upon timeframes. Testing for infrastructure patching, service pack or upgrades shall be accomplished by the Contractor's engineering team at the Reston lab. Once testing is completed, a Request for Change (RFC) shall be completed and submitted through change management along with documented test results and risk assessment on the impact on the production environment and users. The Contractor's Production Service functional area lead shall review and make recommendations for consideration by the UOCM and SSCB. Once the test results and risk assessment recommendations are reviewed by UOCM and SSCB, those organizations shall

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 92
-----------------	------------------------------------	--	--------------

determine whether the infrastructure patch, service pack or upgrade is deployed into the production environment.

C.4.9.3 Internet Protocol Telephony (IPT)

The Contractor shall provide Internet Protocol Telephony (IPT), Voice over Internet Protocol (VoIP) services, on a "seat" basis and shall include instruments, services and cabling with bundled services/features as ordered.

The VoIP service characteristics and requirements are as follows:

- 1) The particular Internet Protocol Telephony (IPT) solution selected by the Contractor is Voice over Internet Protocol (VoIP). This solution relies on the TSA network and encompasses an in-house implementation consisting primarily of call routing servers, voicemail and site survival telephony.
- 2) The solution is centrally located for sites under 200 users and provides 2 tiers of redundancy should the TSA network become unavailable. Local services are leveraged to provide local numbers and provide access to basic inbound and outbound calling when access to the TSA network is not available.
- 3) The end user device is an intelligent phone capable of providing XML web pages through specific web based telephony phone services.
- 4) The VoIP solution is considered an application and makes the technical assumption that the following network items are available:
 - a. Wide area network with quality of service
 - b. Gatekeeper functionality for bandwidth management
 - c. Required security zones
 - d. Local area network with quality of service
 - e. Data center infrastructure required for servers
 - f. DC inline local network station delivery point for a VoIP phone
 - g. Local data cabling
- 5) Managed Services include:
 - a. A basic Cisco IP phone
 - b. Unit license
 - c. Logistics and outbound freight charges
 - d. Deployment
 - e. Asset management
 - f. 7x24 Single Point of Contact/ help desk
 - g. Infrastructure maintenance (break/fix, warranty, sparring)
 - h. Service delivery management

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 93
-----------------	------------------------------------	--	--------------

6) Conference VoIP Phone

- a. Definition: 360-degree room coverage VoIP Conference Phone that offers superior voice and microphone quality, with simplified wiring and administrative cost benefits which are derived when converging voice, video, and data across a common IP infrastructure. The IP Conference Station voice instrument is a full-featured, IP-based, full-duplex hands-free conference station
 - b. Logistics and outbound freight charges are included
 - c. Deployment
 - d. Asset management
 - e. 7x24 Single Point of Contact/ help desk
 - f. Infrastructure maintenance (break/fix, warranty, sparring)
 - g. Service delivery management
- 7) Ability to place and receive calls
 - 8) Hold
 - 9) Transfer
 - 10) 3-way conferencing
 - 11) Voice mail (VM) (set on/off by phone number)
 - 12) Redial last number
 - 13) Call forward
 - 14) Ability to have calls ring on a group of phones at one time
 - 15) Ability to have an assistant answer calls for an executive (before VM)
 - 16) Ability to display busy status on a button
 - 17) Ability to have rollover/hunt groups
 - 18) Ability to do fixed call forward busy and call forward no-answer
 - 19) Ability to have ring-down (auto-dial) service on a button
 - 20) Ability to have hot-line service (auto-dial on pick up)
 - 21) Ability to support analog lines for FAX, secure phones and modems
 - 22) Integrated directory service (corporate directory)
 - 23) Synchronized (NTP) date/time display on phones with screens
 - 24) Ability to support no-ring/no incoming calls
 - 25) Ability to suppress phone number display in public areas if requested
 - 26) Prevention of additional toll calls such as "976" "001" without a PIN number or other method of approval.

Call Manager Clusters

- 1) Call Manager cluster voice service provides for Call Manager clusters containing one publisher, one TFTP server, and two subscribers supporting up to 5,000 VoIP terminals. The Call Manager cluster provides the necessary phone functions such as dial plans, route patterns, call transfer, etc.
- 2) Intrusion Detection
- 3) IDS at the call manager
- 4) Voice Mail Server

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 94
-----------------	------------------------------------	--	--------------

C.4.10 Testing

The Contractor shall conduct testing in accordance with the SDLC for all new software, upgrades, patches, and hardware. The Contractor shall document testing in a Test and Evaluation Master Plan (TEMP). The Contractor shall simulate the production environment for testing in an Integration Test facility, and shall document all test findings and results in test reports consistent with the SDLC.

The testing services shall incorporate the following:

- 1) Provide seamless integration of new and revised products with the production environment.
- 2) Conduct testing on planned hardware and/or software installations to avoid adversely affecting the operation of the existing environment.
- 3) Conduct standardization of testing procedures.
- 4) Conduct acceptance testing and inspection for systems to be implemented into production for configuration compliance.
- 5) Provide a test lab environment with established policies and procedures that support all project personnel including third-party vendors throughout the systems development life cycle. This shall result in a higher quality product and reduce overall cost of development.
- 6) Establish and support lab environments that simulate the TSA Operating Platform (TOP). The lab environments proposed include support for network component integration testing, application development, development integration testing which includes subsystem testing, system testing, security testing, acceptance testing, and product/service acceptance testing.
- 7) Provide patch testing results, including a technical impact analysis, for critical Windows Server, network infrastructure (refer to the ODC and Travel requirements attachment listed in Section J), and Windows client patches for devices managed under ITMS.
- 8) Provide TSA with a recommendation on critical patch implementation to include potential functional impact in the environment.
- 9) The Contractor test for applications identified in Section J shall be limited to the following iterations:
 - a) Feature functionality integration testing shall be limited to four (4) build and test cycles;
 - b) User acceptance testing shall be limited to one (1) execution of the test;
 - c) Production validation testing shall be limited to one (1) execution of the test; and
 - d) Performance testing shall be limited to execution of three (3) performance test cycles;
 - e) If additional test iterations are requested, funding shall be provided within a project future delivery or task order.

The Contractor shall provide TSA with a soft copy of testing documentation in a Microsoft Word document format. The documents shall be stored in a central electronic repository in a location agreed to and accessible by TSA. TSA may choose to have the deliverable also sent to an e-mail address. If requested, the Contractor shall be required to provide a copy to a postal address that TSA will specify for project deliveries. The Contractor shall also provide a copy of the contract deliverables to TSA contracting office. TSA remains the owner of the testing documentation. For testing, the Contractor shall also refer to the ODC and Travel requirements attachment listed in Section J.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 95
-----------------	------------------------------------	--	--------------

C.4.10.1 Integration Testing

The Contractor shall conduct integration testing in accordance with the TSA SDLC for all software and hardware prior to installation in the production environment. The Contractor shall create and load the test databases and execute integration testing.

The Contractor shall conduct this testing using standard testing procedures based on mutually agreed test and evaluation master plan in a simulated production environment prior to installation in a production environment. The Contractor shall complete the integration of configuration items, create and load the test databases, and execute integration tests to ensure that the program components properly integrate. The Contractor shall provide documentation of the test findings and results consistent with the TSA SDLC. The Integration testing process and deliverables shall be evaluated using mutually agreed upon quality assurance plan by the Contractor and the Government. The Contractor shall verify the ability to build and integrate components into the delivered configuration items. The Contractor shall integrate the configuration items within a simulated production environment. The Contractor shall create and review integration test(s) cases and scripts. The Contractor shall run the integration tests. The Contractor shall document the test findings and results in a repository. The Contractor shall handle failed components based on the TSA direction consistent with the SDLC. For testing, the Contractor shall also refer to the ODC and Travel requirements attachment listed in Section J.

TSA and the Contractor shall agree to test cases after completion of development and at least 10 days in advance of the actual UAT event. The Contractor agrees to provide free unconstrained testing during the System Test portion of the SDLC.

C.4.10.2 Subsystem/System Testing

The Contractor shall conduct subsystem/system testing for all Contractor software development. The Contractor shall create/load the test database and execute system testing. If any component fails, the Contractor shall migrate it back to the development phase for rework. When a component passes, it migrates to the security testing phase.

C.4.10.3 Security Testing

Once the component passes subsystem/system testing, the Contractor shall conduct security testing. The Contractor shall create/load the test database and execute security testing. The terms and conditions and pricing of testing will be the subject of a Special Project. □

C.4.10.4 Acceptance Testing

The Contractor shall conduct acceptance testing in accordance with the TSA SDLC of all software and hardware prior to installation in the production environment. The Contractor shall conduct this testing using standard testing procedures based on a Test and Evaluation Master Plan in a simulated production environment prior to installation in a production environment. The Contractor shall create and load test databases to facilitate acceptance testing. The Contractor shall complete functional acceptance testing for correctness and satisfaction of functional requirements. The Contractor shall evaluate System interoperability, documentation, system reliability, and the level to which the system meets user requirements. The Contractor may use performance tests to ensure that performance

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 96
-----------------	------------------------------------	--	--------------

meets performance requirements documented by TSA. The Contractor shall provide documentation of the test findings and results consistent with the TSA SDLC. The testing processes shall include, as appropriate: functional acceptance and performance tests performed on an established configuration within a simulated production environment; the Contractor is responsible for creating, reviewing and verifying the functional test cases and scripts; the Contractor is responsible for running the functional acceptance tests; the Contractor is responsible for documenting in a repository all functional test findings and results; when required, the Contractor is responsible for creating, reviewing and verifying the performance test cases and scripts; when required, the Contractor is responsible for running the performance acceptance tests; when required, the Contractor is responsible for documenting in a repository all performance test findings and results; the Contractor is responsible for identifying failed components and handling them based on the TSA direction consistent with the SDLC; TSA will retain the authority for acceptance or non-acceptance of testing based on a review of the above deliverables.

The Contractor shall support user acceptance testing. The Contractor shall create/load the test database. If any component fails, the Contractor shall migrate back to the development phase for rework. When a component passes, it migrates to acceptance testing.

The Contractor shall perform product and/or service Acceptance in accordance with the TSA SDLC of all software and hardware prior to installation in the production environment. The Contractor shall perform this acceptance testing using standard testing procedures based on a test and acceptance plan. The test and acceptance plan shall detail the test procedures that are used to make sure service, operations, and management support systems that satisfy the requirements of the Performance Work Statement and service levels. The Contractor shall provide documentation of the test findings and results consistent with the TSA SDLC. The task shall support criteria listed in Section E – Inspection and Acceptance; the product and/or service test and acceptance shall be performed on an established configuration within a simulated production environment; the Contractor is responsible for creating, reviewing and verifying the test cases and scripts; the Contractor is responsible for executing the acceptance test cases and scripts; the Contractor is responsible for documenting in a repository all test findings and results; the Contractor is responsible for identifying failed components and handling them based on the TSA direction consistent with the SDLC; TSA shall retain the authority for acceptance or non-acceptance of testing based on a review of the above deliverables.

Successfully passing Acceptance Testing should trigger the start of any production applicable SLAs and/or performance metrics.

C.4.10.5 Product/Service Acceptance

The Contractor shall develop a comprehensive Test and Acceptance plan that describes the approach to service acceptance testing of all managed services and systems. The plan shall detail the test procedures that shall be used to ensure that the Contractor's service and operations and management support systems satisfy all the requirements of the Performance Work Statement and service levels.

The Contractor shall deliver, within the stated timeframes a Master Test and Acceptance Plan, which will identify the Test and Acceptance procedures for inspection and acceptance activities. During contract performance, the requirements of the Master Test and Acceptance Plan shall be applied on a case-by-case, project specific basis. The Contractor shall propose, in response to the Government's requirements, the project-specific test and acceptance procedures that are applicable to that project.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 97
-----------------	------------------------------------	--	--------------

The Government, through system develop life cycle, will accept or reject the Contractor's recommendation.

The plan shall include milestones and measures that shall be used by the Government to determine: the Contractor's ability to successfully accomplish the complete assumptions and full performance of all ITMS contract functionalities (e.g., Contract Network Operations, Helpdesk, Provisioning System, and Ticketing System—(Troubles and IMACs).

Additionally, the plan shall include inspection and test procedures/processes that shall be used as a guide for testing and accepting new equipment and services beyond the transition period. The Plan shall be delivered in accordance with the timeliness in Section F, Table F-1, Deliverables.

C.4.11 Program Management

The Contractor shall provide management, administration, planning, and scheduling for projects, products and services required by this Performance Work Statement. The Contractor shall be solely responsible for managing the work performed under this contract, supervising its personnel and subcontractors, and taking appropriate corrective measures for all performance related problems in the course of performing assigned duties.

The Contractor shall assign a Program Manager to this contract to oversee project, products, and services performed under this contract. The Program Manager shall be responsible for coordinating work performed and shall act as the central point of contact (POC) with the TSA OCIO senior leadership, Government Program Manager, COTR, and Contracting Officer and any other officers at the direction of TSA. The Contract Program Manager shall have direct accountability for the technical correctness, timeliness, and quality of project and services performed and products delivered. The Contractor shall updated and revise the existing Program-level Program Management Plan within 60 work days after contract award.

The Contractor's Program Manager shall coordinate with other ITMS vendors. The Contractor shall participate in TSA OCIO team meetings at TSA discretion.

TSA considers the PWS as Work Breakdown Structure (WBS). The PWS has been developed to be consistent with best practice to define logical work packages to the lowest level required to accomplish the work at the Government has requested.

C.4.11.1 Program Office

The Contractor shall provide a Program Office to provide general support of the management and oversight of all ITMS core managed services and project activities. The Program Office functions shall include, at a minimum:

- 1) Performance Management:
 - a) Monitor and report Contractor performance against SLAs and KPIs in accordance with the ITMS Performance Management Incentive Plan (PMIP) (Attachment 5, Section J)
 - b) Perform duties associated with Performance Management Incentive Plan (PMIP) as described in Attachment 5, Section J.
 - c) Follow the PMIP process to introduce new measures
- 2) Project Monitoring and Control:

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 98
-----------------	------------------------------------	--	--------------

- a) Assists providing the TSA Project Office in control and reporting to provide visibility, accountability, and traceability for management reviews.
- b) Monthly and Weekly Program and Project status reports.
- c) Monthly briefings to TSA Executives.
- d) Monitor, collect and control project cost, schedule, and performance data of selected project as required in the proposed SRs.
- 3) Project Documentation Support:
 - a) Support, both Projects and Unisys Contract, in providing timely and high quality deliverables and artifacts to TSA.
- 4) Quality Management:
 - a) Support validation and verification reviews conducted by TSA and IV&V Contractor
 - b) Maintain a Quality Management program at both a program and project level to include processes, procedures, metrics, and reporting to ensure increasingly effective and efficient operations,

Other Program Office functions shall include the additional Financial and Procurement oversight activities as follows:

- 1) Providing TSA Monthly Estimate to Complete (ETC) Reports
- 2) Financial Management and Reporting
- 3) Invoice Management and Reporting
- 4) CLIN Management and Reporting
- 5) Order to Invoice Management and Reporting

C.4.11.2 Progress Reports

C.4.11.2.1 Status Reports

The Contractor proposal shall report the following data elements to the TSA CO on a monthly basis:

- 1) Funds obligated by SR or Project
- 2) For each modification: date issued and amount
- 3) Work orders issued: number, date, purpose, proposed cost
- 4) A short narrative review of work accomplished during reporting period and/or significant events
- 5) Status of all ongoing program activities
- 6) Identification of problems encountered and recommended solutions
- 7) Anticipated activity for the next reporting period
- 8) Updated list of milestones scheduled

In addition to monthly written reports, the Contractor shall attend periodic status meeting and provide general updates as well as ad-hoc reports on topics such as defects, bugs, or problems and high-level documentation related to the resolution or retesting of any fixes, bugs, enhancements, setup or configuration.

C.4.11.2.2 EVMS Reporting

The EVM reporting will not be done at the Program level in any form. If TSA requests EVM reporting for a specific SR, TSA will request via the SR vehicle and the Contractor shall responds with the additional cost of adding EVM reporting to that individual SR. EVMS reporting shall be done at either the Project Summary level or the appropriate sub-level (phase or site). SRs meeting the following thresholds may be requested to report:

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 99
-----------------	------------------------------------	--	--------------

- 1) SRs that are Time and Materials, Level of Effort, and Cost-Plus Incentive based efforts are considered in scope with regards to cost reporting and earned value metrics.
- 2) Fixed Price efforts will not be required to be managed via an EVM.
- 3) Operations and Maintenance activities are beyond the scope of cost reporting, earned value metrics, and WBS requirements.
- 4) The Contractor shall provide Earned Value metrics for non-firm fixed price projects that meet the following criteria:
 - a. Acquisition Category (ACAT) 4a or above, defined as equal to or greater than \$500K of acquisition
 - b. Projects with a period of performance equal to or greater than six months
 - c. Formats 1 (Work Breakdown Structure) and 5 (Explanations and Problem Analyses) will be delivered for all EVMS projects using the OMB standard formats. Formats 2 (Organizational Categories) and 4 (Staffing) will be requested in each SR and Format 3 (Baseline) will be used when there is a change order. (The Government has no requirements in DI-MGMT-81466 beyond the submission of Formats 1 and 5. approved and base lined project schedule).
 - d. Unless otherwise directed the Contractor shall use the 50/50 rule to earn value for work packages.

EVMS Reporting Guidance will be provided by TSA in the SR request:

- 1) The Contractor shall provide a monthly report for SR/Project Summary details and/or at the second level of the WBS (Phase or Site dependent on project type)
- 2) Reports shall be based on the relevant standards found in DoD and OMB Cost/Schedule Status Report (CSSR) and CPR (the CPR is Form OMB No. 0704-0188).
- 3) If the Summary cumulative cost or schedule variance is greater than +10%, or less than -10% for an Earned value project, the Contractor shall provide variance analysis. The variance analysis shall include additional detail outlining of which next-lower-level WBS items are contributing to the variance along with a summary explanation. The Contractor shall submit a variance analysis (using the format DD Form 2734/5).

The Contractor shall submit a variance analysis (using a format similar to DD Form 2734/5) if the cumulative cost or schedule variance is greater than +10%, or less than -10%, (and also greater than \$1,000 variance). The Contractor shall provide qualitative variance analysis of which next-lower-level WBS items are contributing to the variance along with a summary explanation.

C.4.11.3 Risk Management

Risk Management at the Program level will not be required of the Contractor. The Contractor is not required to create or submit a separate program level Risk Management Plan or to produce a correlated report based on project risks. However, inherent program risks shall be incorporated during normally scheduled executive reports. The Contractor shall follow best practices in establishing Risk Management within individual SR/projects. Risk Management, at the project level, shall include but is not limited to risk identification, quantification, and ranking of all identified risks and a strategy for management of each risk. The inclusion of Risk Management Plan for each project shall be requested in the project SR and the final copy shall be provided to the COTR and/or project manager as a life cycle deliverable in both printed and electronic form.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 100
-----------------	------------------------------------	--	---------------

C.4.11.4 Issues Management

The Contractor is not required to have a correlated issue management repository or tracking based upon project risk at the Program level, nor is the Contractor required to produce a program-level Issue Management Plan. Each SR/Project shall individually account for issues and concerns that arise during execution of each task orders, specifically focused on implementation activities.

C.4.11.5 Performance Standards and Quality Assurance Plan (QAP)

The Contractor shall maintain a Quality Management Team that will focus on activities promoting improved quality and performance. These goals shall be supported by the following:

- 1) Develop, implement, and maintain Quality Assurance processes, activities, and procedures on identified and selected PMO projects.
- 2) Perform Quality Assurance Reviews (QAR) on identified and selected projects.
- 3) Perform process audits on various internal processes.
- 4) Provide recommendations on process improvement, organizational design, Change Management, and System Implementation.
- 5) Identify and document required changes for effective implementation.
- 6) Deliver a program-level Quality Assurance Plan (QAP) within 30 calendar days of award; the document will follow the TSA-supplied QASP template (see Section J)

For operational infrastructure and other security related audits, the Contractor shall make raw data of the audit available to the Government as well as any associated reports for TSA managed systems. Government sponsored audits may include all TSA managed systems user accounts at the Government's discretion. Contractor sponsored audits shall target segments of user accounts for a more in-depth review. The Contractor may use random sampling to select the audit population for the system audits and privileged accounts at the Government's discretion. The Contractor shall draw the sample from all devices on the TSA network including those devices that are not managed under the ITMS II Contractor. The sampling technique must be approved by an authorized TSA official. The Contractor may use random sampling to select the test population. The sampling technique and the scope of the audit will be reviewed by TSA. The Contractor shall perform audits against the version of TSA policy that is published at the time of audit plan formulation. The Contractor shall publish the audit findings with the TSA Office of the Chief Information Officer (CIO).

C.4.11.6 Co-Chair of Configuration Control Board and Change Management Review Board

The Contractor shall, with TSA counterparts, track and record changes to the Network and shall assist TSA in the adherence to TSA established/existing processes for managing and coordinating those changes. The Contractor, in concert with TSA, will present information packages (Request for Change (RFC) documents) to the Systems Change Control Board (SCCB), a TSA owned and governed board along which is chaired by TSA personnel.

Contract	Document No. HSTS03-06-D-CI0500	Document Title ITMS Bridge Contract	Page # 101
-----------------	------------------------------------	--	---------------

C.4.12 Project Management

The Contractor shall provide Project Management Support Services for distinct projects from core managed services that directly support end user requirement as ordered via SR process. The purpose this section of PWS is to ensure that SR/projects will be separated from managed service tasks so that work directly related to the development and deployment of projects will be included in the scope of the work (SOW) of the projects, as described in a Work Breakdown Structure (WBS), and paid for by the TSA project sponsor (Solutions Delivery, AV Ops, or others). If required, the Contractor shall define and provide justification, in the individual SR, of those projects in support of sustaining managed services, the Contractor should keep in mind that all activities associated with these projects will be included in the individual SR established for each project.

The Contractor shall provide a detail proposal for each project that is requested via the SR process. The proposal will outline the scope of work (SOW), including how the Contractor shall provide project management to the project as requested by TSA. The project management response may be part of a SOW or an additionally requested document. TSA may request in the SR that the Contractor provide a project management plan that will address as a minimum the following listed elements;

Project Planning

- The Contractor shall simplify and automate, to the greatest extent possible, project planning tools for collection, validation, and distribution of project schedules, plans/documentation and status information, including the capability to track and manage tasks and milestones. Included in the SR should be a project WBS and project schedule that will be baselined upon project approval.

Earned Value Management

For further guidance on EVM see PWS section C.4.11.2.2.

Project Scheduling

- The Contractor's shall perform project management scheduling in MS-Project and thereby providing graphic display of project scheduling and progress status. MS-Project allows for the use of PERT, Gantt, Critical Path Method (CPM), and/or other best-practice scheduling methodologies that TSA requires. At a minimum, project WBS detail shall be developed on an agreed to level that is document in the SR to facilitate budgeting and performance measurement control.

Project Profiles

- The Contractor shall provide project profile/description for each project which falls in the level 1-4a of the Capitol Planning and Control (CPIC) guidelines. This description shall be noted and agree to in the SR. The project profile shall be a concise description of the business problem the Government is requested to be addressed, the project approach, the benefits to be derived as noted by the Government, and Contractor estimated project costs and a projected project timeline.

Project Costing

- The Contractor shall, if requested in the SR, provide detailed projection of planned project costs at the agreed to project WBS level.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 102
-----------------	------------------------------------	--	---------------

Cost Tracking

- On a monthly basis, the Contractor shall, as noted in the SR, provide a detailed report of the actual and earned costs by project WBS element, in sufficient detail to track percent of planned versus percent of project completed following the EVM guidelines in ANSI/EII 748-A.

Interdependency Management

- The Contractor shall not be required to provide automated identification and management of interdependent items and variables across the program or multiple projects. This includes the capability to manage issues, resources and project/task status across multiple projects. Interdependency Management at the Program Level will be handled by TSA: TSA Schedules and resource changes in a project which impact another project shall be reflected and reported to the Contractor and the project teams in the affected project. TSA will document these subsequent changes and perform cause analysis.

Risk and Issue Management

- Project level risk and issues will be collect by the individual project and project manager. The Contractor shall not be required to provide interactive and collaborative identification, management, and disposition of issues (delays, failures, change in plan, change in specifications, etc.) across multiple projects or at the Program level. Program level Risk and Issue Management will be done by TSA

Project Schedule Baselines (Project Version Control)

- The Contractor shall provide a version control process for all project schedules that are required to be baselined. Each project shall have documented version control for each project schedule, and thereby allowing for multiple baseline reporting with in the limitations of MS-Project.

Project Reporting

- The Contractor shall provide an accurate reporting of project, phase or site, milestone status, deliverable/artifacts status and earned value if requested in the project SR.

TSA Access to Contractor Status Reports

- The Contractor shall provide project status reports to TSA for authorized distribution to TSA Project Managers, TSA project team members, TSA Directors, and TSA end-users.

C.4.13 Additional Services

Special Projects as required in accordance with the ordering process (see Section G.10).

C.4.14 Documentation

The Contractor shall maintain hardware and software documentation for the ITMS program in a repository accessible to authorized Government agents without request. The Contractor shall provide a document management system to manage version control and allow access for appropriate TSA

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 103
-----------------	------------------------------------	--	---------------

staff. All documentation exclusive of copy righted and Unisys proprietary materials, shall become the property of the Government and shall be made available electronically at no additional charge.

C.5 SPECIAL SITE REQUIREMENTS

TSA has numerous field locations that require a combination of standard service offerings and unique service requirements. The special sites with unique requirements are described as follows:

C.5.1 TSA Headquarters

Background

TSA Headquarters has over 1,900 users located at 601 and 701 South 12th Street, Arlington Virginia, 22202. TSA also has an office location located within Crystal City commonly referred to as the Crystal Park location. The users at these locations include administrative staff, middle management and Senior Executives (also know as VIPs). Support of the TSA headquarters requires that the Contractor provide management functions and technical support for the support services below. The Contractor shall provide an integrated team an integrated HQ Support Team includes personnel who provide HQ VP and on-site Tier II support.

C.5.1.1 Management

The Contractor shall provide Headquarters' management user support as follows:

- 1) Be responsible for functions of supervision of assigned shifts, including determining, and maintaining staffing levels.
- 2) Knowledge of principles and practices of enterprise infrastructure environments, including VoIP; information systems management; operating system characteristics; network architectures and principles of network integration; internet/intranet technologies; systems integration and optimization concepts.
- 3) Propose systems and practices to either lower operational costs and/or raise operational effectiveness.
- 4) Interface, as necessary, with TSA management on all issues related HQ IT Operations.

The Contractor shall provide the Government with an HQ Service Improvement team that at a minimum provides IT support to TSA Senior Executives (also know as VIPs). Tasks include but are not limited to responding to trouble reports, investigating chronic IT problems, and providing follow-up and training where appropriate. The team provides a central focus for ITMS HQ Operational entities, coordinating the efforts of the SPOC, NCC, and CIC and provides feedback and direction as necessary. The HQ Service Improvement team follows TSA required SDLC and CMMI processes. They provide trend analysis information to management so real-time and historical information regarding customer service issues shall be available for review and analysis by the TSA CIO team. The team provides a central point of contact for customer-impacting IT initiatives for TSA HQ.

In addition , the Contractor shall provide the Government with an HQ Service Improvement team that at a minimum provides support Tier II Support (C.5.1.2) to include: normal business hour support; performing installs. moves, adds and changes; resolution of complex technical problems including reconfiguration of laptops, desktops, and troubleshooting various software and hardware related

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 104
-----------------	------------------------------------	--	---------------

issues; Microsoft desktop and application configuration where necessary; network accessory maintenance; minor cable repair; analog support; network user support; Blackberry support; asset tracking; POTS management, VOIP support.

C.5.1.2 Tier II Support

The Government requires on-site Tier II support that is comprised of cleared Secret technical specialists who shall resolve complex technical problems to include the reconfiguration of laptops, desktops, and troubleshooting various software and hardware related issues. The on-site Tier II support's primary function is to perform Installs, Moves, Adds, and Changes. This team will work on-site at Headquarters' during normal business hours 7a-7p. The Headquarters Technical Support Team duties shall include the following:

- 1) Microsoft Desktop and application configuration
- 2) Network accessory maintenance (printers, file storage, CD burners, etc)
- 3) Analog technology support (fax, modems, etc)
- 4) Network user support
- 5) Performing Installs, Moves, Adds and Changes
- 6) Blackberry Support
- 7) Asset Tracking
- 8) VoIP Support

C.5.1.3 Operations

- 1) Provide on-site technical support for all end users to support trouble calls, resolution tracking and monitoring.
- 2) Provide Premium and Premier levels of service, as described in Section C.4.3.15.1, Grades of Service, and end user support for VIPs. The VIP list will be maintained by TSA and provided to the Contractor.
- 3) Perform individual assignments associated with the support, maintenance, scheduled deployment of applications on the approved software list to TSA HQ users and Install, Moves, Adds, and Changes
- 4) Act as a technical resource coordinator for IT users; determines users' needs; works with PC users to resolve problems and provide guidance to the TSA Headquarters Support Team.
- 5) Report unsafe or insecure computing practices for management's follow-up.

C.5.1.4 Monthly Progress Report Requirements

Contractor shall provide the following operational progress reports:

- 1) Written monthly status reports to the Headquarters OCIO Coordinator,
- 2) Written weekly activity reports to the Headquarters OCIO Coordinator

The status report shall be submitted on the 10th of the month following the performance of the support activities. Should the 10th of the month fall on a Saturday, Sunday or a Government Holiday, the Contractor shall submit the reports on the next business day.

The Weekly Activity Report will consist of an itemization of each ticket worked that includes, at a minimum, (HQ's)

- 1) Date and time
- 2) Individual user

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 105
-----------------	------------------------------------	--	---------------

- 3) Source of activity (SPOC/Local phone call/observation)
- 4) System malfunctioning
- 5) Short descriptor of activity
- 6) Work/fix performed
- 7) Impact to the mission

The Monthly Status Report will include: (HQ's)

- 1) Description of work accomplished during the period (the report will cover the previous month)
- 2) Status of all activities in progress
- 3) Planned activities for the upcoming period and associated schedule information, including dependencies with other activities/projects
- 4) Trouble ticket status for all tickets that were opened during a specific reporting period, including aging reports for open tickets that exceed defined closure thresholds. All VIP tickets will be identified separately in the same report. In addition, Headquarters ticket reports will not include any non-headquarters related tickets.

Monthly Asset Status Report:

The Contractor shall include in the monthly asset management report the list of Contractor supported equipment at TSA HQ. The report shall identify equipment that was recovered as part of the entry exit process that TSA will provide to the Contractor upon contract award.

Government Property—TSA will provide administrative supplies and onsite office facilities for Contractor support personnel, to include, but not limited to, a workspace, workstation, desk and phone. Dedicated TSA laptop(s) and telephone(s) will be provided for the HQ Support personnel.

Support Site Review— Due to the criticality and sensitivity of Headquarters operations, the Government intends to review Contractor qualifications prior to assignment at the Headquarters location sites.

Security Clearances—Contractor shall ensure that all assigned personnel are appropriately cleared for their designated position as stated in site specific service requirements. Contractor personnel providing operational, development or maintenance support shall possess the required clearance consistent with OCIO Policy Directive No. 2005-1, as revised.

C.5.2 TSOC

Background:

TSOC requires a variety of O&M support, including 24X7 operations support, IT operations maintenance and security support, and other related IT services within the scope of available resources. This includes operation and maintenance of existing systems and the implementation of functional enhancements and upgrades to these systems.

TSOC requires The Contractor to provide management functions and technical support for the following basic support services:

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 106
-----------------	------------------------------------	--	---------------

C.5.2.1 Management

The Contractor shall:

- 1) Manage an IT operations team for a 24 X 7 mission critical command operations center.
- 2) Manage the IT support for TSOC and related infrastructure hardware and software components. During the course of TSOC operation, certain additions and revisions to installed hardware/software components will be required.
- 3) Manage staff on a daily basis.
 - a. Provide direction to subordinates on general policies and management guidance.
 - b. Is responsible for all functions of supervision of an assigned shift, including determining and maintaining appropriate staffing levels, conducting employee performance evaluations, providing counseling, and investigation and making recommendations regarding disciplinary actions.
- 4) Knowledge of principles and practices of enterprise infrastructure environments, including VoIP; information systems management; operating system characteristics; network architectures and principles of network integration; internet/intranet technologies; systems integration and optimization concepts.
- 5) Assist with documentation and communication of user requirements for new systems and additional IT support to TSOC program management.
- 6) Responsible for planning and implementation of authorized and assigned projects. Ensure integration and successful implementation of cost effective business, infrastructure or support solutions, where success criteria include meeting cost, schedule, and performance and quality requirements for designated client personnel.
- 7) Propose systems and practices to either lower operational costs and/or raise operational effectiveness.
- 8) Administer a configuration management system for TSOC and related infrastructure systems.
- 9) Interface, as necessary, with senior level TSA/DHS management and reports on TSOC IT Operations.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 107
-----------------	------------------------------------	--	---------------

C.5.2.2 Tier II support

The Government requires on-site Tier II support that is comprised of cleared Secret technical specialists who will resolve complex technical problems to include the reconfiguration of laptops, desktops, and troubleshooting various software and hardware related issues. There will be a sufficient staff of individuals assigned to the TSA TSOC Support Team with the primary function of performing Installs, Moves, Adds and Changes. The Contractor shall provide a 24x7 on-site Operations and Maintenance Support organization for full 24x7x365 support. The Contractor shall provide cleared (secret) specialist to provide the following:: Microsoft Desktop and application configuration where necessary; network accessory maintenance; minor cable repair; analog support; network user support; performing Installs, moves, adds and changes; Blackberry support; asset tracking; POTS management; VOIP support; emergency conference room set-up as required. All TSOC personnel shall be cleared to the Secret level. This team will work on-site at the TSOC. The TSOC Technical Support Team duties will include the following:

- 1) Microsoft Desktop and application configuration
- 2) Network accessory maintenance (printers, file storage, CD burners, etc)
- 3) Minor cable repair as required
- 4) Analog technology support (fax, modems, etc)
- 5) Network user support
- 6) Performing Installs, Moves, Adds and Changes
- 7) Blackberry Support
- 8) Asset Tracking
- 9) Manage all HQ POTS dial tone
- 10) VOIP Support
- 11) IMACs
- 12) Emergency conference room setup support

C.5.2.3 Tier III support

The Government requires on-site Tier III support that is comprised of cleared Secret technical specialists who will resolve complex technical problems. The Contractor shall provide sufficient staff of cleared (secret) personnel to provide at minimum the following: documentation of existing infrastructure and operational systems; solve complex, high impact design/development/support problems. Provide quality improvements and root-cause analysis; Act as a technical resource coordinator for IT users; determines users' needs; works with PC users to resolve problems and provides guidance on a variety of hardware; Analyze requirements, develop test data, scripts and test cases, execute testing, analyze and document test results; Troubleshoot, maintain, upgrade, and provide solutions to complex voice infrastructure problems; Analyze the existing voice network and recommend solutions; Perform client consultation: Plan, design, implement and support the voice infrastructure; Sets up, configure and test Cisco Call Manager. There will be a sufficient staff of individuals assigned to the TSA TSOC Tier III Support Team with the primary functions described below:

- 1) Document existing infrastructure/operational systems.
- 2) Solve complex, high impact design/development/support problems.
- 3) Provide quality improvements and root-cause analysis.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 108
-----------------	------------------------------------	--	---------------

- 4) Assist with documentation and communication of user requirements for new systems and additional IT support to TSOC program management.
- 5) Analyze requirements, develop test data, scripts and test cases, execute testing, analyze and document test results.
- 6) Trouble-shoot, maintain, and install approved upgrades; and provide solutions to voice infrastructure problems.
- 7) Analyze the existing network and recommend solutions.
- 8) Perform client consultation; to include planning, designing and implementation in the support of the network infrastructure (refer to the ODC and Travel requirements attachment listed in Section J).
- 9) Set up, configure and test Cisco Call manager.

C.5.2.4 Operations

The Contractor shall provide operational support to the TSOC watch floor. Operational support responsibilities shall include, but shall not be limited to: assistance with the implementation, operations and maintenance of networks, servers, systems, desktops, laptops and applications; define system operations procedures and perform necessary systems operations and maintenance functions for TSOC and related infrastructure systems. Perform normal system administration and backup activities, when enabled for TSOC and related components; provide immediate end user support to watch floor personnel on a 7x24 basis as required; provide on-site technical support to support trouble calls, resolution tracking, monitoring; perform individual assignments associated with the support, maintenance, deployment of applications, and management of the information systems, products and services that support the internal operations of the TSOC; act as a technical resource coordinator for IT users; determine users' needs; work with PC users to resolve problems and provides guidance on a variety of hardware components and software programs; coordinate the installation of Commercial-off-the-Shelf (COTS) software, including the installation of new applications, upgrades and assisting users to solve software problems; coordinate the installation and configuration of specialized peripheral equipment, including troubleshooting problems with hardware and software; schedule and coordinate all Information Technology support and upgrades; coordinate the installation and maintenance of network systems hardware and related peripheral equipment; support the Federal Air Marshall's ITMS requirements; coordinate and facilitate network monitoring and management capability for TSOC and related network infrastructure components, including routers, servers and switches; troubleshoot and facilitate repairs to failures in communications connectivity/operability; create and administer network and email accounts, enabling access and utilization; provide recording and retrieval of incoming or outgoing voice calls on demand; develop and follow procedures and checklists that mirror communication support required by operational entities on the TSOC watch floor; Furnish resumes of assigned personnel to the OCIO TSOC management for review.

- 1) Provide operational support to the watch floor and administrative personnel assigned to TSOC to include:
 - Assistance with the implementation, operations and maintenance of the networks, servers, systems, desktops, laptops, and applications.
 - Define system operations procedures and perform necessary system operations and maintenance functions for TSOC and related infrastructure systems.
 - Perform normal system administration and backup activities. when enabled, for TSOC and related components.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 109
-----------------	------------------------------------	--	---------------

- 2) Provide immediate end user support to watch floor personnel 24X7. Activities performed on the watch floor in conjunction with command center operations must be timely and correct.
- 3) Provide on-site technical support to support trouble calls, resolution tracking and monitoring.
- 4) Perform individual assignments associated with the support, maintenance, deployment of applications, and management of the information systems, products and services that support the internal operations of the TSOC.
- 5) Act as a technical resource coordinator for IT users; determines users' needs; works with PC users to resolve problems and provide guidance on a variety of hardware components and software programs.
- 6) Schedule and coordinate all Information Technology support and upgrades with The Contractor to include:
 - Installation of COTS software, including the installation of new applications, upgrades and assisting users to solve software problems
- 7) Installation and configuration of specialized peripheral equipment, including troubleshooting problems with hardware/software.
- 8) Assist with installation and maintenance of network systems hardware and related peripheral equipment
- 9) Support the Federal Air Marshall's ITMS requirements.
- 10) Coordinate and facilitate network monitoring /management capability for TSOC and related network infrastructure (refer to the ODC and Travel requirements attachment listed in Section J) components, including routers, servers and switches.
- 11) Troubleshoot and facilitate repairs to failures in communications connectivity/ operability.
- 12) Create and administer network and email accounts, enabling access and utilization.
- 13) Reports unsafe or insecure computing practices for management's follow-up.
- 14) Provide recording and retrieval of incoming or outgoing voice calls on demand.
- 15) Develop and follow procedures and checklists that mirror communication support required by operational entities on the watch floor.

C.5.2.5 Monthly Progress Report Requirements

Contractor shall provide the following operational progress reports:

- 1) Oral weekly status reports,
- 2) Written monthly status reports,
- 3) Written weekly activity reports, and
- 4) Weekly timesheets to the TSOC OCIO Coordinator.

The Monthly Status Report will include:

- 1) Description of work accomplished during the period
- 2) Status of all activities in progress
- 3) Planned activities for the upcoming period and associated schedule information, including dependencies with other activities/projects
- 4) Staffing issues, include security clearance status
- 5) Updated issues register with description of problems/issues/concerns affecting the project and how they were resolved. If TSA action is required, describe proposal solutions for Government review.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 110
-----------------	------------------------------------	--	---------------

- 6) Trouble ticket status for all trouble tickets that were open for an portion of the reporting period, including aging report for open tickets that exceed defined closure thresholds

The Weekly Activity Report will consist of an itemization of each ticket worked that includes, at a minimum:

- 1) Date and time
- 2) Individual user
- 3) Source of activity (SPOC/Local phone call/observation)
- 4) System malfunctioning
- 5) Short descriptor of activity
- 6) Work/ fix performed
- 7) Impact to the mission

Monthly Funds Status Report:

The Contractor shall submit a monthly funds status report that covers the support provided under this tasking. The funds status report will be segregated by Government fiscal year and reported in a format approved by the TSOC OCIO Coordinator. The following data will be included in each report:

- 1) Identification of the most recent invoice submitted, including the date submitted, period of performance and amount invoiced.
- 2) Cumulative costs to date.
- 3) Outstanding costs (incurred, but not yet invoiced).
- 4) Estimated cost to complete (ETC) by month through the end of the performance period.
- 5) Labor details – name, labor category, and billing rate of each employee charging to the task along with associated number of hours billed in the reporting period and cumulative period.

Monthly Asset Status Report:

As a function of the asset management portion of the monthly managed services, on the 10th working day of each month, the Contractor shall submit a monthly report of all the Contractor installed hardware and software. Additionally, a weekly consumable report will be provided to the TSOC OCIO Coordinator.

C.5.2.6 Government Property

TSA will provide administrative supplies and onsite office facilities for The Contractor support personnel, to include, but not limited to, a workspace, workstation, desk and phone. Dedicated TSA laptop(s) and telephone(s) will be provided for the IT Field Support personnel. One dedicated office will be provided at the TSOC facility by TSA.

Support Staff Review—The Contractor shall furnish resumes of assigned personnel to the OCIO TSOC Coordinator for review.

Security Clearances—Contractor shall ensure that all assigned personnel are appropriately cleared for their designated position as stated in site specific service requirements. Contractor personnel providing operational, development or maintenance support will possess the required clearance consistent with OCIO Policy Directive No. 2005-1, as revised.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 111
-----------------	------------------------------------	--	---------------

C.5.2.9 TSOC Disaster Recovery

The Contractor shall create a TSA TSOC Disaster Recovery plan within 90 days of contract award. The Disaster Recovery plan shall focus on the restoration of services in the event of catastrophic failure of the TSOC facility. The plan must include restoration of all hosted systems and applications, as prioritized by the Government. The Contractor must assure that all Government archived data is stored off site from TSOC. The Contractor must demonstrate to the Government that the Disaster Recovery plan is implementable in the event of a catastrophic failure at TSOC. Contractor's Disaster Recovery plan must be reviewed and approved by the Government prior to acceptance. On an annual basis, the Contractor shall execute the Disaster Recovery plan in conjunction with TSA Continuity of Operations exercises to ensure that it restores of services.

Within 30 days of the Governments acceptance of the final TSOC Disaster Recovery plan the Contractor shall provide cost and technical proposals to include a WBS, implementation plan, test and acceptance plan for implementation of the TSOC Disaster Recovery plan.

C.5.2.9.1 TSOC COOP – Continuity of Operations

The Contractor shall plan for TSOC Continuity of Operations (COOP). The Contractor shall working with TSA Office of the CIO and TSA Office of Emergency Preparedness in providing all necessary IT services for continued operation of the TSA facilities as documented in TSA's Office of Emergency Preparedness "TSA Headquarters Plan – Assistant Administrator for Information Technology / Chief Information Officer and Information Technology and Provisioning Support."

The Contractor shall develop a TSOC COOP plan that documents the Contractor's roles and responsibilities as they apply to TSOC COOP operations. The Contractors must demonstrate their ability to compliment and facility the Government in the event of a COOP activation or exercise.

The Contractor's COOP plan must be delivered to the Government within 120 days of contact award.

The Contractor shall plan for TSOC COOP. In concert with the TSA Office of the CIO and the TSA Office of Emergency Preparedness the Contractor shall provide all necessary IT services for continued operation of the TSOC facilities consistent with the guidelines documented in TSA's Office of Emergency Preparedness TSA Headquarters Plan – Assistant Administrator for Information Technology / Chief Information Officer and Information Technology and Provisioning Support as summarized below:

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 112
-----------------	------------------------------------	--	---------------

Provides information technology (IT) and telecommunications systems support to the Transportation Incident Management Group (if activated), the TSOC, the Emergency Preparedness Staff, and the TSA headquarters COOP team(s) at all TSA headquarters Alternate Operating Facilities (AOFs).

Ensures the development, maintenance, and availability of a disaster recovery capability for critical essential IT and telecommunications systems and equipment supporting the TSA headquarters offices and field operating elements.

Ensures that all contracts relating to IT services provide for continued and uninterrupted support during emergencies. Contractor developed emergency plans are to be forwarded to the Emergency Preparedness Staff for review, concurrence, and inclusion as part of Annex K (Information Systems Disaster Recover Plans and Telecommunications Plans).

Provides to the headquarters offices and field operating elements, the capability to electronically store and retrieve vital records and data, both hard copy and electronic, and ensures that these records and data are available for their use at all TSA AOFs.

Assists in the development, maintenance, and execution of AOF site support plans contained in Annex F (Alternate Operating Facilities) to this plan.

Develops, maintains, and executes the IT and provisioning support plans contained in Annex F (Alternate Operating Facilities) and Annex K (Information Systems Disaster Recovery Plans and Emergency Telecommunications Plans) to this plan.

Assigns appropriate personnel to each TSA headquarters AOF Site Activation Team (SAT) to cover and/or execute the following areas:

- o Activation of the supporting IT and telecommunications systems at the activated TSA headquarters AOF(s).
- o Set up of pre-positioned IT and telecommunications equipment at the activated TSA headquarters AOF(s).

Upon execution of this plan, deploys appropriate emergency teams to the IT disaster recovery site(s) supporting the activated TSA headquarters AOF(s).

Provides a senior staff officer to represent the CIO on the TSA COOP & Recovery Management Team.

Provides sufficient staffing for assigned missions and functions to support 24-by-7 operations at the activated TSA headquarters AOF(s) for the duration of the emergency or exercise.

Information Technology and Provisioning Support

Each of the Alternate Operating Facilities supporting TSOC COOP emergency operations will have a common basic set of information and telecommunications systems and functional capabilities to support emergency operations. To ensure this, all sites will have the following functional capabilities:

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 113
-----------------	------------------------------------	--	---------------

- 1) An UNCLASSIFIED local area network sufficient in capacity to support the type and size of the emergency team designated for that site and the vital records and data required during emergency operations.
- 2) Desktop access for each team member to the Internet.
- 3) Desktop access for each team member to the TSA intranet site established to support information sharing during the emergency or crisis.
- 4) Email and voice-mail connectivity among all emergency sites, as part of an overall integrated system.
- 5) The ability to send and receive FAX messages either from shared FAX machines or directly from the desktop of each team member.

A telephone system with the same capabilities that currently exist in the headquarters during normal operations.

- 6) Secure (via STU (Secure Telephone Unit) III or STE (Secure Telephone Equipment)) voice capability for each team member, as required, and secure data and FAX at least to the office/division director level offices and above, as required.
- 7) A Secure telecommunications center with access to the Defense Messaging Systems (DMS), to provide electronic distribution to customers where feasible and over-the-counter service where electronic distribution is not feasible.
- 8) Information systems to support the critical applications identified by each TSA office represented on the emergency team.
- 9) Connectivity to the systems operated by the National Law Enforcement Communications Center (i.e., SECTOR, COTHEN, etc).
- 10) Connectivity to the TSA Wide Area Network (WAN) to provide access to and from all TSA field operating elements.
- 11) Voice and video (capable of supporting both CLASSIFIED and UNCLASSIFIED) teleconferencing capability.
- 12) Multi-media telecommunications capability including, as a minimum, the public switch telephone network (PSTN) and high frequency (HF) radio.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 114
-----------------	------------------------------------	--	---------------

13) Dedicated emergency power sufficient to power the supporting IT and telecommunications network and full emergency team operations for at least 48-hours without refueling.

14) A Classified LAN with an associated email system.

C.5.3 IT Requirements in support of International Programs

Background:

TSA has 18 OCONUS and 3 CONUS sites with approximately 80 users located overseas and an additional 40 users located within the states. Users at these locations include administrative staff, middle management and senior staff level personnel. Support of the International Program Office requires that the Contractor provide management functions and technical support services at the following locations:

CONUS: (Multiple Personnel at each of the locations listed—additional site details will be provided under separate cover)

- Miami
- Dallas
- Los Angeles

OCONUS: (Multiple Personnel at each of the locations listed—additional site details will be provided under separate cover)

- Brussels
- Frankfurt
- Singapore

OCONUS: (Multiple Personnel at each of the locations listed—additional site details will be provided under separate cover)

- Philippines
- Columbia
- Brazil
- Greece
- Thailand
- Canada
- Australia
- Italy
- England
- Japan
- Argentina
- Venezuela
- China
- Spain
- France

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 115
-----------------	------------------------------------	--	---------------

The Contractor shall provide Tier II support to 14 of the 18 listed TSA international locations. The locations that are excluded are Columbia, Brazil, Argentina, Venezuela and Canada. Based on their location, support for the Argentina site shall be on a Time and Materials basis using ODC funding associated with the IT specialist supporting Frankfurt and Singapore. If TSA elects to place personnel at the 4 sites listed above or any new locations, the Contractor shall evaluate the requirements and provide proposals to perform the support.

As TSA makes these five and other locations operational, the Contractor shall evaluate the requirements and provide proposals to perform the support in accordance with the ordering process (see Section G.10).

C.5.3.1 International IT Management

The Contractor shall:

- 1) Begin providing the onsite support 30 days after award.
- 2) Manage international Contractor support staff.
 - a. This shall include management and tracking of all assets stored and deployed at the various international sites
 - b. Management of diagrams associated with cabling (i.e., network cabling)
 - c. Managing of all diagrams associated with the cabling at all locations (i.e. network cabling, POTS lines)
- 3) Knowledge of principles and practices of enterprise infrastructure environments, including VoIP; information system management; operating system characteristics; network architectures and principles of network integration; internet/intranet technologies; system integration and optimization concepts.
- 4) Operational system and practices to either lower operational costs and/or raise operational effectiveness.
- 5) Timely and efficient interface with TSA management, as necessary, on all issues related to the International Program Office.

C.5.3.2 Tier II International Technical Support:

Working within TSA IT guidelines, the Contractor shall provide an International Tier II Technical Specialist. The specialist tasks are defined by the TSA Branch Chief or designee with the objective of creating an efficient IT environment to assist in the TSA mission. The assigned tasks include but are not limited to: Microsoft desktop and application configuration; Network accessory maintenance (e.g., printers, file storage, CD burners); Analog technology support (e.g., fax, modems); Network user support; Performing Installs, Moves, Adds, and Changes; Blackberry Support; Asset Tracking; VoIP; Monitor and report IT concerns/needs to the TSA Region Branch Chief and/or Unisys Region Manager; Act as on-site focal point for users to address ITMS service inquires, provide status updates, handle incident escalations after hours, or escalate ITMS events to key TSA and Unisys management teams. Offices supported out of the base site of Frankfurt include Brussels, Belgium-Athens, Greece-Rome, Italy-London, England-Madrid, Spain, and Paris, France. Offices supported out of the base site of Singapore include Manila, Philippines-Bangkok, Thailand- Sidney, Australia, Tokyo, Japan, and Beijing, China. Two remote site visits from each base site will be done on a monthly basis, rotating through all sites. Other international sites, including Ottawa, Canada, and Buenos Aires, Argentina, will receive SPOC support only. The International Technical Support personnel shall be comprised of cleared Secret technical specialists who can resolve complex technical problems to include the reconfiguration of laptops, desktops, and troubleshooting various

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 116
-----------------	------------------------------------	--	---------------

software and hardware related issues. The Government requires a Tier II specialist stationed at the TSA Frankfurt location to support the European offices and a Tier II specialist stationed at the TSA Singapore location to support the Asian offices. These Tier II specialist shall be able to perform Installs, Moves, Adds and Changes in addition to resolving complex technical issues. These individuals shall work on-site during normal business hours and shall be available after hours on a short-term basis if required, to address emergency situations within the constraints of available resources/funding, tasking and skill requirements. Technical Support duties shall include the following:

- 1) The Contractor shall provide service spoke offices served from the Frankfurt hub with two remote site visits on a monthly basis, rotating basis
- 2) Technical support for sites in Buenos Aires and Ottawa shall not be provided by the Frankfurt technical support staff, and shall be dispatched from their respective regional technical support staff
- 3) Microsoft Desktop and application configuration
- 4) Network accessory maintenance (printers, file storage, CD burners, etc)
- 5) Minor cable repair as required
- 6) Analog technology support (fax, modems, etc)
- 7) Network user support
- 8) Performing individual Installs, Moves, Adds and Changes
- 9) Blackberry Support
- 10) Asset Tracking
- 11) VoIP Installation

C.5.3.3 Operations

The Contractor shall:

- Provide on-site technical support for all end users to support trouble calls, resolution tracking and monitoring.
- Act as a technical resource coordinator for IT users; determines users' needs; works with PC users to resolve problems.
- Provide International spare parts CLINS.
- Reports unsafe or insecure computing practices for management's follow-up.

C.5.3.3.1 Monthly Progress Report Requirements

Contractor shall provide the following operational progress reports:

- Oral weekly status reports,
- Written monthly status reports to the OCIO HQ Support Team Coordinator,
- Written weekly activity reports to the OCIO HQ Support Team Coordinator,
- Monthly labor burn report to the TSA Field Relations Team OCIO Coordinator.

The status report will be submitted on the 10th of the following month following the performance of the support activities. Should the 10th of the month fall on a Saturday, Sunday, or a Government holiday, the Contractor shall submit the reports on the next business day.

The Weekly Activity Report will consist of an itemization of each ticket worked that includes, at a minimum, (international locations):

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 117
-----------------	------------------------------------	--	---------------

- Date and time
- Individual user
- Source of activity (SPOC/Local phone call/observation)
- System malfunctioning
- Short descriptor of activity
- Work/fix performed
- Impact to the mission

The Monthly Status Report will include: (International Locations)

- Description of work accomplished during the period (the report will cover the previous month)
- Status of all activities in progress
- Planned activities for the upcoming period and associated schedule information, including dependencies with other activities/projects
- Trouble ticket status for all tickets that were opened during a specific reporting period, including aging report for open tickets that exceed defined closure thresholds. All VIP tickets will be identified separately in the same report. In addition, International Location ticket reports will not include any non-International location related tickets.

Government Property—TSA will provide administrative supplies and onsite office facilities for Contractor support personnel, to include, but not limited to, a workspace, workstation, desk and phone. Dedicated TSA laptop(s) and telephone(s) will be provided for the TSA.

Support Staff Review—Due to the criticality and sensitivity of international operations, the Government intends to review Contractor qualifications prior to assignment at all International sites.

Security Clearances—Contractor shall ensure that all assigned personnel are appropriately cleared for their designated position as stated in site specific service requirements. Contractor personnel providing operational, development or maintenance support will possess the required clearance consistent with OCIO Policy Directive No. 2005-1, as revised.

C.5.4 TSA Cat X and Cat 1 Airport locations

Background

The Government requires the Contractor provide TSA Cat X and Cat 1 locations the management functions and technical support for the support services below.

C.5.4.1 Management

The Contractor shall:

- 1) Provide user support at Cat X and Cat 1 Airport locations user support to include the following
 - a. Direction to subordinates on general policies and management guidance
 - b. Management and tracking of all assets stored and deployed within Cat X and Cat 1 Airport locations
 - c. Supervision of assigned Contractor shifts, including determining and maintaining appropriate staffing levels, conducting employee performance evaluations, providing

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 118
-----------------	------------------------------------	--	---------------

counseling, and investigation and making recommendations regarding disciplinary actions

- 2) Ensure compliance with the principles and practices of enterprise infrastructure environments, including VoIP; information systems management; operating system characteristics; network architectures and principles of network integration; internet/intranet technologies; systems integration and optimization concepts
- 3) Propose systems and practices to either lower operational costs and/or raise operational effectiveness
- 4) Interface, as necessary, with TSA management on all issues related to Cat X and Cat 1 Airport locations IT Operations

C.5.4.2 Tier II Support

The Government requires on-site Tier II support that is comprised of cleared Secret technical specialists who will resolve complex technical problems to include the reconfiguration of laptops, desktops, and troubleshooting various software and hardware related issues. The Contractor provided Tier II Technical Specialist shall work on-site at Cat X and Cat 1 FSD locations during normal business hours and will be available after hours on a short-term basis, if required, to address emergency. These individuals shall provide weekly oral briefs to FSD and/or staff on services and status of FSD-assigned projects. The individual shall proactive service and capacity trending review, working closely with ITMS groups to confirm validity and accuracy with SLA performance review. This is done on a monthly basis. There shall be a sufficient staff of individuals assigned to the TSA Field Relations Team with the primary function of performing Installs, Moves, Adds and Changes. This team shall work on-site at Cat X and Cat 1 Airport locations during normal business hours and will be available after hours on a short-term basis if required, to address emergency situations within the constraints of available resources/funding, tasking and skill requirements. The Cat X and Cat 1 Airport locations Technical Support Team duties shall include the following:

- 1) Microsoft Desktop and application configuration
- 2) Network accessory maintenance (printers, file storage, CD burners, etc)
- 3) Minor cable repair as required
- 4) Analog technology support (fax, modems, etc)
- 5) Network user support
- 6) Individual Installs, Moves, Adds and Changes
- 7) Blackberry Support
- 8) Asset Tracking
- 9) Manage all HQ POTS dial tone
- 10) VOIP Support
- 11) Data Collection/Download
- 12) Training Software Update Installs

C.5.4.3 Tier II Support Management

The Government requires a geographic customer support manager responsible for all TSA facilities within a geographic area. TSA requires that each customer support manager shall be responsible for a maximum of five (5) states. The customer support manager shall be responsible for all Tier II support, deployments; office moves etc. within their geographic area and coordinate activities with the TSA Regional Branch chief.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 119
-----------------	------------------------------------	--	---------------

C.5.4.4 Operations

The Contractor shall:

- 1) Provide on-site technical support for all end users to support trouble calls, resolution tracking and monitoring.
- 2) Provide immediate end user support for all VIP's. The VIP list will be maintained by TSA and provided to the Contractor
- 3) Perform individual assignments associated with the support, maintenance, deployment of applications, and management of the information systems, products and services that support the internal operations of TSA. (Install, Moves, Adds and Change team member)
- 4) Act as a technical resource coordinator for IT users; determines users' needs; works with PC users to resolve problems and provide guidance to the TSA Headquarters Support Team.
- 5) Reports unsafe or insecure computing practices for management's follow-up.

C.5.4.5 Monthly Progress Report Requirements

Contractor shall provide the following operational progress reports:

- 1) Oral weekly status reports,
- 2) Written monthly status reports,
- 3) Written weekly activity reports, and
- 4) Monthly labor burn report to the TSA Field Relations Team OCIO Coordinator.

The monthly status reports will be submitted on the 10th working day of the following month, or such other date as may be specified by the TSA Field Relations Team OCIO Coordinator. Each monthly status report shall include a funding status summary for the report period. This report shall include excess hours available as may result from personnel departures or unavailability.

The Weekly Activity Report shall consist of an itemization of each ticket worked that includes, at a minimum, (Cat X and Cat 1 Airport locations)

- 1) Date and time
- 2) Individual user
- 3) Source of activity (SPOC/Local phone call/observation)
- 4) System malfunctioning
- 5) Short descriptor of activity
- 6) Work/ fix performed
- 7) Impact to the mission

The Monthly Status Report will include: (Cat X and Cat 1 Airport locations)

- 1) Description of work accomplished during the period (the report will cover the previous month)
- 2) Status of all activities in progress
- 3) Planned activities for the upcoming period and associated schedule information, including dependencies with other activities/projects
- 4) Trouble ticket status for all tickets that were opened during a specific reporting period, including aging report for open tickets that exceed defined closure thresholds. All VIP tickets will be identified separately in the same report. In addition, Headquarters ticket reports will not include any non-headquarters related tickets
- 5) Funding status summary

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 120
-----------------	------------------------------------	--	---------------

The Monthly Asset Status Report in Section C.4.3.17.7 shall include all assets for airport and offsite locations.

Support Staff Review—Due to the criticality and sensitivity of Airport operations, the Government intends to review Contractor qualifications prior to assignment at all Airport/offsite locations.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 121
-----------------	------------------------------------	--	---------------

C.6 DHS Headquarters

C.6.2. DHS Headquarters Performance Work Statement Requirements

C.6.2.1. Background

DHS Headquarters is geographically dispersed throughout the Washington DC metropolitan area at 24 locations, and currently has more than 4,000 user seats. Users at these locations include the Department Secretariat, Senior Executives, administrative staff, middle management, and the bulk of the DHS workforce. Additionally, DHS HQ supports an office location at Plum Island New York. Support of the DHS headquarters requires that the Contractor provide management functions and technical support as described throughout this solicitation.

C.6.2.1.1. Baseline Services

The Contractor shall baseline IT services provided to DHS with the support required to operate and maintain the DHS unclassified infrastructure, and may manage assets associated with LANs B and C as ordered by the Government. With these services, DHS is assured a properly managed and stable computing environment that supports the Department's mission objectives.

C.6.2.2. Scope of DHS Headquarters Work

The Contractor shall provide the DHS Headquarters a full line of Information Technology (IT), telecommunications, and related s to manage the baseline requirements defined here.

The Contractor shall provide the DHS Headquarters an enterprise architecture and IT infrastructure that conforms to specified standards for reliability, readiness, sustainability, supportability, availability, stability, security, flexibility, responsiveness, and cost effectiveness.

The Contractor shall provide necessary IT and telecommunications services as ordered to include, but not limited to: hardware, software, maintenance, asset inventory tracking, help desk, security, data center, WAN/LAN, server, wireless, PDA, land mobile radio, voice and data telecom, training and program management that meet or exceed DHS HQ program objectives.

The Contractor shall provide the full range of services needed to analyze requirements, develop and implement recommended solutions, and operate IT products and services needed to deploy, as well as maintain, IT and telecommunication services for the DHS Headquarters within contract scope and level of effort. The Government may request additional services via an Initiation /Task Order.

The Contractor shall, in the performance of the work required by this bridge effort, interact and coordinate with other contractors and vendors.

The Contractor shall perform requirements in a Work Breakdown Structure (WBS) format as outlined herein in Appendix A-F. Each WBS section shall be performed as a "stand alone" package of work. Resources needed to accomplish a work package shall be identified in the Contractor's proposal for that work package. All resources needed to accomplish the WBS work packages shall be reflected in the staffing for that work package, and shall not be included elsewhere. All reporting requirements in support of each WBS work package are the responsibility of the WBS staff and its management team;

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 122
-----------------	------------------------------------	--	---------------

The Government reserves the right to cancel the requirement for any specific CLIN or sub-CLIN so long as a 60-day written notification is provided to the Contractor of the Government's intent to cancel. The Government and Unisys must mutually agree to the cancellation terms and conditions.

The Government intends to make more space available to the Contractor as soon as possible, but no later than April 30, 2006. In the meantime, Unisys agrees to notify the Government of its space requirements under the bridge contract based on the approved and agreed staffing levels by location and type of resource (engineering, security, desk side technician, etc.).

The Government's space requirements in the Unisys facility at Pentagon City for the bridge are for two offices and approximately 20 cubicles (one person/cubicle); Unisys will develop a separately orderable CLIN for inclusion in the bridge contract that will allow the DHS to order this space as needed. There will be no minimum order quantity associated with this CLIN.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 123
-----------------	------------------------------------	--	---------------

C.6.2.3.1 User Population and locations
Total Current Users 4500
Expected growth to 5800

C.6.2.3.2 Facilities:

LOCATIONS	
7th & D 301 7th Street SW Washington, DC	NAC 3801 Nebraska Avenue NW Washington DC 20016
Vermont Ave 1120 Vermont Avenue, Washington DC 20223	New York Ave 1201 New York Ave, NW Washington DC 20005
ODP Tech World 800 K Street, NW Washington DC	Glebe Rd 1110 N. Glebe Road Arlington VA
BIO Watch 675 North Washington Street Alexandria VA	JPO Fair Lakes Fair Lakes VA
National Press Club 529 14th Street, Suite 200 NW Washington DC	Wilson Blvd, MANPADS Wilson Blvd Arlington VA
WMP Greenwood Fair Oaks VA	Hoover Building NIPC 935 Pennsylvania Ave. NW Washington DC 20228
TSA Building 701 South 12th Street, West Tower Arlington VA 22202	New Mexico Ave New Mexico Ave Washington DC
PCII Old Gallows Road McLean VA	Pentagon City 1200 South Hayes Street Arlington VA 22202
RDS 245 Murray Drive Washington DC 20223	Plum Island Plum Island NY
Wisconsin Ave 1150 17th Street, NW Washington DC 20036	One Lafayette Center 1120 20th Street, NW 3rd Floor Washington DC 20223
4803 Eisenhower Avenue Alexandria VA 22304	1331 F Street Washington DC
500 C Street NW Washington DC	Site A

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 124
-----------------	------------------------------------	--	---------------

C.6.2.3.3 End User equipment

Table – End User Equipment Estimates as of May 2005

End User Product	Quantity (Estimated)
Desktop	3647
Laptop	2059
Cell Phone	1580
Pager	386
PDA	3290
Copier	140
Fax	296
Paper Shredder	32
Projector	87
Scanner	207
Secure Fax	15
Multifunction - Printer/Scanner/Fax	103
Plotter	8
Printer	870

C.6.2.4 Requirements

C.6.2.4.1 List of Applicable Laws, Regulations, Policies, and Guidelines

The laws, regulations, policies, and guidelines that apply to this Program are listed in Appendix G. The Contractor is expected to be informed and knowledgeable of these requirements.

C.6.2.4.2. Task Orders and Delivery Orders

Task Orders and Delivery Orders initiated after the award date shall be governed by the terms and conditions of the contract resulting from this award.

Substitution of product will be allowed so long as the price of the substituted product is less than or equal to the price of the current product, and the features, functionality, and performance of the substituted product is equal to or greater than the features, functionality, and performance of the product being substituted. Unisys must submit a report to the Government's Contracting Officer or designated representative of product substitutions under an existing CLIN as soon as practical after notification from supplier. Unisys will provide salient characteristics of the product. The Government will promptly review and accept or reject the Contractor substitution report. This language supplements the requirements of the Substitution Clause in Section H of the TSA contract.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 125
-----------------	------------------------------------	--	---------------

C.6.2.4.3. Deliverables

The Contractor will track the deliverables shown in the Table below, and regularly report on their status in the Deliverables Tracking List:

TABLE OF DELIVERABLES		
C-6 RFP REFERENCE	NAME OF DELIVERABLE	REMARKS
C.6.3.1.2.11.	SLA Statistics Briefing	Monthly
C.6.3.1.2.11.	SLA Reports	
C.6.4.1.	Program Management Plan	
C.6.4.1.	Program Status Report	Monthly
C.6.4.1.	ETC report	Monthly
C.6.4.1.1.	Asset Inventory Management Report	
C.6.4.1.1.	Quality Plan	
C.6.4.1.3.	Government Property Report(Form 700-5 (7/03)	Annually
C.6.4.1.	Weekly Program Activity Report	Weekly
C.6.4.3.1.1.	Management and Usage Report-Tier 1 Services	Monthly
C.6.4.4.5.1.	Up/Down Status Report of Major Applications on the Network	
C.6.4.4.5.2.		
C.6.4.4.5.3.	Ad Hoc Reports (Executive) based on tool capability	As Requested NTE 5/mon
C.6.4.5	Integrated Security Program Management Plan	
C.6.4.5	Security Status Report	Weekly
C.6.4.5	DHS Security Improvement Plan	
C.6.4.5	CAP ATO Packages For New Sites And Expanded Facilities	
C.6.4.5	Risk Management System (RMS) and Trusted FISMA Agent (TFA) Reports	
C.6.4.5	C&A Packages for LAN A Sub-Architecture to include BlackBerry, VOIP, , Sharepoint, Project Server	
C.6.4.5	Enterprise Risk Assessment	
C.6.4.5	Risk Assessment Status Reports	Monthly, Quarterly, As Needed
C.6.4.5	Risk Level Matrix	Quarterly, As Needed
C.6.4.5	ECR Tracking and Status Report	Weekly
C.6.4.5	Baseline of ECR Submission Artifacts	Quarterly
C.6.4.5	Baseline of Configuration Artifacts	Quarterly
C.6.4.5	Draft Enterprise Security Component Target Architecture	
C.6.4.5	Project Plan for Phase I Automation Capability	
C.6.4.5	VIM Strategy Document	
C.6.4.5	Security Situational Education Assessment Report and Project Plan	
C.6.4.5	IDS Activity Reports	Daily, Weekly, Monthly
C.6.4.5	LAN A Incident Response Handbook, Version 2.0	
C.6.4.5	Incident Report and Metrics	Weekly

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 126
-----------------	------------------------------------	--	---------------

C-6 RFP REFERENCE	NAME OF DELIVERABLE	REMARKS
C.6.4.5	Misuse Report	Monthly
C.6.4.5	Incident Reports	
C.6.4.5	Moratorium Report	
	(Duplicate above)	
C.6.4.6.	Asset Inventory Management Report by Organizational Component	
C.6.4.6.	DHS Inventory Data base and EA Repository Report	Monthly
C.6.4.6.	TTO/TTR Report	Monthly
C.6.4.6.	IMAC Report	Weekly
C.6.4.6.	DD Form 250 Status Report	Monthly

C.6.3. Task Order Objectives Statement

C.6.3.1. Task Order Information

C.6.3.1.1 Requirements

Table 1.1 below sets forth the requirements that must be met in this Task Order.

Table 1-1 Task Order Information

<p>Task Order Number Work Order Number Task Order Title Task Order Issue Date Proposal Due Date Task Order Summary The United States Department of Homeland Security (DHS) requires a comprehensive, enterprise-wide information technology partner to assist the Department in meeting its responsibilities under current statutes and DHS Management Directives. Various services will be required in a number of separate work orders or categories of effort. These include Program Management Services, Engineering Operations, End-User Services, Application Services, Security Services, and Asset Inventory Management. The period of performance for this work order is from date of award through the base period as agreed. The price proposal for this effort shall be presented for contract base period as agreed. General discussions related to each of these areas are included below.</p>
--

C.6.3.1.2. Statement of Work Description

C.6.3.1.2.1. Task Monitors

The task monitors for this effort are set forth in Table 2-1, DHS Task Monitors, below.

Table 2-1 DHS Task Monitors

	Primary	Alternate
Name	Peter Kuhmerker	Tina Honey

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 127
-----------------	------------------------------------	--	---------------

Phone Number 202-260-0200 (202) 772-0904

E-Mail Address peter.kuhmerker@dhs.gov tina.honey@dhs.gov

Table 2-2 Contractor Task Monitors

	Primary	Alternate
--	----------------	------------------

Name
Phone Number
E-Mail Address

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 128
-----------------	------------------------------------	--	---------------

C.6.3.1.2.2. Requirements Definition

This section identifies Information Technology (IT) services required by the Government. The Government requests this support through a combination of time and materials (T&M) and fixed-price level of effort (FPLOE) labor. Applications Services and Business Management are firm fixed price.

DHS requires that all active service requests from ITMS Work Orders Nine and Eleven be transferred to the new contract with the terms and conditions under which those service requests were originally issued. These existing service requests are to continue to remain in effect, uninterrupted, for products and services currently provided. For products and managed services delivered under these service requests, DHS requires that the original payment terms continue in effect. For additional time and materials and fixed-priced labor services, DHS requires that existing terms and conditions remain in effect until such a time as modification to those terms and conditions are requested by DHS under this new contract.

For legacy products, Unisys will transfer ITMS task order CLINS to which the Government has a continuing payment obligation. The transfer will occur, without modification to the terms and conditions governing legacy products. The Government will continue its monthly payment obligations until such time the Government executes a TTO or TTR CLIN.

For Government Furnished Equipment (GFE), the Government will provide the products to the Contractor, who will manage the asset using the Asset inventory management CLIN as ordered.

For products and services purchased directly from the Contractor, the Government retains the option to manage the product on its own, or order an Asset inventory management CLIN. Assets the Government elects to manage are beyond the scope of this contract unless those services are ordered.

C.6.3.1.2.3. Summary

The newly formed and evolving DHS HQ faces a series of challenging mandates that rely heavily on establishing and implementing sound IT processes and practices, and obtaining the best available resources and technology.

DHS and Unisys will work jointly to develop a Program Management Plan that will conform to the levels and extent of services expressed within the performance work statement and associated service level agreements.

C.6.3.1.2.4. Background

DHS requires the Contractor to establish and maintain an information technology and telecommunication infrastructure support services capability for the employees at DHS Headquarters previously defined.

DHS requires a comprehensive enterprise-wide information technology partner to assist the Agency in meeting its statutory responsibilities.

Services and products identified and discussed in the subsections to follow are to provide required IT services to the DHS organization as well as management visibility, quality, and defined mission support. DHS requires predictability of service; visibility into the impact of the IT program on mission objectives; flexibility in terms of IT product offerings and services; speed of service; and innovation in

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 129
-----------------	------------------------------------	--	---------------

terms of new product integration. The Contractor shall seamlessly manage changes and improvements to the DHS IT environment as DHS evolves toward the integration of multiple IT environments.

C.6.3.1.2.5. Customer/IT Requirements

The following DHS business objectives are considered key and are followed by the corresponding recommended approach. The contractor shall work with the Government and its Team in deciding the best approach to achieving these goals. In this regard, the following guiding principles govern:

- Data created in the performance of the contract becomes the property of the Government, in accordance with Section I, Rights in Data clauses.
- The Government desires that costs during this bridge performance period be kept to an absolute minimum without sacrificing mission accomplishment; exit costs must also be minimized;
- The Government expects full functionality when the Contractor provides tools, software, or other products for this contract, including contractor-provided upgrades, patches, and product releases;
- The Government expects the Contractor to pass on enhancements to tools, software, or other products for this contract that are made available to the Contractor by software or product vendors;
- The Contractor is expected to pass along benefits such as free licenses, upgrades, etc., that accrue to the Contractor as a result of this contract;
- Government guidelines and standards relating to privacy, confidentiality, and integrity of systems and data must be considered along with the importance of availability;
- The Government expects the Contractor to provide industry standard services that would be available from an established, world-class integrating contractor; and,
- Since this is a performance-based statement of requirements, the Contractor is expected to provide the performance levels specified in Service Level Agreements contained in this contract.

C.6.3.1.2.6. Statement of Objectives Risks

C.6.3.1.2.6.1. DHS-Identified Business Objectives Requirements

- To provide desktop and communications tools as ordered to designated DHS and support contractor staff within the agreed timeframe. Deliver the right product or services at the right time and at a fair and reasonable price
- To anticipate customer IT requirements and provide DHS management demand forecasts to proactively meet those needs, including proposing and adding to the contract new IT products and services to anticipate these demands

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 130
-----------------	------------------------------------	--	---------------

- To proactively propose process improvements on current operations and problems that are accepted by DHS and implemented and reported in a timely manner.
- To achieve a high degree of network availability for IT tools, especially for mission critical activities
- IMACs are completed in accordance with the requirements of an advanced scheduling plan as provided by the Government
- All work performed by the Contractor shall conform to DHS standards and guidelines for security and enterprise architecture:
- The Contractor shall provide 7 X 24 x 365 intrusion detection and prevention services
- All systems provided by the Contractor shall be capable of being certified and accredited
- Services provided by the Contractor shall comply with standards set for the DHS One Infrastructure, to be provided by DHS
- The Government intends to transition to the DHSOne Infrastructure Program; Unisys will assist the Government in this initiative viaa separate Task Order or Delivery Order;
- The Contractor and the Government will work together to apply the project management principles and practices set forth in existing DHS HQ management directives;
- The Contractor shall, to the greatest extent possible, leverage Government-furnished equipment (GFE) and government-provided software licenses.

C.6.3.1.2.6.2. DHS Desired Approach to Identified Business Objectives Requirements

- The Contractor shall provide the DHS Standard Desktop Configuration to designated DHS and support contractor staff within the standard established by the Service Level Agreement.
- To meet this objective, the Contractor shall receive advance notification of personnel arrival. The Contractor shall provide site support according to the 100:1 ratio for clients/desk side technicians and as required, additional network engineers.
- As the DHS organization grows, the Contractor shall make support recommendations to DHS management in the form of a support CLIN.
- The 100:1 ratio shall be based on the client/desk side technician ratio that supports the weekly calls at all locations where calls require a desk side visit.
- To successfully support continued growth of the user population, the Contractor shall add one additional technician for every 100 new users. Addition of new users will be based on active accounts; these are defined as accounts that have been actively used within the past 30 days. The Government will order/approve the additional technicians when proposed by the

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 131
-----------------	------------------------------------	--	---------------

Contractor to meet the support of objectives and applicable SLAs based on the criteria for adding new technicians.

- To facilitate the ability to anticipate DHS customer IT requirements, and to identify and propose candidates for process improvement, the Contractor shall provide DHS management with a monthly program update. This update will provide feedback to the DHS management team on identified customer needs, new trends within industry, and areas recommended for improvement based on organizational metrics. The Contractor shall also provide recommendations of potential solutions to the management team based on this feedback.

In support of the goal for a high degree of network availability for IT tools, the Contractor shall collaborate with DHS performance management personnel and report monthly on mission critical SLAs. All SLAs will be evaluated quarterly by the DHS management team to ensure that the SLA measurements are indeed the priorities of the organization.

- As required by the Government, desk side technicians shall provide moves, adds, and changes as a part of their normal day-to-day- responsibilities. The Government reserves the right to notify the Contractor when the Government's mission priorities have changed, and expects the Contractor to adjust its desk side resources accordingly. Installations in support of new build-outs will be addressed in specific project-related Task Orders.
- 7 X 24 X 365 intrusion detection and prevention services utilizing Intrusion Detection Software has been approved, tested, and successfully piloted at DHS. The cost for this service shall be included in a Task Order or Delivery Order.
- The Contractor shall certify and accredit LAN A systems and equipment within DHS in accordance with DHS guidance, and will continue to ensure that LAN A equipment remains certified by providing the necessary engineering technical support.
- The Contractor shall comply with the DHS One Infrastructure guidance which will essentially change the network connection from DCN to MPLS.
- The Government intends to transition to the DHSOne Infrastructure Program; Unisys will assist the Government in this initiative via separate Task Order or Delivery Order;
- The Contractor may provide system and network monitoring from its Network Operating Center (NOC). The Contractor shall use the data from its monitoring systems to provide reports as specified in the SLA section (e.g., MS Exchange Server Disk Space Utilization). This data will also be used to validate any applicable SLAs.
- The Contractor shall use the DHS SDLC for all project work within DHS HQ.
- The Contractor shall be cognizant of the desire for DHS to utilize GFE and Government-provided software licenses, and will provide GFE CLINs as required to support this initiative. GFE equipment and software will be tested and then approved via the Change Control Board, utilizing a GFE equipment/software CLIN to ensure DHS integrity.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 132
-----------------	------------------------------------	--	---------------

C.6.3.1.2.7.1 DHS-Identified Program Management Objectives

- Repeatable Project Management processes, especially to handle build-out projects and moves
- Program Operations – provide robust measurable metrics and performance tracking
- Ensure a smooth running service fulfillment process – streamlined, repeatable, and customer accessible
- Ensure appropriate response and follow-up with customer requests, including customer-focused SLAs and reports

C.6.3.1.2.7.2. Approach to Management Objectives

- In an effort to standardize and streamline project management processes, the Contractor shall utilize the DHS SDLC. The Contractor shall create standard DHS templates for the basic build-out and move work packages which will significantly increase the repeatability of processes and procedures.
- The Contractor is expected to cooperate with DHS HQ during the agreed “normalization” period to refine and improve SLAs contained in this solicitation.
- The Contractor approach to the fulfillment process shall focus on Visibility. The focus of fulfillment shall be to complete orders in a timely manner. The Contractor shall provide status reports to the appropriate DHS leaders and customers that accurately portray all pending fulfillment actions, utilizing a Web Ordering System (WOS) site as well as weekly reports. This ensures the process is streamlined, repeatable, and easily accessible by DHS.
- The Contractor shall utilize all available assets to quickly and efficiently respond to customer requests. This data will be examined monthly by the DHS Management Team to ensure that the SLAs are effectively tracking the most significant business needs of the organization.

C.6.3.1.2.8. Global Objectives

C.6.3.1.2.8.1. DHS-Identified Global Objectives

- Establish joint program management for DHS SDLC/Capital Planning and Investment Control (CPIC) processes to supplement the formal planning and project methodologies to develop project plans and other processes and procedures that will facilitate the accomplishment of program objectives
- Establish the DHS requirement of a dedicated on-site support team to manage the infrastructure and handle user problems/requests
- Develop and institutionalization of processes and tools that integrate planning, development, implementation, operation, and maintenance
- Design, deploy, and manage the security equipment and applications required to comply with DHS Security Architecture

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 133
-----------------	------------------------------------	--	---------------

- The Government intends to develop a fully-functioning DHS portal for collecting, sharing, and organizing information that supports and enables designated communities of interest to collaborate and share information, thereby increasing their mission effectiveness; Unisys will cooperate with the Government in this endeavor. This effort would be addressed via a separate Task Order or Delivery Order.
- Authorized DHS representatives shall be able to electronically order services, report troubles, and receive service status alerts
- Establishment of efficient and effective lines of communication that allow real time transmission of information 24X7
- The use of experienced professional staff to work closely with DHS personnel and other concerned parties to successfully achieve DHS and ITMS objectives
- Provide recommended customer-facing SLAs, KPIs, and incident linkages and the management processes that improve service and reduce the Total Cost Ownership (TCO).
- Contractor team members meet DHS security requirements, including those required to support the DHS Secure Compartmented Information Facility (SCIF) and receive appropriate credentials to access DHS locations, as required.
- Demonstrate the effective use of warranties and volume pricing that is consistent with DHS business objectives

C.6.3.1.2.8.2. DHS Desired Approach to Global Objectives

In an effort to establish joint program management for DHS, the Contractor shall share schedule information, the status of projects, the status of tickets, and the status of engineering initiatives in weekly meetings following the format in mutually agreed upon reports.

- The Contractor shall provide customer service and provide 24x7 infrastructure support by structuring the team to provide Help Desk support, engineering support, and Desk Side support for all LAN A users at agreed locations.
- The Contractor will cooperate with the Government in making relevant content data available to the DHS portal; communities of interest will provide their requirements for Contractor-generated content and the Contractor is expected to cooperate in pushing this data to those communities of interest based on their requirements.
- The Contractor shall, in cooperation with the DHS Information Systems Security Manager (ISSM), develop an internal DHS Headquarters Security Program as part of an integrated framework capable of meeting mission requirements. The Contractor shall provide the following services to the ISSM Management Directorate:
 - Assist in developing DHS Management Directorate's security policies and procedures, with particular focus on the management of the Local Area Network (LAN).
 - Assist the ISSM, Management Directorate with the certification and accreditation (C&A) process for management systems and applications and evaluation of LAN A-related issues.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 134
-----------------	------------------------------------	--	---------------

- Assist the ISSM, Management Directorate in identifying and mitigating risks for all management operational systems
- DHS and the Contractor shall utilize a Web Ordering System (WOS) to electronically order products and services or other method as agreed. Additionally, the Contractor shall provide a 24x7 Help Desk to report trouble calls and receive service status reports.
- The Contractor shall structure the engagement to provide dedicated engineering support in an effort to establish efficient and effective lines of communication and allow real time transmission of information for all DHS personnel 24x7.
- The Contractor shall meet monthly with the Government to review the results and discuss any issues identified by the SLAs.
- All Contractor personnel shall meet the current DHS security clearance requirements set forth in DHS Management Directive 4300. The negotiated labor rates include a security clearance level to the Secret level; if a higher security clearance level is required, and the Contractor provides a staff who already possesses the required clearance, the Government and Unisys will negotiate the labor category and rate for the staff position; if the Contractor chooses to upgrade a staff position's security clearance to fill a current or future requirement, the administrative cost for obtaining this increased security clearance level shall be addressed via the G&A cost accounts, and shall not be billed as a direct charge. New security and SCIF requirements should be promptly addressed in order to allow personnel time to become compliant in support of the DHS mission
- DHS has a 100% interoperability goal within the DHS enterprise. The Contractor shall identify areas that require processes, procedures, or products within the enterprise and provide them as suggestions to senior DHS Management Team in the proposed monthly program review. The impetus behind the monthly program review is to provide a report that integrates all aspects of the ITMS Team (desk side support, engineering, business operations, PMO) and provide a report that encompasses and reports on the overall health of the organization and makes recommendations, or describes solutions, that impact mission accomplishment within the Department.
- Warranties shall be included in all services and ODC Contract Line Item Numbers (CLIN). Service CLINs based on standard and extended manufacturer-provided warranties. The Contractor will make every effort to obtain volume discount pricing on personal computers and discount pricing on products that are purchased through preferred contractors.

C.6.3.1.2.9. Specific Requirements

C.6.3.1.2.9.1. DHS-Identified Specific Requirements

- Provide DHS LAN connectivity, Internet access, VPN capability, and servers and applications that make up the core foundation of networks architected to optimize information security, Total Cost of Ownership, reliability, and user satisfaction in meeting DHS objectives
- Provide application (commercial-off-the-shelf [COTS]/Government-off-the shelf [GOTS]/custom) integration and implementation and maintenance support for DHS systems, such as the E-Gov Platform

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 135
-----------------	------------------------------------	--	---------------

- Establish and maintain backup/disaster recovery consistent with DHS plans
- Provide an integrated call center capability that supports various DHS operational needs
- Implementation of a near real-time operations monitoring tool
- Server equipment and infrastructure deployment to support DHS mission critical applications and be upgradeable
- Effective use of Web technologies to keep DHS customers current with DHS IT status, capabilities, and planned enhancements (i.e., Help Desk Web site). These efforts shall also include the development and maintenance of a DHS service ordering system.
- Pricing that demonstrates DHS is receiving the most cost-effective solution

C.6.3.1.2.9.2. Approach to Specific Requirements

- The Contractor shall provide an Engineering and Operations Team that will perform as an integrated staff that will enhance DHS operations by allowing DHS to retain and leverage a core team, level the costs for a core effort, and eliminate separate design charges from projects. Total Cost of Ownership, based on monthly cost, planned obsolescence of equipment, projections for growth costs, and DHS One Infrastructure compliance will follow the DHS growth plan and will be outlined to DHS management. Reliability of the core network and user satisfaction will be measured utilizing the appropriate SLAs.
- The Contractor team shall make every effort to use Commercial-off-the-shelf (COTS) software and other tools in supporting the Government's requirements; the Contractor's commitment to this approach will be specifically monitored by the Government and will be construed by the Government as an indication of the Contractor's commitment to manage costs and improve efficiencies and service.
- The engineering team shall focus on the core infrastructure foundation of DHS to provide proactive monitoring and maintenance, responsive troubleshooting and correction of issues, and thought leadership in evolving enterprise architectural designs, and in developing disaster recovery and back-up capabilities for the Government; the Contractor is expected to create standard operating procedures (SOP) to ensure all backup/recovery operations are documented; the Contractor is expected to employ sound, industry best practice-based back-up and recovery technologies to ensure consistent and reliable protection of user and system data.
- To align with DHS strategic architecture visions, as well as to meet overall DHS operational reliability and customer satisfaction objectives, all significant infrastructure proposed changes will follow the established DHS Change Management process from engineering review, to final approval, to implementation.
- The Contractor will make every effort to leverage existing network and application monitoring toolsets within the Command Integration Center, Network Control Center, Server Management Center and the on-site Engineering and Operations Team to ensure near real-time monitoring of the DHS infrastructure.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 136
-----------------	------------------------------------	--	---------------

- The Contractor shall work directly with DHS business, technical, and security management to ensure that infrastructure network, server, and storage equipment is deployed per Government and manufacturer standards. These efforts are monitored by the DHS change control board.
- Web technologies will be utilized to provide monitoring information of systems and product orders utilizing a DHS proposed portal with access to Peregrine and the Web Ordering System.

C.6.3.1.2.10. Department of Homeland Security – Service Level Agreements

SLAs are based on industry best practices and are designed to capture performance measures where they have the greatest impact on the end user. SLAs will be managed by a team from the Contractor, with oversight from the Government's PMO function. The Contractor shall provide a monthly SLA statistics briefing to the DHS management and leadership team addressing each of the areas discussed below.

The Contractor shall implement service level agreements established by the Government in the following performance areas using the guiding principles set forth here:

- Asset Inventory Management – The effective management, control, and reporting of assets enables the DHS to meet the needs of its customers as they pursue their specific mission responsibilities. For this reason, asset inventory management is a critical component of the DHS's mission performance capability. In addition, an effective asset inventory management system is necessary for meeting other statutory and fiduciary reporting requirements.
 - The purpose of this Service Level Agreement (SLA) is to measure the effectiveness of the Contractor in setting up and administering such an asset inventory management system that provides these capabilities.

The Contractor must provide a complete set of data, reports, analysis, recommendations, defined processes, and performance-related information to conclusively demonstrate that the Asset Inventory Management system performs as agreed.

- Infrastructure Support – This support is the fundamental enabler of DHS's mission performance capability. The Contractor must provide a comprehensive plan for managing infrastructure for which the Contractor has responsibility and control.
 - The Contractor must provide a comprehensive set of performance measures that demonstrate integrity and effective management to achieve and maintain needed capabilities of the existing DHS infrastructure.
 - The Contractor must have a complete plan, and clearly defined, repeatable, documented processes that represent industry best practices for managing infrastructure requirements.
- Help Desk – The help desk provides the primary interface between the requester and the service provider, and is the primary contact that customers will use to obtain services and support for day-to-day needs; therefore, the quality of this help desk service must be consistent and delivered at a high performance level.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 137
-----------------	------------------------------------	--	---------------

- The Contractor's role in accomplishing the mission of the help desk function will be to act as the Single Point of Contact for the initial service request; the Contractor will assess the nature of the requestor's service issue (i.e., LAN A, LAN B, or LAN C), determine the appropriate solution provider, and forward the detailed service request to the selected vendor; if the vendor is a DHS third-party vendor (e.g., Verizon, TWD, Northrop Grumman, etc.) then the Contractor help desk will close the service ticket by annotating the service ticket with the vendor to whom the service request was referred; reporting of the service ticket status and resolution will be the responsibility of the DHS HQ third party vendor; if the Contractor is the responsible vendor for the help desk service request, the Contractor will retain ownership of the service request, and will interact with the customer until the service request is resolved, and status is reported to the Government.
- The SLA for this area establishes key performance factors to regularly assess the quality of help desk services provided to customers.
- This contract is the authority for the Contractor to act as the Government's agent in accomplishing this help desk function.
- As new help desk management capabilities are obtained, the Contractor will collaborate with the Government to modify SLA to conform to these new capabilities.
- The Contractor must provide a comprehensive help desk capability that provides easy and ready access, user profiling, data management, response management, agent management, end-to-end functionality, and other features that enable quick and effective resolution of customer requests.
- Security
 - The Contractor and the Government will jointly agree on critical systems that must be kept secure at all times.
 - A comprehensive set of performance factors as described in the Security WBS KPIs and SLA factors must be established and carefully managed to support the security requirements of the enterprise.
 - The Contractor must provide appropriate safeguards of all systems and applications within the Contractor's area of responsibility and control.
- Customer Satisfaction – Customer satisfaction is the ultimate measure of the effectiveness of service delivery.
 - The Contractor must provide high quality, responsive, and complete services to the DHS customer community.
 - This SLA is designed to capture important and timely customer feedback that will enable the Contractor to implement an effective continuous improvement program responsive to customer needs.
 - In this context, data gathered for the performance factors listed in the SLA and as agreed with the Government must be used to continually adjust products and services being delivered to the customer community based on their changing mission needs.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 138
----------	------------------------------------	--	---------------

- Program Management Services are the key enablers of the day-to-day mission activities, and specifically support key infrastructure and customer support requirements.
 - The Contractor is expected to deliver program management services that recognize the Government's key requirements for operational project management and financial management services in support of the Government's internal control and CPIC reporting responsibilities.
 - Effective program and project management are essential components of the DHS Capital Planning and Investment Control (CPIC) process. The Contractor is an integral contributor to this process; ;
 - The purpose of this Service Level Agreement is to regularly assess a) effectiveness of the Contractor's support to these key enablers, b) the Contractor's program and project management capabilities and services, and c) to make sure that all Government requirements are addressed, and d) to assist with the compliance of Federal mandates.

Summary

Service Level Agreements are included in Appendix H. This set of Service Level Agreements has been generally agreed, with the understanding that each of them will undergo a mutually agreed "normalization" period, during which time additional data will be collected, reviewed, and discussed to make sure that the SLAs, as established, are meeting the intent of the Government, and that the Contractor is being asked to perform at a level for which the Contractor has control over the outcomes embodied in the SLA.

The Government acknowledges that the recoverability requirements established in the Service Level Agreements do not apply to the Science and Technology's Local Area Network since adequate redundancy capabilities do not currently exist; in the event such redundancy is created during the performance period of the contract, the SLA recoverability requirements will apply;

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 139
-----------------	------------------------------------	--	---------------

C.6.4. Performance “Work Packages” (The WBS)

The Government's requirements to support the DHS HQ have been organized into the following WBS-oriented “work packages” and include the following areas:

- Program Management Services
- Engineering Operations (Including Laboratory Services)
- End-User Services
- Application Services
- Security Services
- Asset Inventory Management

Each of these “Work Packages” is discussed in more detail below; the details of each WBS are provided in Appendices A-F.

For each WBS element or sub-element, Unisys provided the following:

- Tasks that the Contractor has determined are needed to address each WBS element or sub-element (whether to be accomplished by the Contractor or a subcontractor);
- All labor categories required to accomplish each task; if multiple labor categories are needed, identify each category associated with that task; provide skill-level qualifications for the labor category or categories, and level of effort needed for each labor category to accomplish each task;
- A Contract Line Item Number (CLIN) for each separately orderable work package;
- Labor category or categories and skill-level qualifications and level of effort needed by CLIN;
- Provide cost information by task, then by labor category, then by skill level.

C.6.4.1. Program Management Services

(A detailed Work Breakdown Structure for this Performance Area is included in Appendix A)

The Unisys PMO will provide oversight for reporting of inventory management data. Unisys will apprise the DHS of weekly inventory levels; Unisys and the DHS will cooperate to reach agreement on what this regular and continuing inventory level should be; the DHS will promptly notify Unisys of any impending mission changes that could significantly affect current inventory levels; Unisys will not be responsible for any SLA performance requirements that depend on the availability of new inventory levels resulting from new mission requirements;

The Government views the Program Management Services function within the Contractor's organization as the top-level management function that maintains an enterprise view of all Contractor information technology services and support, and integrates all components of the WBS “work packages” where supporting and integrating services are needed.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 140
-----------------	------------------------------------	--	---------------

For example, in Engineering Operations where Engineering Technical managers perform technical project oversight of DHS project work, the Contractor's PMO would provide project managers on the business side to support those projects.

In the case of program and project planning activities, the Government envisions the Contractor's PMO as monitoring and guiding, as necessary, those Contractor activities occurring in support of the several planning activities such as, business management, security management, and Service Level Agreement management.

The role of the PMO is to provide management oversight and guidance to operations activities. The Contractor's PMO staff shall coordinate and cooperate with the Government's PMO function to make sure that Contractor's PMO is actively contributing to the Government's desire to have an "integrated" PMO team.

The Contractor is to provide a fully integrated team experienced in required disciplines and skill sets, including contract management, project and program management, IT management, internal controls, program control, , and security management needed to execute these objectives of the Program. Other disciplines such as disaster recovery, contingency planning and business continuity will be addressed via a separate Task Order or Delivery Order. The Contractor shall provide to the Government a comprehensive Program Management Plan within 45 business days of contract award.

The Contractor shall provide a Monthly Program Status Report to the Government detailing the following factors:

- Overall Program health;
- Financial condition (Monthly Funds Status Report, Obligated Funding Report, Monthly Invoice Summary Report, Cost Performance Report);
- Performance issues;
- Current issues requiring management's attention;
- Program risks and issues;
- Customer relationship management issues;
- DHS issues affecting the Contractor's ability to perform; and,
- Any other significant issues relating to the success of the Program.
- The Engineering Operations Director and Chief Architect are moved to WBS 2.0; the Security Director is moved to WBS 5.0;
- Executive oversight staff are approved as follows:
 - Deputy Program Executive;

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 141
-----------------	------------------------------------	--	---------------

- Administrative support
- PMO staff are approved as follows:
 - One PMO Director;
 - Three project managers;
 - One Performance Manager;
 - One Quality Assurance Manager;
- The Business Management staff is approved as fixed price.

C.6.4.1.1. Key Integration Functions of the PMO

The Contractor is expected to provide the following types of support:

- Deployment Project Management – In this role, the PMO is expected to make sure that all current and planned projects are properly staffed with skilled project managers, and are planned and executed using industry best principles and practices for project and program management.
 - The Contractor’s PMO project managers will, assume an end-to-end responsibility for project planning, execution, and control, from project inception to completion, for all contractor activities.
 - The Contractor shall provide complete project management oversight of infrastructure build-out and other deployment projects.
 - The PMO will proactively support technical projects from a business perspective. The response must be in a project management plan that addresses, as a minimum, the following elements:
 - How the PMO will provide oversight to technical projects, and how PMO project managers will interact with EO technical leads,
 - How project information will be reported to the Government.
 - How the PMO will ensure best practices are implemented, documented, and reported at a minimum (see DHS Management Directive 0782 and Management Directive 1400) Communication planning is to occur at the project level.
- Unisys agrees that it will assign the required complement of staff with needed skill sets to each project it manages for the DHS (e.g., team membership and level of effort).

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 142
-----------------	------------------------------------	--	---------------

- Unisys agrees that it will make every effort to establish and implement those project management processes the customer defines as necessary for successful completion of the project (e.g., change control, issues management, risk management, etc.).
- Unisys will make every effort to respond to the customer's requirements on the timeline established by the customer.
- Unisys will provide quality audits of project management activities to the fullest extent possible based on the approved quality assurance and quality control resource.
- Unisys will provide timely input to the customer on key findings of quality assurance and quality control assessments.
- Business Operations – The business operations role includes management of all financial issues affecting support to the Government including:
 - Creation of financial and other business management reports as shown in the WBS 1.1.3 and the Table of Deliverables(e.g., ETC report, TTO/TTR report, and DD250)
 - Overseeing the Contractor's response to Government requests for data
 - Provide data in support of Government activities needed to implement the Capital Planning and Investment Control process
- Performance/SLA Management – The PMO will act as the focal point for Performance Management and SLA Management. These duties will include:
 - Making sure that necessary data bases are created to enable collection of data needed for agreed SLAs;
 - Assigning responsibility for collection of data;
 - Creating processes for inputting data into relevant data bases to enable analysis of SLAs;
 - Preparing presentations of SLA results for designated Government management meetings;
 - Assisting in revising SLAs as needed, based on trends revealed during SLA analysis;
 - Identifying to the Government those areas needing improvement, along with appropriate remediation plans;
 - Suggesting new areas where SLAs would be appropriate.
- DHS and Unisys will identify counterparts for O&M, engineering, end-user services, build-outs, security, application services, inventory control, and contracting to address day-to-day issues affecting support of DHS mission requirements.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 143
-----------------	------------------------------------	--	---------------

Notify and seek approval from DHS OIM for significant communications intended for the DHS community to ensure appropriate coordination occurs prior to dissemination;

- Project Planning - The Contractor shall provide a detailed proposal for each requested project. The proposal will outline the scope of work and how the Contractor will provide project management for the task envisioned by DHS HQ. The response must be in a project management plan that addresses, as a minimum, the following elements:
 - A project charter that clearly sets forth the overall goals of the project;
 - A detailed explanation of how the scope of work will be accomplished;
 - An explanation of resources envisioned to accomplish the work;
 - An estimate of the duration of the work, including an optimistic, pessimistic, and most likely projection;
 - Identification of other contractors and agencies needed to accomplish the work that is outside the Contractor's contractual coverage (facilities, wireless, telecom, etc.);
 - An estimate of the budget required to accomplish the work;
 - Any known stakeholders who will be affected by the work (e.g., displaced by build-outs, etc.);
 - Any key dependencies that must be addressed prior to commencement of work;
 - Any essential assumptions that must hold for the work to be successfully completed according to schedule;
 - Any key contingencies that could adversely impact planned effort;
 - The Contractor shall identify risks associated with services implementation, classify them, and provide mitigation plans for identified risks in a manner consistent with industry best practices and task order requirements.
 - Any issues that currently exist, even if from other projects, that could affect planned work;
 - Any critical resources, whether human, capital, or facilities, that must be available prior to commencement of work to enable successful completion;
 - Any known political issues or other factors that need to be addressed prior to commencement of work;
 - A communications plan for each business owner, key stakeholder, or other "interested parties" that identifies what will be communicated, when it will be communicated, the means by which it will be communicated, and the responsible party for gathering the required information and disseminating it;
 - A detailed method that will be used to provide project status;

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 144
-----------------	------------------------------------	--	---------------

- The performance measures that will be used to track project performance, and how they will be used in the performance measurement “roll-up” of all projects into a dashboard or similar reporting structure; and,
- A Microsoft Project Plan (or equivalent) that details task durations, task sequence, task interdependencies, and critical path or paths for the project.

C.6.4.1.2. Program Management Office Structure

The PMO shall provide guidance and oversight for all information technology-related projects and product offerings; PMO reporting must enable visibility into what each component is spending for IT services; additionally, the PMO must work with DHS to establish industry standard IT project management practices, methods and tools, all designed to enable the following:

- Increase project success rates as measured by schedule, budget, and customer and stakeholder satisfaction;
- Centralized visibility of project status, and risk and issues management
- Centralized visibility into project costs (see Project Cost Reporting in the WBS breakout)
- Increase coordination of resource management within and across projects

C.6.4.1.3. Government Property Report

The Contractor shall submit a Government Property Report using Department of Homeland Security Form 700-5 (7/03). The report shall be submitted annually and not later than 15 September of each calendar year.

Government property is defined as property in possession and control of the Contractor.

C.6.4.1.4. Seat Management

This contract includes a combination of Time and Materials, Fixed-Price, and managed services efforts with varying levels of support to be provided for different types of “Seats.” A seat may consist of services (with or without equipment) ranging from an end-user seat (desktop, laptop, etc.) to an infrastructure seat (router, switch, server, etc.).

The level of seat managed service support requirements will vary depending upon seat functionality which may include maintenance, COTS software, help desk services, trouble resolution, asset inventory management, security management, network maintenance, planning, system engineering, provisioning and billing.

All services seats, as defined in this Performance Work Statement, shall be provided by the Contractor and included in the managed services seat CLIN price for each seat type. The “Seat CLIN” price shall be distinct from any corresponding “Product CLIN” price.

Seat Management services may be acquired via the following options:

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 145
-----------------	------------------------------------	--	---------------

- Managed services for Government Furnished Equipment (GFE) within original “warranty” period, e.g., first 36-months, when this CLIN is ordered
- Managed services for (GFE) beyond original warranty period when this CLIN is ordered and,
- The outright purchase of product as Government property or Government Furnished Equipment.

Delivery of seat management services will be evaluated using a variety of performance factors included in Service Level Agreements in Appendix H.

C.6.4.2. Engineering Operations

- The position shown for DHS-052, ProSight Infrastructure Support, Systems Engineer, is deleted since this effort was moved to Applications Services, WBS 4.0;
- The Government reserves the option to directly obtain the EMC staff resource and Microsoft Premier Support and, in turn, provide these to Unisys at the agreed level of effort; Unisys will include these two items in its price proposal as separately-orderable CLINS;
- Thirty-eight FTEs are approved (see Table below) to address O&M which includes base, contingency, and build-out projects; of those positions, the 1 EMC staff resource has been included and the Engineering Operations Director, the Chief Architect, and the resources identified in SR40088 and SR50076 have also been included;
- Security-related projects will be funded via separate Working Capital Funded Task Order or Delivery Orders; Unisys’ proposal for Engineering Operations shall account for work and analysis performed under the Security Services WBS 5.0;
- DHS OneNet and ADEX will be addressed via a separate ITO-funded Task Order or Delivery Order;
- Production Engineering will re-align resources to make sure that DHS receives 24 X 7 coverage;
- For the agreed upon set of tools, the Government retains the option to order the tools from Unisys, or to provide them as GFE;
- Up/Down Status should be based on an analysis of all available data sources; local logs take precedence over remote logs;
- Devices and applications (including interfaces) introduced into the network must go through the ERG process; in exigent situations, the Government reserves the right to waive that process and relieve Unisys of any associated SLA requirement; in the event the Government chooses to require Unisys to manage any such device or application, the Government will order the appropriate managed services CLIN;
- If the Government elects to obtain the Contractor’s proposed monitoring tool sets, Unisys shall provide the Government monitoring status and details when requested;

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 146
-----------------	------------------------------------	--	---------------

- For Upgrades, New Releases, both parties agree to the following definitions:
 - An Update is a patch or other interim "fix" provided to licensees of a particular version of software and/or hardware, at no additional charge, so long as the update has a valid license, and a current maintenance or support service agreement from the software and/or hardware manufacturer; Updates and patches are "unplanned" and usually address potentially harmful or disruptive conditions and, for this reason, should be addressed as quickly as possible and coordinated with the Government prior to installation and roll-out so that critical systems are addressed first, and so that disruptions are minimized.
 - Upgrades or Releases are versions or releases of the software and/or hardware that require a new license agreement and payment of a new license fee; These can be dealt with as "planned" events and should be coordinated with the Government and scheduled so as to minimize disruption, interference, etc., with normal operations.
- Unisys shall manage the approved images on those devices managed by Unisys;
- The DHS OCIO will provide guidance on priorities; will recognize and accept reasonable resource constraints; and will facilitate the necessary scheduling or rescheduling of engineering efforts for projects and or activities under the Engineering FPLOE CLIN to make sure that DHS OCIO and Unisys can successfully deliver on the respective projects. Unisys will re-align such project priorities in accordance with guidance provided by the DHS OCIO, and will provide the DHS OCIO with ramifications of the re-alignment or re-prioritization. The DHS OCIO and Unisys will collectively agree as to what the acceptable impacts are to the Unisys ITMS/DHS OCIO project list. These impacts may include rescheduling of projects and or removal of projects from the list. When projects are rescheduled or reprioritized, DHS OCIO will not hold Unisys accountable for those projects that do not get completed by the original proposed date;
- If the DHS OCIO is unable to reprioritize the Unisys ITMS/DHS OCIO project list to address conflicting schedules, or if DHS requests projects that are out of scope of the current Contract, Unisys reserves the right to present to DHS OCIO, any staff augmentation proposals necessary to continue the successful completion of these projects;
- DHS will provide approval for program plans, designs, Task Orders, purchase requests, and Delivery Orders as specified by the DHS specified timeline. Unisys shall provide the documentation necessary for submission to the ERG which has ultimate responsibility for approval of the project;

Unisys is responsible for the SBU network availability up to the DHS Metro or Wide Area Connection and connection port to the Internet Service Provider (ISP); Unisys is not responsible for Wide Area Network performance or availability unless the Government has contracted with Unisys to provide the service;

- DHS will provide a minimum 30-day advanced notification of new facilities that are planned for build-out;

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 147
-----------------	------------------------------------	--	---------------

- In relation to specific projects, any request made for service delivery within the 30-day planning window shall be considered a "special project" and may incur fees for expedited "special" services;

C.6.4.2.1. The following set of "Other Direct Costs" and Monitoring Tools are approved for the bridge contract effort. The Government reserves the right to provide these tools to the Contractor, or require the Contractor to provide these tools under licensing agreement with vendors.

WBS	ODC Name	Total
2.1.3.1	146GB Hard Drive, Ultra 320 SCSI, 15K RPM, 80 pin PowerVault, Customer Install. 3 required in each server	
	146GB Hard Drive, Ultra 320 SCSI, 15K RPM, 80 pin Power Vault, Customer Install. 3 required in each server-2	
	AppManager 6.0 Dell OpenManage	
	AppManager 6.0 for Microsoft Exchange Server	
	AppManager 6.0 Microsoft Active Directory	
	AppManager 6.0 Microsoft Cluster Service (MSCS)	
	AppManager 6.0 Microsoft Internet Information Server	
	AppManager 6.0 Microsoft SQL Server	
	AppManager 6.0 Microsoft Terminal Service	
	AppManager 6.0 Network Devices	
	AppManager 6.0 Operator Console/Control Center	
	AppManager 6.0 Oracle RDBMS	
	AppManager 6.0 Response Time for Active Directory (10 pack)	
	AppManager 6.0 Response Time for Exchange (10 pack)	
	AppManager 6.0 Response Time for Networks	
	AppManager 6.0 Response Time for Web	
	AppManager 6.0 RIM Blackberry Enterprise Server	
	AppManager 6.0 SNMP Toolkit	
	AppManager 6.0 Veritas NetBackup	
	AppManager 6.0 Web Access Console (5 concurrent connections)	
	Base Agent for Microsoft Windows 2000 Advanced Server / Enterprise Server 2003	
	Base Agent for Microsoft Windows NT Workstation/2000/XP Professional	
	Base Unit 3.4GHz/2MB Cache, Xeon 800 MHz Front Side Bus for PowerEdge 2850 and associated components	
	Base Unit 3.66GHz/1MB Cache, Xeon Redundant, Power Edge 6850 and associated components	
	Full User Cost Unisys Quest Management Suite for AD & Events	
	NETIQ Annual Maintenance	
	Prepaid On site services and implementation for Products (includes Travel and Expenses set not to exceed this amount	
	Product Implementation services/day by NetIQ	
	Quest Exchange Management Suite	
2.2.2.1	Client Mgt. Suite Level 1 - No Carbon Copy	
2.2.3.1	LMS 2.5 Large Ent WIN/SQL Dev UnRestricted - Rev May 05	
	Cisco Secure ACS 3.3 Solution: includes H/W and SW	

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 148
-----------------	------------------------------------	--	---------------

	Four -Port HDX or Two-Port FDX FE Probe, High Capacity Gigabit GBIC PHY for Snifferbook Ultra Gigabit GBIC SX transceiver kit SMARTNET 8X5XNBD Cisco Secure ACS 3.3 Sniffer Portable Field Services Suite Sniffer Portable Field Services Suite - 1 yr SW Core Spt SnifferBook Ultra Base Unit VMS 2.3 WIN/SQL Unrestricted	
2.3.1.1	Off-site Storage for DOE & NAC sites Off-site Storage-Ashburn & Vermont Tape Media for DOE & NAC sites Tape Media-Ashburn & Vermont sites	
2.3.3	BlackBerry Enterprise Solution T-Support TX2 / Device Fee (1-99) - Base Rate BlackBerry Enterprise Solution T-Support TX2 Per Server Fee Hyena 10-Admin Enterprise Edition - 2yr Maintenance Hyena 10-Admin Enterprise Edition License	
Total		

(A detailed Work Breakdown Structure for this Performance Area is included in Appendix B)

Availability of Qualified O&M Personnel and DHS-approved Maintenance Downtime
Successful operation requires a dedicated team of experts to ensure that necessary maintenance procedures are routinely followed. The Contractor shall provide DHS 7x24x365 coverage. The Contractor shall provide near-site support, in conjunction with the Network Control Center (NCC) and the Single Point of Contact (SPOC) personnel, and will make every reasonable attempt to identify trends and emerging issues for resolution before they become serious outages.

C.6.4.2.2. On-Site Engineering Support

- Labor Categories and Staffing Costs – Engineering and Operations
 - Staffing costs within the Engineering Operations WBS are to be reduced via attrition using one of the following options (positions to be reduced shall not exceed 15 total positions):
 - Option 1 – Fill vacant staff position with labor category at least one level below the current level, e.g., when an SE V leaves, replace with an SE IV, etc.;
 - Option 2 – Fill vacant staff position with a skill set within another labor category at a cost equal to or less than the cost that the Government would incur if the position were filled using Option 1, e.g., when an SE III leaves, replace with a Systems Administrator Level IV;
 - The Government may waive this requirement for any position.
 - The DHS will execute a contract modification to adjust the FPLOE price based on changes in labor categories.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 149
-----------------	------------------------------------	--	---------------

- The Engineering Operations Director position and the Chief Architect position are moved from WBS 1.0 to WBS 2.0.
- Engineering Operations LCATS and LOE:

	SE I	SA IV	SE III	SE IV	SE V	SE VI	SE VII	NE III	NE IV	NE V	NE VI	NA III	NA IV	Proj/Task Mgr II	Proj/Task Mgr III	Practice Prog Mgr V
TOTAL	1	1	1	10	8	5.25	.25	1.5	1	1	2	1	1	1	1	1

Total FTEs 38

Legend:

SE -Systems Engineer

NA-Network Administrator

NE -Network Engineer

PM –Project Manager

1.5 of the 8 SE V positions is to accomplish the effort in SR 40088 for S&T Computing Center.

Staffing includes support for the Email Remediation for the DOE to Ashburn relocation effort covered by SR-50076.

- Tools – The Government's options for providing system monitoring tools include:
 - Option One – The Government will order from Unisys approved tools via licensing arrangements with vendors on a “usage” basis, i.e., when the license period expires, DHS will need to re-procure the tool license;
 - Option Two – The Government will order from Unisys approved tools via licenses that will transfer to the DHS if and when so desired by the DHS;
 - Option Three – The Government will procure approved tools and provide them to Unisys as Government Furnished Property/Equipment.
 - Unisys will provide cost and pricing information for these options at which time the Government will select the option it determines to be most advantageous to the Government.
- Approved tools and ODCs are shown above in a separate table.
- The Government reserves the right to provide the required tape media as GFE.
- Unisys must maintain and update the configuration documentation and “gold image” of equipment they manage.
- Corrective and Preventive Maintenance. Such maintenance will be in accordance with manufacturer recommendations and contract SLA requirements. In the event that a DHS priority impedes the performance of such maintenance activities, a time equal to the duration of the delay will be subtracted from the applicable SLA measurement.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 150
-----------------	------------------------------------	--	---------------

- The Government will ensure that the appropriate software licenses provided to Unisys for deployment and management will include full software assurance for those software packages that the Government requires Unisys to maintain with patches and upgrades.

Unisys must advise the Government of the changes in products that will be used to fulfill a CLIN requirement.

The Contractor shall propose an engineering team that will continue to deliver the following mission-critical services for DHS:

- Immediate response (within 2 hour) to all 3rd/4th level system or network engineering issues upon notification by DHS security, the SPOC, or any customer reporting a verified problem. These include the following customer-based services:
 - On-call services 24x7x365
 - All server/network performance/response time issues, service interruption/outages
 - Tracking and reporting on suspicious e-mails, spamming, and spoofing
- Design, engineering, configuration and implementation of approved changes, projects, and site build-outs as agreed to by the DHS OCIO and identified in the project list. These include the following customer-based services:
 - Engineering support for all new site build-outs and department moves
 - Oversight of all Sensitive but Unclassified (SBU) network, server and operations growth plans
 - New infrastructure design and user rollout support including testing, clearing, packaging, and installing customer hardware on the DHS workstation image
- Response to all Data Center issues and maintenance to include the following customer-based services:
 - Monitoring event alarm response and troubleshooting
 - General health of servers, Storage Array Network (SAN), and network components
 - Monitor network for all server and network service interruptions/outages and perform troubleshooting and repair
- Response to all 2nd/3rd level systems or network administration issues to include the following customer-based services:
 - Account management (adds, changes, deletions)
 - End-user e-mail account issues and configuration
 - Blackberry account setup and troubleshooting

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 151
-----------------	------------------------------------	--	---------------

C.6.4.2.3. Laboratory Services will be provided as follows:

- The method of obtaining Laboratory Services set forth in C-6 is hereby modified to enable the DHS to obtain testing on a case-by-case basis; testing requirements identified in C.6.4.4 will also be addressed viaa separate Task Order or Delivery Order;
 - O&M testing requirements within Engineering and Operations will also be handled separately;
 - Testing for new requirements (hardware and software) will be handled viaa separate Task Order or Delivery Order;
 - The Government expects Unisys to accomplish due diligence (requirement 1), as determined by the DHS formal change control process, and have a "back-out" plan (requirement 2);
 - If the Government elects to waive testing, Unisys will not be held responsible for any SLA failure associated with the specific installation as long as Unisys met requirements 1 and 2 above;
 - If the Government tasks Unisys to perform testing, Unisys will be held responsible for any SLA failure associated with the specific installation;
 - Unisys will maintain a "Gold" image for every configuration in the DHS environment for which Unisys has responsibility to support.
- The Contractor shall propose a dedicated on-site engineering team to provide the services described above, to support projects (e.g., new architecture/infrastructure designs, new deployments of network/systems, etc.), and to provide operation and maintenance activities (maintenance of infrastructure, maintain stability of environment, monitoring, ticket resolution, etc.). The team shall be structured and staffed based on the current needs.

C.6.4.2.4. Technical Services Management

The focus of the Engineering and Operations Group is divided into two Technical Service areas:

- Operations and Maintenance (O&M) and
- Project Engineering

Respective service responsibilities are:

Operations and Maintenance:

- Immediate response to all 3rd/4th level system or network engineering issues upon notification from The Contractor shall monitoring, DHS security, the SPOC, or any customer reporting a verified problem. These include the following customer-based services:

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 152
-----------------	------------------------------------	--	---------------

- On call services 24x7x365
- All server/network performance/response time issues, service interruption/outages
- Tracking and reporting on suspicious e-mails, spamming, and spoofing
- Response to all Data Center issues and maintenance to include the following customer-based services:
 - Monitoring event alarm response and troubleshooting
 - Preventative maintenance General health and of the servers, SAN, and network components
 - Monitoring of network for all server and network service interruptions/outages and perform troubleshooting and repair
- Response to all 2nd/3rd level systems or network administration issues to include the following customer-based services:
 - Account management (adds, changes, deletions)
 - End-user e-mail account issues and configuration
 - "Blackberry" account setup and troubleshooting

Project Engineering

- Proactive design, engineering, configuration and implementation of approved changes, projects and site build-outs. These include the following customer-based services:
 - Engineering support for all new site build-outs and department moves
 - Oversight of all SBU network, server and operations engineering growth plans, including:
 - E-mail and messaging services
 - File share services
 - Active directory services
 - Storage area network services
 - Backup and archive technologies
 - Blackberry and wireless technologies
 - Management, configuration and utility servers
 - Network configuration and planning

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 153
-----------------	------------------------------------	--	---------------

- Client platform designs including software images and hardware configurations
- New infrastructure designs and user rollout support
- Network and server enhancements based on recommended best practices, and technical assessments

Table 3.1 – Task Descriptions Associated with Typical Projects in Engineering and Operations

The Infrastructure & Deployment Projects encompass the projects that Unisys will perform to implement technology or deliver infrastructure and connectivity services. The efforts of the infrastructure engineering team will require close management and coordination to ensure efforts are appropriately prioritized to meet the demands of DHS. Unisys will work closely with the DHS HQ Engineering Review Group/CAG, NCR Infrastructure Director(s), and other DHS Executive Staff, as required, to manage these efforts. Unisys recognizes that the DHS list of projects and their associated priorities is likely to change and will work closely with the OCIO and PMO to manage this process. One step in the process will include a regular project review with DHS to discuss status, priorities, revisions to the project list, and schedules. Unisys will complete each project based on agreed-upon schedules and scope. Unisys will also provide advance notice to DHS and discuss alternatives if project staffing shortages or schedule conflicts affect the on-time completion of a project. **Table 3.1** provides the known projects at the time this contract was awarded.

Project Name	Objectives
– Email Scalability Phase III – Replacement Site for Primary	<ul style="list-style-type: none"> • “Metro-Core” • Swing space for Primary move • Potential new home for DHS.GOV, DHSONLINE, etc. • Transition to Enterprise Backup and Archive
– Email Scalability Phase IV – Final Environment	<ul style="list-style-type: none"> • Standup of additional sites on Metro Area Network (MAN) to provide continuity of service • Potential new home for DHS.GOV, DHSONLINE, etc. • Standup of Remote site (Site “R”) that will provide Disaster Recovery (DR) and Continuity of Operations (COOP) • Implementation of new/replacement technologies more consistent with enterprise solutions, specifically the determination of resource/system recovery management.
– Relocation of secondary HSOC systems at the NAC to Site A	<ul style="list-style-type: none"> • Extended DR capability for the CNC domain
– Improve Security Services for Public Facing Mail Services	<ul style="list-style-type: none"> • Evaluate system alternative to the use of public facing Outlook Web Access services – to include decommissioning of the existing services
– S&T DR to Ashburn	<ul style="list-style-type: none"> • Develop plan to use Ashburn as S&T disaster recovery site
– Extend DHSNet services to Regions	<ul style="list-style-type: none"> • Determine network package to support up to 10 remote sites • Determine appropriate VPN level services or equivalent for secure connection from remote site to DHSNet core services
– Extend DHSNet	<ul style="list-style-type: none"> • Determine network package to support up to 10 remote sites. This

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 154
-----------------	------------------------------------	--	---------------

Project Name	Objectives
services to National Labs	would include, at least: EML, Plum Island, Sandia, PNNL, LLL, etc. <ul style="list-style-type: none"> • Determine appropriate VPN level services or equivalent for secure connection from remote site to DHSNet core services
- NAC Building 19 LAN A Support	<ul style="list-style-type: none"> • This involves the contractor accepting the transition of LAN A network and server support within Building 19 at the Nebraska Avenue Complex, from Northrop Grumman, according to a finalized and mutually agreed-upon transition plan. • This is also based on the approval and execution of requirements listed within the Assumptions section of this document.
- Data Archiving	<ul style="list-style-type: none"> • Deploy at the major data Center (Ashburn) the ability to move old and/or little used email and files to alternative (lower cost) storage as well as meeting the file retention and compliance requirements for these systems.
- Nebraska Avenue Complex, Buildings 1, 2, 17, 43, 100	<ul style="list-style-type: none"> • Provide build-out and O&M of the SBU network for Buildings 1, 2, 17, 43, and 100 – all floors. • Integrate the infrastructure of these buildings with the DHS enterprise architecture. • Provide all end-user equipment for LAN A.
- Glebe Road Facility (finalizing)	<ul style="list-style-type: none"> • Provide LAN connectivity through access and redundant core switches to five floors at 1110 N. Glebe Road for IAIP. • Provide for up to 600 computers (laptops and desktops) and the associated printers, fax, and copiers in accepted ratios. • Provide operations and maintenance support for LAN A network infrastructure and user equipment.
- Member Server upgrade to Windows 2003 (finalizing)	<ul style="list-style-type: none"> • Upgrade all member servers to Windows 2003 Server Enterprise Edition due to the increased security and stability of Windows 2003 Server released by Microsoft. This upgrade provides DHS with the latest Microsoft technology and better access to the support facilities Microsoft provides. • This project includes upgrades to the operating system only, and does not specifically include upgrades to applications or services that may reside on any specific member server.
- PKI/Smartcard Initiative	<ul style="list-style-type: none"> • A Desfire ISO 1443-G proximity chip to facilitate the purchase and use of new physical security access controls. • Three digital certificates to be located on a contact chip embedded on the card. These chips would provide the user a digital signature certificate, an identity certificate, and an encryption certificate. These certificates provide for the following: users can use the card to authenticate to the network either locally or remotely using on their card, eliminating the need for standard username and password credentials; users can digitally sign and encrypt their emails; users can securely access sensitive web sites that have been enabled to inspect their certificates. • This effort has yielded a pilot program to install the required technology into the existing DHS infrastructure. With the maturation of this pilot, this program is beginning preparations to move into a production mode. Currently, the • Infrastructure for this project is located at the Vermont Ave. facility, but

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 155
-----------------	------------------------------------	--	---------------

Project Name	Objectives
	will need to move to another facility by the end of first quarter 2005.
– DHS Metro Area Network Integration into OneNet	<ul style="list-style-type: none"> • This initiative has been picked up by the DHS ITO which has approved a Metro Area Network Initiative to utilize cost and performance effective metropolitan area network solutions to reduce the number and cost of traditional telco data services like T1/DS1s and T3/DS3s and OneNet RackPacks. The consolidation of this impacts all DHS/HQ main sites: NAC, DOE, 7th&D, VT Ave., as well as smaller sites like Ft. Dietrick. • The ITO and OCIO are responsible for the costs and direction and the contractor is responsible for the appropriate design and deployment of the MAN network infrastructure, as well as providing ongoing operational and engineering support. • Phase I – SLGCP & VT ave • Phase II – NAC, Ashburn, Glebe, and 7th & D • Phase III – Tail sites (i.e., NY Ave)
– Network Port Security using 802.1x	<ul style="list-style-type: none"> • Directive from CISO to implement port security. The contractor shall plan for and use the industry standard 802.1x Port Authentication & Authorization. This technology will permit DHS the ability to control access to the DHS network via a user and/or host-based authentication. It will also allow for finer granularity and control, as necessary, of access to DHS network services.
– DHS OneNet Integration	<ul style="list-style-type: none"> • Directive from ITO to support the phased implementation of the DHS OneNet. DHS ITO has approved the DCN upgrade from the ATM/Frame architecture to the new MPLS/VPN solution. The first phase is the upgrading of the existing layers 1 and 2, which will require the integration, migration, and testing of the new MPLS solution. Additional phases will require similar efforts. This impacts all DHS/HQ main sites: NAC, DOE, 7th&D, VT Ave., as well as smaller sites like Ft. Dietrick. • Phase 1 – Transition from ATM/Frame Relay to IP/MPLS Complete • Phase 2a – Components internal networks migrated to IP/MPLS • Phase 2b – Implementation of Network Switching Nodes
– DHS DCN RackPack Split – NAC Facility	<ul style="list-style-type: none"> • Directive from OIM/DC Metro Infrastructure Director. To ensure the highest levels of network availability, the contractor shall work with the DCN engineering team to split the redundant DCN Rackpacks that are currently co-located in the same rack, to physically diverse buildings. This will ensure that physical service interruptions that impact a single building will not impact other buildings. This is in line with the ITO Network design for the OneNet.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 156
-----------------	------------------------------------	--	---------------

Project Name	Objectives
– SLA Management – End User Performance	<ul style="list-style-type: none"> Desired by DHS OCIO, the need to measure performance of services from an end user perspective. The contractor shall design, procure, and implement a set of SLA management tools (systems and software) to measure end user performance and underlying systems and network elements as related to and impacting end-user performance.
– Improved Account Provisioning	<ul style="list-style-type: none"> For operational efficiency, this would include the incorporation of automated utilities to streamline the process and to ensure security and procedural compliance during the account creation and modification process.
– Enhanced Distribution List and File Share Membership Provisioning	<ul style="list-style-type: none"> For operational efficiency and customer satisfaction, this would include implementation of automated tools to allow for enhanced operator and user control over distribution lists and file share memberships.
– Enhanced Desktop Image Protection	<ul style="list-style-type: none"> Incorporating Anti-Spyware, Anti-SPAM, Firewall, and other security and integrity protection tools.
– Mobile Device Security	<ul style="list-style-type: none"> Leveraging/implementing encryption technology, day-zero protection, and other capabilities to protect mobile devices such as laptops and Blackberry handsets.
– Network Admission Control	<ul style="list-style-type: none"> To prevent day-zero viruses from infecting the network Enhanced security protection to prevent unauthorized and unprotected workstations and laptops from connecting to the network.
– ADEX Integration	<ul style="list-style-type: none"> Integration of ADEX initiatives such as MIIS and other ITO project requirements
– Extranet Deployment and Integration	<ul style="list-style-type: none"> Integration of FTP Proxy, OWA services, Firewall Exception Exit Point, and other Extranet/DMZ capabilities in direct support of mission critical services required by HSOC and IA, and mission support services required by CFO, OCHO.

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 157
-----------------	------------------------------------	--	---------------

Project Name	Objectives
- Mantech IAIP Application Support	In support of IAIP scheduled initiatives
- SAMS Deployment and Hosting	<ul style="list-style-type: none"> Extend LAN A into Battelle ADC space to allow for DHS HQ connectivity to SunFlower application
- SMS Deployment and Hosting	<ul style="list-style-type: none"> Provide engineering support and high level design work for S&T Staffing Management System Provide oversight to ensure S&T compliance with DHS EA and TRM Procure and manage LAN A equipment
- NAC Building 19 1 st and 2 nd Floors	<ul style="list-style-type: none"> Provide build-out and O&M of SBU network in SCIF space of building 19, floors 1 and 2 Integrate the infrastructure on floors 1 and 2 with the DHS enterprise architecture Provide end-user equipment for 350 users
- NAC Building 7 room 007	<ul style="list-style-type: none"> Provide build-out and O&M of SBU network in building 7, room 007 for Security Integrate the infrastructure with the DHS enterprise architecture Provide end-user equipment for LAN A
- NAC Building 18 1 st floor	<ul style="list-style-type: none"> Provide build-out and O&M of SBU network in building 18, 1st floor Integrate the infrastructure with the DHS enterprise architecture Provide end-user equipment for LAN A
- Sigaba Pilot	<ul style="list-style-type: none"> Provide engineering support in deployment of Sigaba product to enhance vertical information sharing among various federal agencies, local governments, and first responders
- NY Ave Training Room	<ul style="list-style-type: none"> Provide build-out and O&M of SBU network for training room Integrate infrastructure with DHS enterprise architecture Provide end-user equipment for LAN A Provide security and software evaluation of special package SynchronEyes for classroom training tools Provide security and software evaluation of Group Systems collaboration tool
- CHCO SQL server	<ul style="list-style-type: none"> Design and implement an interim reporting solution for CHCO because current solution is at capacity Provide LAN A equipment to support this effort Provide multiple instances on enterprise SQL server
- SLGCP – FEMA connection	<ul style="list-style-type: none"> Provide engineering and design work to allow SLGCP employees remote access to their DHS HQ network resources while in location under control of FEMA Provide LAN A equipment
- NAC Building 59	<ul style="list-style-type: none"> Provide build-out and O&M of SBU network in building 59 Integrate the infrastructure with the DHS enterprise architecture Provide end-user equipment for LAN A
- Prosight Remediation	<ul style="list-style-type: none"> Provide engineering and design work to connect Prosight natively via DCN Eliminate Gold domain and have all users authenticate against DHSNET Upgrade Prosight application to 5.0 version

Contract	Document No. HSTS03-06-D-CIO500	Document Title ITMS Bridge Contract	Page # 161
-----------------	------------------------------------	--	---------------

Security			Jan	Feb	Mar	Apr	May	June	July	Aug	Sep	Nov	Dec	Size
EOT Projects	<i>Benefit</i>	<i>Category</i>												
<i>Top Priorities</i>	Benefit	Category	Jan	Feb	Mar	Apr	May	June	July	Aug	Sep	Nov	Dec	
Sigaba Pilot	OIM	Security	█	█										M -> S
Sigaba Phase II	OIM	Security				█	█	█	█					L
Application Domain	OIM	Security	█	█	█									M
Network Admission Control	OIM	Security				█	█	█	█	█	█			XL
Enhanced Desktop Image Protection	OIM	Security				█	█	█	█	█	█	█	█	XL
													Total	
													Per Eng #	
													FTE Eng	

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	162

C.6.4.3. End User Services

(A detailed Work Breakdown Structure for this Performance Area is included in Appendix C)

The objective of End User Services is to provide all DHS HQ with Tier 1, Tier 2, and Tier 3 support.

C.6.4.3.1 Help Desk Services (SPOC) – Tier 1 Support Team

The objective of these Help Desk services is to provide all DHS HQ with Tier 1 service. The Help Desk Service Level Agreement is included in Appendix H.

The DHS HQ requires a single point of contact (SPOC) to act as the primary interface to the thousands of end users of various COTS and custom-developed applications. This service can take the form of, but is not limited to, answering questions concerning problem resolution for DHS HQ standard COTS and some specialized applications for its end users.

Additionally, the Contractor is expected to coordinate the transfer of information from Tier 1 to Tier 2 and Tier 3 services, some of which will be provided by the Contractor, the DHS HQ and various 3rd party contractors and Original Equipment Manufactures (OEMs). Supporting DHS HQ user requires the ability, on the part of the Contractor, to take customer calls, log the call into the helpdesk database, analyze the call, resolve the problem or assign the problem to another helpdesk technician and log the resolution in the helpdesk's knowledge base.

The Government may choose to review Unisys' SPOC policies and procedures on a mutually agreeable schedule. Procedures for the management of DHS end user requests will be in accordance with Contract requirements as mutually agreed between Unisys and DHS. Unisys will retain the final authority on any changes to its policies and procedures so long as a suitable solution is implemented.

The DHS HQ expects timely, courteous and competent responses by the Contractor to end-user problems.

Any Help Desk requests for a move shall not be acted on without Government approval and will be referred to the appropriate Government Facilities POC, for processing.

The Contractor will provide basic helpdesk operations that include Tier 1 call center support, Network Systems Monitoring, Tier 2 support including remote desktop management for COTS/GOTS applications and operate and maintain the interface with other Tier 2 and Tier 3 support organizations.

The Contractor will maintain a SPOC for all systems for end users to obtain resolution of IT problems and/or technical issues including Tier 1 helpdesk service; continually integrate industry best practices for helpdesk tools and technologies that enhance the productivity of the helpdesk agents, thereby driving down helpdesk support costs for the DHS HQ;

The Contractor's solution must provide the following features:

- A single point of contact for help desk support (Tier 1) and referral to solution providers (Tier 2 or Tier 3) or third party vendors;
- Ownership of problems from identification to solution/resolution unless specifically stated to the contrary in the PWS;

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 163
---------------------	--------------	--	---------------

- The use of an enterprise management tool for enterprise-wide monitoring and management of the network and systems infrastructure; and,
- Seamless call distribution and call management support.

The helpdesk interface is responsible for operations, problem resolution, and facilitation of Contractor activities to make sure that end users are operationally restored as quickly as possible.

Required services include the following:

- Helpdesk support for Tier 1 requirements
- Interfacing with Tier 2 and Tier 3 support organizations
- Remote Desktop Management
- Reporting trouble call metrics

As necessary, the Contractor will apply automated tools and methodologies in support of these efforts. In addition, the Contractor shall periodically refresh the tools and technologies for providing this support so that the government continues to get best value for its investment.

In accomplishing this Help Desk function the DHS HQ expects the Contractor to provide a comprehensive, state-of-the-art, Single Point of Contact (SPOC) help desk solution that aligns with industry best practices, and that represents the best value to the Department and the Government. This solution must include, as a minimum, the following features:

- Single Point of Contact Level 1 Service Desk for call reception and logging
- End-to-end responsibility and accountability for problem resolution
- Triage calls and perform first level trouble shooting
- Establish resolution groups to include notification, escalation, and referral procedures (e-mail, voice, pager)
- Call and problem management
- Routing and referral to existing Level 2 and Level 3 support providers and third party contractors per defined scripts;
- Visibility into problems referred to Level 2 and 3 resolution groups that are being addressed and escalated per defined service level procedures
- Monthly Level 1 Service Desk performance reports
- Monthly end-user satisfaction report

The Contractor shall provide and support end-user Help Desk services as follows:

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 164
---------------------	--------------	--	---------------

- The Help Desk shall be manned with live telephone coverage 365 days per year including all Federal holidays.
- The Help Desk shall be available to all DHS HQ authorized users through the phone at all times.
- The Contractor shall provide a toll free number for all DHS HQ users throughout the United States.

C.6.4.3.1.1 Tier 1 Role and Responsibilities

The Contractor's SPOC will:

- Provide Tier 1 helpdesk support to all users within the DHS HQ.
 - Provide helpdesk services at the Contractor's facilities, and include a SPOC for desktop support and coordination of computer service needs for all DHS HQ users.
 - Provide a single toll-free phone number, supported with Automatic Call Distributor (ACD) capabilities, for all IT problems.
-
- Staff and maintain helpdesk
 - Set up and maintain a ticket management system; this will include logging of all trouble tickets into a Contractor provisioned, configured, and managed automated trouble-ticket management system that is electronically accessible to DHS HQ staff via the internal LAN or the Internet.
 - Thoroughly document all trouble ticket problems and the steps taken to resolve these problems.
 - Log all trouble ticket resolutions into the helpdesk's knowledge database.
 - Monitor and document all trouble ticket hand off and resolutions.
 - Receive and answer calls
 - Allow trouble ticket generation via 1) phone, 2) electronic form
 - Enable access to the asset inventory database
 - Determine inquiry/problem resolution requirements
 - Resolve inquiry/problem within 15 minutes, if possible, otherwise escalate to appropriate Tier 2 resource
 - Interface and monitor the enterprise management system
 - Track calls at Tier 2 and Tier 3 until resolution; in case of a delay, inform the appropriate DHS HQ personnel

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 165
---------------------	--------------	--	---------------

- Refresh the helpdesk technology and software used to run and manage the helpdesk to the most current versions available
- Answer DHS HQ end user calls from a Contractor provisioned, configured, and managed ACD system.
- Resolve issues over the phone or through the use of remote control software.
- Provide hardware diagnostic procedures on PCs and printers, place hardware trouble calls to the appropriate support organization, and coordinate the replacement of any defective parts.
- Perform basic Network and Systems monitoring using the latest Network Systems Monitoring software.
- Perform any required daily routines such as database backups, database initialization, etc. on Contractor or DHS HQ provided systems, consistent with the latest database management tools.
- Arrange for on-site support as required for problem diagnosis and/or resolution.
- Coordinate warranty issues for all managed assets.
- Provision monthly management and usage reports.
- Perform root cause analysis on systemic issues, recommend solutions or elevate unresolved issues to the appropriate support personnel.
- Track each call received, even if the call was elevated or routed to another support organization (i.e., Tier 2 or 3), to ensure the customer's needs were met unless specifically required by the PWS
- Maintain superior service during fluctuations in the call volumes.

C.6.4.3.2. Desk Side Services (Tier 2)

The Contractor will provide:

On-site knowledge base, troubleshooting, and diagnostic support in response to a SPOC service request to resolve problems and questions that cannot be resolved over the telephone or remotely.

C.6.3.2.1. Tier 2 Role and Responsibilities

The Contractor's Desk Side Services Team will:

Provide on-site Tier 2 support comprised of Secret clearance level specialists who will resolve complex technical problems to include the reconfiguration of laptops, desktops, and troubleshooting of various software- and hardware-related issues. Specialists providing support within a SCIF are required to hold a TS/SCI with appropriate compartments.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 166
---------------------	--------------	--	---------------

In addition to other support duties, the Contractor will assign sufficient staff to the DHS HQ Support Team and DHS HQ specified field locations support Installations, Moves, Adds, and Changes (IMACs).

This team will work on-site at Headquarters during normal business hours 7am - 7pm. Field location and hours of operations will be designated by site.

Support will be provided after hours for other than agreed requirements, on a short-term basis if required to address emergency situations within the constraints of available resources/funding, tasking, and skill requirements

Tier 2 team duties will include the following:

- Knowledge of Tier 1 technician processes and responsibilities;
- Use of the Knowledgebase
- Microsoft Desktop and application configuration
- Network accessory maintenance (printers, file storage, CD burners, etc)
- Minor cable repair as required
- Analog technology support (facsimile, modems, etc.)
- Network user support
- Processes and policies for performing Installations, Moves, Adds and Changes
- "Blackberry" support
- Asset tracking
- VOIP support –e.g., handset installation, and configuration
- Identify problem characteristics and, if possible, root cause
- Resolve inquiry/problem within prescribed time limits, if possible, otherwise escalate to appropriate resource
- Notify the DHS HQ and contract managers as required
- Notify Tier 1 personnel about call status/resolution
- Assist Tier 1 personnel in logging the resolution in knowledge database
- COTS/GOTS Applications support

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	167

- Outline the current hardware configuration of the desktops and laptops being used at the DHS HQ.
- Interface with Tier 2 and Tier 3 Support Organizations

C.6.4.3.1.2. Deployment of Services

The DHS HQ has standardized its desktop and laptops to create a homogeneous desktop environment. The Contractor will provide support to the "trouble ticket" management process. DHS HQ may request optional support on COTS/GOTS that currently are not supported.

The Contractor shall:

- Provide deployment planning and requirements validation
- Provision the desktop and network products required to implement the solution
- Install and test equipment, operating systems, and connectivity
- Install and configure the hardware and operating system (OS) software

C.6.4.3.3 Staffing

- Forty-eight positions are agreed for Desk Side Services in the Labor Categories and skill levels based on the Government's stated requirements.
 - Manager Positions are agreed as follows:
 - Two Practice/Program Manager II; and,
 - Three User/Technical Support Manager I.
 - Technician Positions are agreed as follows:
 - Seven User/Support Technicians I;
 - Twelve User/Support Technicians II;
 - Sixteen User/Support Technicians III;
 - Four User/Support Technicians IV; and,
 - Four User/Support Technicians V.
- This staffing level is based on the agreed user population of 4,500 current active accounts on the network and meets the 100:1 ratio;
- The Government deems that the level of staffing is sufficient to meet SLAs of 2hours/4hours response/resolution times for VIP and 4hour/8hour response/resolution times for non-VIP

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 168
--------------	--------------	--	---------------

users. At anytime during the period of performance, Unisys has the opportunity to present data and justification for an increase in staffing to meet the above SLAs.

- Unisys will provide information during regular program reviews on active users and level of service delivery, and make recommendations for the need for changes in staffing (level of effort, labor categories, etc.) for desk side services based on changes in active user population; the Government will evaluate the information provided by Unisys with the intent of maintaining Service Level Agreements for desk side services.
- Unisys and the Government agree that Desk Side Services includes IMACs as a normal day-to-day activity; IMAC efforts that need to occur outside normal duty hours, or are of such magnitude that they could disrupt the delivery of desk side services, would be addressed via a project Task Order or Delivery Order.

C.6.4.3.4. Notification Requirements

The Government agrees to provide the following notification to the Contractor:

- Employee moves – Three day minimum notification required;
- New Personnel arrivals – Five day minimum notification required including the following data elements:
 - Name
 - Date of arrival
 - Work location
 - Status (Contractor, Government employee, vendor)
 - Services required (equipment, email account, applications, BlackBerry, etc.)
- Other Delivery Purposes – The Government will provide the following:
 - Name
 - Phone Number
 - Location including cubicle number

Delivery of Products to End User requires that the end user or other designated Government representative be present and available to receive the product;

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 169
--------------	--------------	--	---------------

C.6.4.4. Application Services

(A detailed Work Breakdown Structure for this Performance Area is included in Appendix D)

C.6.4.4.1. Infrastructure Maintenance Services

Remedial (Break-Fix) Maintenance services include the repair or replacement of malfunctioning hardware or software, as well as transportation, labor, and parts required to return the malfunctioning component to its original operating condition.

C.6.4.4.2. Availability of Qualified Personnel and Approved Maintenance Downtime

Successful operation requires a dedicated team of experts to ensure that necessary maintenance procedures are routinely followed. The Contractor shall provide DHS 24 X 7 coverage. The Contractor shall provide near-site support, in conjunction with the Network Control Center (NCC) and the Single Point of Contact (SPOC) personnel, and will make every reasonable attempt to identify trends and emerging issues for resolution before they become serious outages. The Contractor shall provide on-site Project Manager with the DHS Office of the Chief Information Officer to ensure that required maintenance is performed.

C.6.4.4.3. DHS-Approved Maintenance Downtime

The Contractor shall coordinate with the Government to schedule any system maintenance downtime sufficiently in advance to enable smooth operations during maintenance windows.

C.6.4.4.4. Materiel Transportation and Travel Requirements

The Contractor shall provide Transportation of materiel and equipment in and around the National Capital Region (NCR).

C.6.4.4.5. Application Status and Performance Reports

An application is defined as any program, or set of programs, that runs on a processor, and which can be interpreted as a database, a loadable module, a daemon or a service that an operating system loads so that the application operates properly. Any scheduled jobs, any automated processes (Cron Jobs that operate at predefined time intervals or that occur following notifications), or periodically timed or batched tasks shall also be considered applications.

The Contractor shall provide application status and performance reports as described below.

C.6.4.4.5.1. Up/Down Status and Availability of Major Applications on the Network

As required for determining network status, the Contractor shall provide DHS HQ an Up/Down Status Report of Major Applications on the Network indicating the availability and functionality of applications for end users. This report will include an up/down status of major applications as listed in the following section:

The current status of all major applications integral to the network is a critical data set that must be maintained and available to the Government at all times. In this regard, DHS HQ requires Up/Down status of major applications on the network such as:

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	170

- E-Mail (Exchange)
- All Server-based applications
- All database engines on which application run
- All Backup Systems software (e.g., including real-time replication software, tape back-up software, document management software, etc.)
- Desktop environment
- Internet, intranet, and extranet

(See the WBS breakout section 2.0, Engineering Operations in Appendix B for further details on applications status reporting requirements).

C.6.4.4.5.2. Performance Trends of Major Applications on the Network

When requested by the Government via a separate Task Order or Delivery Order, the Contractor shall provide DHS HQ a Performance Trends of Major Applications on the Network Report (see the WBS breakout section 2.0, Engineering Operations in Appendix B for further details).

DHS HQ requires that the Contractor report upon operational performance of these applications. Historical data on the performance of each application shall also be kept and supplied to DHS HQ in the form of trend reports. DHS HQ will use these reports to assess the performance of each application. The Contractor shall collect and maintain this data, by contract performance year, and retain this data for a two-year period following the end of the contract performance year.

The Contractor shall provide reports on a daily, weekly, and monthly basis showing application availability, and status and results of significant events within the application (Example. Takes 30 seconds to send and e-mail within DHS HQ and show it as being read by recipient. Example: Takes 32 seconds to search for a specific record in xyz database using the following search criteria, etc.).

C.6.4.4.5.3. Ad Hoc Performance Reporting Requirements

The Contractor shall provide ad hoc Executive Reports, upon request, depicting a detailed summary of specific application performance events. See deliverables table.

C.6.4.4.5.4. New Applications

In the event new applications are required, or if the Contractor has determined that a new application is available or otherwise recommends that a new application would be beneficial to the DHS Headquarters and the Government concurs, then the application can be added to the DHS environment only after a Memorandum of Understanding for New Applications is executed describing the new application, its purpose, benefits, and implementation plan.

C.6.4.4.5.5. Service Delivery Management Services

The Contractor shall:

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	171

- Provide overall management in support of the deployment effort
- Provide reporting and documentation deliverables
- Provide a single-point accountability for the managed services function

In performing this effort, the Contractor shall include the following factors in its management of this area:

- The DHS environment has reached a "steady state" and no significant applications are being added to the system;
- The only activity currently on-going in the DHS HQ environment requiring Unisys support are maintenance and content management for www.dhs.gov and network support of the ProSight application in OCIO in support of the Capital Planning and Investment Program effort;
- When new applications are to be added to the environment, the Government expects that a separate Task Order or Delivery Order will be raised. Unisys will conduct a thorough review and propose a solution that addresses, as a minimum, the following areas:
 - Hardware and software requirements;
 - Security requirements;
 - Installation; and,
 - O&M support issues.
- One full-time Content Manager position is accepted;
- One full-time System Engineer position is accepted; the Government expects this position to be firm fixed-priced to manage the servers and dhs.gov and ProSight applications (DHS-052);
- One half-time Project Manager position to oversee the work associated with both applications is accepted;
- One half-time Application Architect position to evaluate environmental conditions, root cause analysis under the auspices of "break fix" is accepted;

C.6.4.4.5.6. Application Services Fixed Deliverables

Unisys will provide on a weekly basis, status reports for DHS.gov and ProSight infrastructure that cover the following data points:

- Funding level
- Significant Events/Outages
- Summary of O&M activity

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	172

Unisys will also provide the Government root cause analysis report (within 72 hours of the incident) following any outages on DHS.gov or ProSight infrastructure. The report will include the following:

- Root cause of outage
- Remediation activities
- Mitigation activities
- Recommendation for platform enhancement to prevent recurrence

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	173

C.6.4.5. Security Services

(A detailed Work Breakdown Structure for this Performance Area is included in Appendix E)

C.6.4.5.1. Requirements Definition

The scope and primary focus of this work statement includes the following three areas:

- Security Program Management;
- Security Policy and Planning; and
- Security Compliance following Clinger-Cohen Act core competencies and industry standards and best practices. In this regard, the following security publications should be followed (See Appendix G for additional Security laws, regulations, policies, and guidelines):
 - NIST 800-63, Electronic Authentication Guidelines;
 - NIST 800-64, Security Considerations in the Information System Life Cycle;
 - NIST 800-65, Integrating Security into the Capital Planning and Investment Control Process;
 - NIST 800-53, Recommended Security Control for Federal Information Systems; and,
 - All other NIST Special Security Publications and/or Federal Information Processing Standards (FIPS)

C.6.4.5.2. Key Responsibilities

The Contractor will work with the DHS Security Program Director, in cooperation with the DHS Chief Information Security Officer (CISO), to develop an internal DHS headquarters security program, as part of an integrated framework capable of meeting mission requirements.

The Contractor's proposal must include the capabilities to provide the following services to the DHS CISO:

- Assist in developing DHS Headquarters' security policies and procedures, with particular focus on the DHS SBU network.
- Assist the DHS CISO with the C&A Process for DHS HQ systems and applications, with a particular focus on System Test & Evaluation and network related issues.
- Assist the DHS CISO in identifying and mitigating risks for all DHS HQ SBU network operational systems.

C.6.4.5.3. Contingency Planning

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 174
---------------------	--------------	--	---------------

When requested by the Government, Contingency Planning requirements will be addressed by a separate Task Order or Delivery Order.

Contingency Planning is the process for making sure that the Government can recover from processing disruptions in the event of localized emergencies or large-scale disasters, and is essential to the continuing accomplishment of the DHS HQ's mission.

The Contractor, when requested, will develop a Contingency Plan that is based upon an industry standard Business Continuity Management Methodology. Such a standard methodology is provided by the Disaster Recovery Institute, International, and the Business Continuity Institute. In addition, contingency planning for the Program shall be in conformance with OMB and DHS guidelines (separately provided to the Contractor) for the Continuity of Operations Plan and the Disaster Recovery Plan.

Following approval by the Government, the Contractor shall implement the Contingency Plan that can support DHS HQ through the entire life cycle of a business continuity program.

Verification of this support capability will be determined by annual drills of the plan, conducted by the Contractor, when and as directed by the Government, with the Government's participation as determined by the Agency.

C.6.4.5.4. DHS' Desired Approach to Solution

The Contractor will propose an integrated teaming structure fully cognizant of the situation, needs, and desired outcomes. We describe in full detail the function and responsibility for each of the subtasks of the Security Program on the following pages.

C.6.4.5.5. Work Order Management Structure and Approach

Department of Homeland Security regulations require that subordinate agencies and organizations be responsible for protecting the information systems under their operational control. To attain this goal, the integrated DHS/Contractor Security team must implement IS security policy that includes the following elements:

- The DHS HQ's security will be addressed in all new system acquisitions, system development and in modifications to existing systems. For example, security requirements must be specified in statements of work for new system acquisitions and for internally developed systems.
- As a minimum, the DHS baseline security requirements specified in MD4300-A would be implemented within each DHS HQ information system and application, to protect its resources and the information that is processed, stored or transmitted. Additional safeguards may be applied, based on risk management and sensitivity of data
- The Certification and Accreditation Process shall be conducted according to NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, in order to comply with FISMA and OMB requirements.

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	175

- DHS sensitive information must be safeguarded against unauthorized disclosure, modification, access, use and destruction. Also, DHS information systems supporting access to and modification of this sensitive information must be protected from delay or denial of service.
- All systems processing, storing or transmitting information must be accredited prior to being placed in production.
- Connectivity between DHS information systems (IS) and any other information systems (IS) or networks not under DHS authority is prohibited, unless documented by a standard Interconnection Security Agreement (ISA) formally approved by the appropriate DHS Signatory Authority. Appropriate appendix section of the DHS Security Policy will contain instructions and additional information on completing an ISA.
- All DHS information systems are for official DHS or Government business only. Users should have no expectation of privacy when using these resources. DHS systems may be approved for "Limited Personal Use" on a case-by-case basis as approved in accordance with the developed policy.
- All individuals who use, manage, operate, maintain or develop DHS information systems, applications, or data must comply with the policy and procedures prescribed in the DHS Security Policy.

C.6.4.5.6. Team Structure

As mentioned above, the integrated security team must support and coordinate activities across all technology and program initiatives under DHS.

The DHS Security Program Director, along with DHS CISO, will work collaboratively with IT Capital Planning, Enterprise Architecture, and IT Security and Information Assurance. Because Clinger Cohen compliance factors contain governance structures, change management and other cross team activities, this is a critical horizontal function that intersects the integrated DHS/Contractor team's organization structure.

Stakeholders of the virtual team play a critical role in forming the Security vision, goals and activities. Subsequently, the integrated DHS Security program will take into account communications with the Investment Review Board and Change Control Board.

C.6.4.5.7. Approach

In addition to this structure, the Contractor must collaborate with the integrated security team on a unified approach. As a first step, the collaboration will establish a jointly-created understanding of the interrelationships between the key work streams underlying DHS headquarters—security strategic planning, capital planning and control, enterprise architecture, and IA Architecture. A joint and clear understanding of the interaction and interdependencies inherent in these work streams is critical to eliminating duplicative activities and to orienting all work to accomplish the appropriate outcomes.

The integrated DHS/Contractor security team will form a management infrastructure to execute the stated mission and management of the DHS CISO's security program. Upon execution of the contract, the integrated security DHS/Contractor management infrastructure will develop the following items:

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 176
---------------------	--------------	--	---------------

- An Integrated Security Program Management Plan to include:
 - A Security Program Work Schedule, which will be integrated into the overall DHS Program Schedule
 - A Risk Management Plan
 - A comprehensive incident response process, reporting, transition and execution plan
 - A vulnerability assessment process, reporting, remediation, transition and execution plan
 - An Anti-Virus vulnerability assessment process, including reporting, remediation, transition and execution plan elements
 - A firewall development and concept of operations plan
 - A security Concept of Operations manual, deployment plan, and maintenance report
 - A security compliance health check reporting, and issues resolution report
 - A Security Program Financial Plan
 - A NIST SP 800-18 Compliant System Security Plan
- A Security Weekly Status Report that includes:
 - Updates of Integrated Security Program Management Plan with complete schedule details
 - Updates of major Integrated Security program risks with associated mitigation and contingency plans
 - Updates of resource changes
 - Updates of the Deliverable(s) Traceability Matrix
 - Task accomplishments for the week
 - Expected task accomplishments for the following week
 - Issues/concerns

C.6.4.5.8. Solutions

The Integrated Security Program solution integrates the following areas that encompass this program:

- Security Management & Strategic Planning (Risk Assessments, Policy and Procedures, SLA Management, Planning), Security SLAs

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 177
---------------------	--------------	--	---------------

- Security Engineering (Infrastructure and Applications Solutions Development)
- Security Enterprise Architecture
- Security and Information Assurance Planning
- Clinger-Cohen Core Competencies
- Security Operations (SOC, Firewall Management, IDS Management, Virus Management, Incident Response, Vulnerability Scanning)
- Security Compliance (Red Team, Blue Team, External Compliance Audit, Internal Policy Audit, Security Training, Certification and Accreditation, SLA Metrics)

Contractor understands the interplay between these security functions and is recommending an integrated solution and approach to synchronize appropriate activities that serve DHS's stated mission in an effective and efficient manner.

C.6.4.5.9. Information Security Policy and Planning

C.6.4.5.9.1. IT Security Strategic Planning

The integrated security management organization will perform the following activities with emphasis placed on joint DHS/Contractor Team collaborative discussions and associated activities to clearly define, prioritize, and execute current and future DHS headquarters security objectives.

The recommended approach is to leverage a business strategy-driven method to align DHS Security program with overall goals and objectives of DHS' stated mission to ensure protection, privacy, and integrity with accelerated value.

C.6.4.5.9.2. IT Security and Information Assurance Planning

This section describes the integrated security program solution for DHS headquarters security and information assurance for DHS' network. IT Security engineers ensure artifacts delivered support all EA tasks, subtasks and activities accurately represent DHS security policy and standards. In other words, IT security engineering and design initiatives are responsible to build secure systems that will leverage overarching EA to ensure the necessary security policies, standards and processes that protect the information infrastructure are preserved. The objective of this function is to employ a DHS Security Management Plan that provides DHS headquarters with guidance for the organization and management of IT Security across the DHS HQ. This includes the development of security plans, policies, procedures, and concept of operations documents. The Security team is an integral part of this task and will be responsible for documenting the necessary security standards and transformational processes associated with the DHS headquarters Security program.

C.6.4.5.9.3. Approach

The Contractor will approach IT Security activities consistent with DHS MD-4300A and other relevant government standards. The recommended approach will employ a three-phase methodology to support DHS in establishing sound information IT Security plans, policies, standards, and

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	178

architectures, while fulfilling government regulations and requirements such as the Government Information Security Reform Act (GISRA). Critical success factor is the dedicated participation and fluid communication with DHS Chief Information Security Officer (CISO) as this will ensure that security related requirements derived from new business applications requirements and analysis, will conform to the security architecture design and that they are incorporated securely into the security EA. Each of the three phases is described below with a list of specific tasks we will accomplish in that phase.

Phase 1 – Planning: Phase one will define planning activities, roles, and responsibilities necessary to coordinate and support DHS headquarters security objectives. DHS and the Contractor will establish a joint Security Working Group with a defined charter and mission. The tasks associated with this phase include:

- Mission and charter development
- Security assessment of existing and required security policies, standards and practices
- Resource Allocation
- Responsibility Assignment

Phase 2 – Process Definition: The focus of Phase 2 is a process definition to address security program requirements planning and analysis consistent with DHS business objectives. The byproduct of this effort will be a documented security processes that includes the following:

- Identification, analysis and communication of DHS Program business security requirements derived from analysis under other tasks, subtasks or activities for the security program
- Conducting security audits of existing infrastructure and all delivered security artifacts (IATO, POA&M, Risk assessments, et al)
- Providing an updated security architecture for inclusion into enterprise EA

Phase 3 – Analysis: Phase 3 will encompass the current and future states of the enterprise security architecture. The integrated security team will work collaboratively to address the activities and coordination required to integrate the development and deployment of current/future DHS initiatives with defined security processes and procedures. This includes adherence to security regulations, mandates, and public law applicable to the DHS, both SBU and classified. Specific activities we will accomplish during this phase are:

- Review/audit security artifact repository
- Map program security baseline requirements to current security architecture
- Develop gap analysis and remediation plan to bring current enterprise security architecture into compliance
- Provide remediation enterprise security architecture to the EA team
- Prepare Transition Plan to deploy remediation security architecture/process

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 179
---------------------	--------------	--	---------------

C.6.4.5.9.4. IT Information Security Plans

Information System Security Plans establish guidance for the security organization, and management, and policy guidance for DHS. The purpose of information system security plans are to provide an overview of the security requirements of the system and describe the controls in place, or planned for meeting those requirements; and to delineate responsibilities and expected behavior of all individuals who access the system. The Contractor will support the creation of System Security Plans in accordance with NIST SP 800-18, Guide for Developing Security Plans for Information Systems.

In general, the system security plan will contain, at a minimum, the following topics:

- System security environment
- Sensitivity of information
- All applicable US Laws, US regulations and DHS policies affecting the system at the time of award
- Management controls
- Operational controls including applications
- Technical controls
- Risk assessment and management
- Security System Life Cycle

In accordance with NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, the Contractor will support the following levels of compliance:

- Level 1 – Control objective documented in security policy (Security policies documented)
- Level 2 – Security controls documented as procedures (Security procedures documented)
- Level 3 – Procedures have been implemented
- Level 4 – Procedures and security controls are tested and reviewed
- Level 5 – Procedures and security controls are fully integrated into a comprehensive program

C.6.4.5.9.5. Firewall Policy

The Contractor will define firewall policy and determine how the firewall handles application(s) traffic such as web, email, or telnet. Additionally, the description of how the firewall is to be managed and updated also fall into the realm of the integrated security team's DHS Firewall Management Policy. The process to create this list requires knowledge of the vulnerabilities associated with each application and the cost-benefits associated with the methods used for securing the applications.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 180
--------------	--------------	--	---------------

The minimum steps involved in creating a DHS firewall policy are as follows:

- Identification of network applications deemed necessary
- Identification of vulnerabilities associated with applications
- Creation of applications traffic matrix showing protection method, and
- Creation of firewall rule-set based on applications traffic matrix

C.6.4.5.9.6. Certification and Accreditation

Contractor will continue to work with DHS to conduct a Certification and Accreditation Process in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, in order to comply with the FISMA and OMB requirements.

The approach that will be used to reduce security certification and accreditation costs involves grouping multiple information systems contained within a single facility or located at a centralized site, or site certification. The scope of the certification and accreditation process shall encompass all SBU sites.

The certification and accreditation process will be completed on information systems at each site with significant reuse of security evaluation results from the site-specific security controls. The results from any reevaluation of site-specific controls will be shared and incorporated into the security certification and accreditation documentation of all information systems at the site.

The security certification and accreditation process consists of four distinct phases: (1) an Initiation Phase; (2) a Security Certification Phase; (3) a Security Accreditation Phase, and (4) a Continuous Monitoring Phase. Each phase consists of a set of well-defined tasks and subtasks that are to be carried out by DHS and Contractor personnel. The security certification and accreditation activities can be applied to an information system at appropriate phases in the system development life cycle by selectively tailoring the various tasks and subtasks.

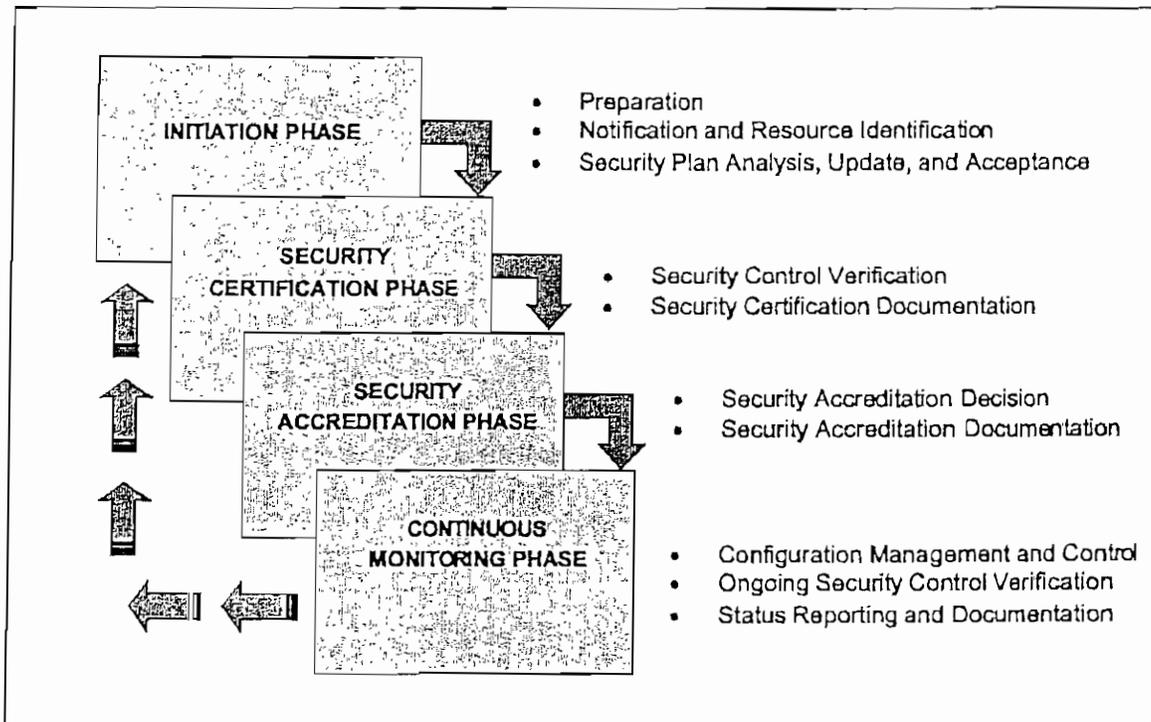
The security **accreditation package** documents the results of the security certification and provides the authorizing official with the essential information needed to make a credible, risk based decision on whether to authorize operation of the information system. Unless specifically designated otherwise by the Chief Information Officer or authorizing official, the information system owner is responsible for the assembly, compilation, and submission of the security accreditation package. The information system owner receives inputs from the information system security officer, certification agent, and senior agency information security officer during the preparation of the security accreditation package. The security accreditation package contains the following documents:

- Approved System Security Plan - The Security Plan (SP) is an overview of the security requirements, the agreed-upon security control supporting security-related document such as risk assessment.
- Security Assessment Report - The Security Assessment Report is the security control assessment results and recommended corrective actions

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	181

- Plan of Action and Milestones (POAM) - The Plan of action and milestones are the measures implemented or planned to correct deficiencies and to reduce or eliminate known vulnerabilities

Contractor will maintain the Security plan for the DHSNET. The designated certification authority will approve the security plan. The security assessment report will be conducted by a third party. Contractor will provide a plan of action and milestone with the direction of CIO office on how and when to complete the certification and accreditation process for the DHSNET.



C.6.4.5.9.7. Initiation Phase

The Initiation Phase consists of three tasks: (1) preparation, (2) notification and resource identification, and (3) security plan analysis, update, and acceptance. The purpose of this phase is two-fold. The first purpose is to allow Contractor to work with DHS personnel to identify the system to be certified, the appropriate DHS personnel to work with Contractor personnel on the certification, and assign roles and responsibilities for those people. The second purpose is to ensure that the Designated Accrediting Authority (DAA), usually the CISO and Contractor personnel, who will act as the Certification Agent, agree with the contents of DHS's NIST 800-18 System Security Plan for that system before the commencement of the certification process. If a System Security Plan does not exist one can be created during this phase.

C.6.4.5.9.8. Security Certification Phase

The Security Certification Phase consists of two tasks:

- Security control verification, and
- Security certification documentation

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	182

Contractor will work with DHS during this phase to ensure that the actual vulnerabilities in the information system are determined by evaluating that system's security controls and that recommended corrective actions are provided to the information system owner and DAA. Upon successful completion of this phase, the DAA will have the information needed from the security certification to determine the actual residual risk to agency operations and assets—and thus, will be able to render an appropriate security accreditation decision for that system.

C.6.4.5.9.9. Security Accreditation Phase

The Security Accreditation Phase consists of two tasks

- Security accreditation decision, and
- Security accreditation documentation

Contractor will work with DHS to ensure the DAA that the actual residual risk associated with the particular system is acceptable, and that the acceptability of that risk forms the basis of the security accreditation decision. Upon successful completion of this phase, the information system owner will have:

- Full authorization to operate the information system,
- An interim approval to operate (IATO) the system under specific terms and conditions, or
- Denial of authorization to operate the information system

C.6.4.5.9.10. Continuous Monitoring Phase

The Continuous Monitoring Phase consists of three tasks:

- Configuration management and control,
- On-going security control verification; and
- Status reporting and documentation

Contractor will work with DHS staff to continuously monitor the systems to ensure that changes do not adversely affect the documented vulnerabilities of the system. Contractor will provide oversight of the security controls on an ongoing basis and will inform the DAA when changes occur that may impact on the security of the system. This process will continue until the need for security reaccreditation occurs, either because of specific changes to the information system (event-driven), changes in federal policies requiring a reaccreditation, or the three year reaccreditation time span has elapsed, whichever comes first.

C.6.4.5.9.11. Risk Management

Within DHS, the network environment will continually be expanded and updated, its components changed, and its software applications replaced or updated with newer versions. In addition,

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	183

personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving.

To maintain a risk acceptable environment, the Contractor Security Team will integrate risk management into the SDLC for IT systems, not because law or regulation requires it, but because it is a good practice and supports the organization's business objectives or mission. There should be a specific schedule for assessing and mitigating mission risks, but the periodically performed process should also be flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies.

C.6.4.5.9.12. Risk Assessment

The Security Team Security Risk Analyst (SRA) task is to conduct comprehensive RAs for systems and applications within the boundaries of the DHS network environment. The risk assessment process is conducted in correlation for DHS as mandated by OMB Circular A-130 and completed in within the security lines of NIST 800-30, Risk Management Guide for Information Technology Systems. Risk assessment is the first process in the risk management methodology. The objective of the risk assessment will be to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC.

To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat exercise of an identified vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data).

The risk assessment methodology encompasses nine primary steps, which are:

- System characterization
- Threat Identification
- Vulnerability identification
- Control Analysis
- Likely hood determination
- Impact Analysis
- Risk Determination
- Control Recommendations
- Results Documentation

The output of this process will help to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. *Risk* is a function of the *likelihood* of a given *threat-source*

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 184
--------------	--------------	--	---------------

exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization.

C.6.4.5.9.13. Risk Mitigation

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Because the elimination of all risk is usually impractical or close to impossible, the Contractor will employ the *least-cost approach* and implement the *most appropriate controls* to decrease mission risk to an acceptable level, with *minimal adverse impact* on the DHS resources and mission. Risk mitigation is a systematic methodology used by senior management to reduce mission risk. Joint Contractor/DHS Risk mitigation will be achieved through any of the following risk mitigation options:

- Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
- Risk Avoidance. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
- Risk Limitation. To limit the risk by implementing controls that minimize the adverse impact of a threats exercising a vulnerability
- Risk Planning. To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
- Research and Acknowledgment. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
- Risk Transference. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

The goals and mission of the DHS should be considered in selecting any of these risk mitigation options. Addressing every identified risk is not practical; therefore, priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. DHS management, the mission owners, knowing the potential risks and recommended controls, may implement controls to mitigate the risk. The following is an example of the proposed risk mitigation process (Figure 3. Risk Mitigation Process):

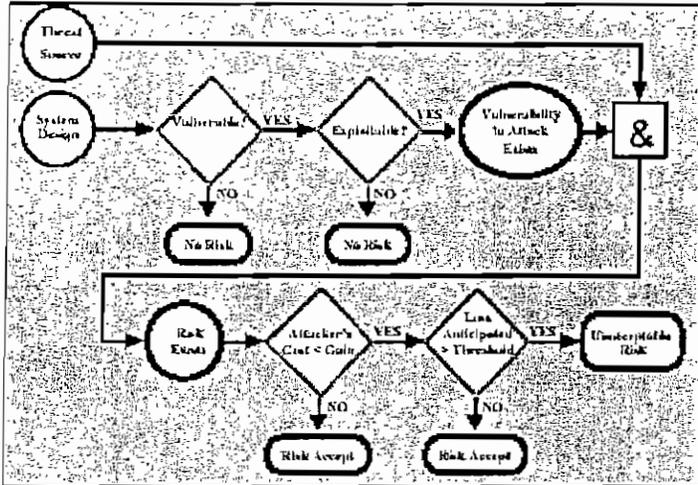


Figure 3 – Risk Mitigation Process

C.6.4.5.9.14. Risk Deliverables

The risk management program will rely on: (1) senior management commitment; (2) the full support and participation of the IT team; (3) the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization; and (4) an ongoing evaluation and assessment of the IT-related mission risks. Expected RA report deliverables are formatted as follows:

Risk Assessment Report Format

- a. Executive Summary
- b. System Description
 - 1) System Characterization
 - 2) Architectural narrative
 - 3) System Interfaces
 - 4) System and Data Sensitivity and Criticality
- c. Threat Statement
 - 1) Potential Vulnerabilities
 - 2) Potential Threats and Scan Results Summary
 - 3) Estimated Impact/Likelihood of compromise
- d. Security Controls Implemented

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 186
---------------------	--------------	--	---------------

1) Management, Operational, and Technical

e. Risk Analysis Findings

f. Architecture Drawing

C.6.4.5.9.15. Vulnerability Management

The Integrated Security Team will be responsible for performing vulnerability assessments, in which security reviews will be performed on a system for the purpose of discovering security vulnerabilities.

The vulnerability assessment team will use a controlled methodology based on a process that evaluates the approved system targets that are visible to an un-trusted entity or an unprivileged user of a system target. The Vulnerability Management methodology and capability will be identified in the LAN A Vulnerability and Incident Management solution. Planning and design of operations automation are priorities for IR, ID, and VM integrated solution. Necessary automation enhancements will be planned for in the Security Improvement Plan.

This service identifies specific security weaknesses on target systems, and provides recommended techniques and/or improvements to strengthen the security of the target system. Using industry standard and proprietary tools, the system is scanned for known security vulnerabilities. Industry standard and proprietary tool for scanning for known security vulnerabilities will be funded via a separate Task Order or Delivery Order.

A vulnerability assessment reviewer will validate any vulnerability identified by the initial scan, and then analyzes the system looking for additional vulnerabilities that wouldn't traditionally be picked up by a scan.

This service is designed to identify unauthorized access points or potential implementation weaknesses that could be used to compromise corporate assets. This very real threat could allow an attacker to bypass all traditional means of protection for example firewall protection.

C.6.4.5.9.16. Vulnerability Assessment

Vulnerability assessments are a crucial component to network security and the vulnerability/risk management process. Inter-networks and Transmission Control Protocol/Internet Protocol (TCP/IP) networks have grown exponentially over the last decade. Along with the advent of this growth, computer vulnerabilities and malicious exploitation have increased. Operating system updates, vulnerability patches, virus databases, and security bulletins are becoming a key resource for any savvy network administrator or network security team. It is the application of the patches and use of knowledge gained from these resources that actually make the difference between a secure network system and a network used as a backdoor playground for malicious hacker attacks. Starting with a system baseline analysis, routine vulnerability assessments need to be performed and tailored to the needs of the company to maintain a network system at a relatively secure level.

The big picture of risk management is the general process of taking necessary steps towards implementing a secure network production environment by providing clear policies and procedures outlining the basic needs and expectations of a corporate network security structure. The main output of interest is the working security policies and parties responsible for maintaining the network systems. The vulnerability assessment is only a part of this larger picture and is "a combination of people, policies, procedures and technologies."

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 187
---------------------	--------------	--	---------------

C.6.4.5.9.17. Site inspections

Site inspections may take place at any time during the term of this contract and may include the use of spot checks, scheduled inspections, random sampling, user reports, and periodic review of Contractor's quality and control programs by the DHS Headquarters or its designated representative. The Contractor shall immediately correct any specific measures where the Contractor is found to be noncompliant with DHS Security Policies and Security Architecture.

C.6.4.5.9.18. Intrusion Detection Reports

The Contractor shall provide Intrusion Detection Reports on a daily, weekly, and monthly basis showing Network Intrusion Detected Events, and Host Intrusion Detection Events. The source of the attempted access shall be provided as well as the mechanism employed to attempt to bypass security. In addition, the Contractor shall provide a report showing corrective actions taken to prevent recurrence of the intrusion events.

C.6.4.5.9.19. Vulnerability Methodology

The Vulnerability Assessment Team analyst will use a controlled methodology based on a process that evaluates the approved system targets that are visible to an un-trusted entity or an unprivileged user of a system target. The primary focus of the test is to discover unauthorized access points to a system target (i.e. open ports, web pages, data exchange applications, etc.). Although testing automated response systems such as intrusion detection, logging, and event reporting is possible, it is not normally within the scope of the Controlled Vulnerability Assessment Methodology (CVAM) for TCP/IP security. The end objective for the vulnerability assessment is to identify specific configuration vulnerabilities within system targets, recommended remediation actions, and assign relative risk ratings for individual vulnerabilities.

In order to appropriately gauge the overall risk to the system target environment, both the impact of vulnerabilities as well as their likelihood of occurrence must be understood. For individual identified vulnerabilities, a Likelihood Rating is provided based on how susceptible the vulnerability is to exploit, and how likely the targeted environment supports the exploit.

C.6.4.5.10 Staffing.

- Sixteen positions are agreed to for the Security Services effort including the Security Director;
 - Eight positions are considered essential for continuity of Security operations from ITMS thru the "bridge" contract;
 - Six positions will be staffed at skill levels equivalent to Computer Security Analysts Level II;
 - Two positions are dedicated to the S&T organization (for SR 40032); these positions will be funded via a separate PR that will add the appropriate funds to the bridge contract; these positions and associated funding are over and above the agreed overall price for the bridge;

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 188
---------------------	--------------	--	---------------

- Both parties believe that the level of staffing agreed upon is sufficient to accomplish the defined Plan of Action and Milestones (excluding Contingency Planning and Identity and Access Management) identified during the FY 05 Certification and Accreditation process, and exercise due care to provide adequate security for DHS HQ;
- The Government reserves the right to re-prioritize task accomplishment to meet the DHS security mission needs within the agreed upon staffing levels;
- No Other Direct Costs are required to support the Security Services WBS.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 189
---------------------	--------------	--	---------------

C.6.4.6. Asset Inventory Management

(A detailed Work Breakdown Structure for this Performance Area is included in Appendix F)

Since these assets provide a service to support mission requirements, their effective management becomes critical to the DHS HQ's mission success. Managing inventory assets, and the services they provide, involves a variety of business processes that support mission readiness and accountability, including work management, inventory management, service management, contract management and procurement.

Key performance factors include, the following, and will be incorporated into the SLA for these services:

- Integrity of data
- Completeness of available data sets
- Reconciliation processes
- Usability of asset data
- Accessibility of data
- Total asset visibility
- Traceability
- Asset consumption history
- Asset aging
- Providing monthly feeds to a DHS Headquarters inventory database that will include, as a minimum, the following asset attributes:
 - MS provider asset tag (Unisys)
 - DHS Headquarters asset tag (GFE)
 - Manufacturer's service tag number
 - Serial number
 - Category
 - Class
 - Manufacturer
 - Make

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 190
---------------------	--------------	--	---------------

- Model
- Description
- Cost (CLIN product price)
- ESN (cellular)
- Status
- Office
- Branch
- Division
- DHS Headquarters supported site
- Building
- Floor
- Room
- User_first_name, User_last_name
- CLIN
- Purchase Order or Delivery Order number
- DD250 date
- In-service date
- Warranty end date
- Government owned/leased
- Disposal method
- Disposal date
- Reporting: role-based, real-time, standard, and ad hoc
 - Standard field reporting shall be able to sort by user, CLIN, type, site category, and class
 - Standard HQ reporting shall be able to sort by user, CLIN, type, site, category, and class

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 191
---------------------	--------------	--	---------------

- Administration reporting shall include above standard capabilities for reporting as well as ad hoc reporting
- Reporting shall include a weekly report of changes or moves of equipment by area or site (see IMAC report shown in the WBS breakout)
- Making sure all managed equipment has been labeled and or tagged with appropriate identification asset tags/stickers for all equipment for which DHS orders the asset inventory tracking CLIN
- Maintaining the hardware inventory database
- Accepting data feed from HR and address for new hires and terminated employees (check-in and check-out procedures)
- Assisting in establishing and maintaining a software inventory database
- Including data elements for software database: type of software, name of software, license number, user_name (first and last), license expiration date, classification (enterprise or individual)
- Leading the annual physical inventory sweeps
- Documenting procedures for maintaining asset inventory tracking accountability for implementing DHS policies
- Maintaining cross-reference listing of leased/Government-Furnished Property to the Task Order or Delivery Order issued for procuring the item and provide to the Government as a section of the Asset Inventory Management Report
- Assisting in annual inventories and assist in establishing and maintaining a software inventory database, and documentation of policy and procedures for maintaining accountability
- Serving as the central point of contact for information relative to the IT inventory database
- Assisting the Government in responding to requests for asset-related inventory information; Unisys and the Government will discuss each such data call and jointly agree on what the appropriate response time should be; both parties acknowledge that a goal of four hours for such requests should be the target, but recognize that some circumstances may require or allow an up or down adjustment to this goal. This requirement, because of the uncertainty associated with such requests, is not included in KPIs or an SLA for this bridge contract; however, both parties agree that this support is important to DHS HQ, and must be managed accordingly.

C.6.4.6.2. Asset Inventory Control

- Asset inventory control requirements will continue to be "as is" i.e., assets inventory management services will continue to be provided at the same levels and in the manner as currently provided

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 192
--------------	--------------	--	---------------

under the ITMS task order. No asset inventory management system enhancements will be included within the scope of the DHS HQ "bridge" effort.

- Unisys will designate an asset inventory control liaison; the liaison must be knowledgeable of DHS HQ asset inventory control policies and procedures, and must be available to address inventory control issues when requested by the DHS HQ OCIO;
- Specific requirements for Asset Inventory Control include:
 - Applying best practices for asset inventory control services as outlined by the Gartner Group for similar organizations;
 - Accurately recording ordered assets in the Contractor's Web Ordering System (WOS);
 - Assigning all end-user assets to either:
 - The end-user, component organization when known, and a physical location (building and cubicle number or office number); or,
 - Inventory stockpile location;
 - Maintaining and safeguarding the asset until it is issued and signed for by the end-user; the Government will provide Unisys secured facilities in which to store assets pending deployment to end users;
 - DHS and Unisys will work together to develop policies that will enhance and enable inventory controls; the Unisys PMO will establish procedures to control inventory movement based on implemented DHS policy, e.g., entry and exit, to improve management of asset inventory controls;
 - Obtaining appropriate signatures and acknowledgement of responsible individuals when assets are issued (e.g., physical or electronic hand receipts);
 - Reconciling information in inventory reports to agree with known asset status;
 - Following base-lining of assets, initiating appropriate reviews, analysis, and suspension of asset inventory control fees when the location and accountability of assets are unknown; when location and accountability of assets are reestablished, the Government will resume payment of asset inventory control fees; if Unisys can demonstrate that those assets were in beneficial use to the Government during the period in question, the Government will adjust the asset inventory control fees accordingly;
 - Unisys will assume liability for assets within its direct control and possession;
 - Demonstrating a reliable audit trail, i.e., the capability to trace an asset through its lifecycle from ordering to current deployment status to end-of-life;
 - Providing an automated "hand receipt" process for end-users to sign for their assets;

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 193
---------------------	--------------	--	---------------

- Enabling end-users to self-verify the status of inventory assets issued to their component organization accounts;
 - Enabling and conducting complete annual inventories and reconciliation;
 - Providing monthly asset change report by component organizations;
 - Providing full access to asset data on an on-line basis, including associated asset inventory reports to the DHS HQ and its component organizations.
- Unisys will create new CLINs for Blackberry service that will include options for the Government to separately purchase hardware, managed services, and data usage; operation and maintenance of the BES is included in WBS 2.0, Engineering Operations; BES software licenses are included as an ODC in WBS 2.0; any products used to host the BES are included in B Table, Section B.7, Legacy Products.
 - The Unisys PMO will provide oversight for reporting of inventory management data. Unisys will apprise the DHS of weekly inventory levels; Unisys and the DHS will cooperate to reach agreement on what this regular and continuing inventory level should be; the DHS will promptly notify Unisys of any impending mission changes that could significantly affect current inventory levels; Unisys will not be responsible for any SLA performance requirements that depend on the availability of new inventory levels resulting from new mission requirements;

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	194

APPENDIX A – PROGRAM MANAGEMENT SERVICES WBS

WBS	Task
1	Program Management Services
1.1	Program Control
1.1.1	Program Executive Management
1.1.1.1	Program Executive
1.1.1.2	Program Executive Staff
1.1.1.2.1	Deputy Program Executive
1.1.1.2.2	RESERVED
1.1.1.2.3	RESERVED
1.1.1.2.4	RESERVED
1.1.1.2.5	RESERVED
1.1.1.2.6	Program Office Director
1.1.1.2.7	RESERVED
1.1.1.3	Executive Staff Support
1.1.1.3.1	Admin Support
1.1.2	Program Office
1.1.2.1	Program Office Management
1.1.2.1.1	RESERVED
1.1.2.1.1.1	RESERVED
1.1.2.1.1.2	RESERVED
1.1.2.1.1.3	RESERVED
1.1.2.1.1.4	RESERVED
1.1.2.1.1.5	RESERVED
1.1.2.2	RESERVED
1.1.2.2.1	RESERVED
1.1.2.2.2	RESERVED
1.1.2.3	RESERVED
1.1.2.3.1	RESERVED
1.1.2.4	RESERVED
1.1.2.4.1	RESERVED
1.1.2.4.2	RESERVED
1.1.2.4.3	RESERVED
1.1.2.4.4	RESERVED
1.1.2.4.5	RESERVED
1.1.2.5	RESERVED
1.1.2.5.1	RESERVED
1.1.2.5.1.1	RESERVED
1.1.2.5.1.2	RESERVED
1.1.2.5.1.3	RESERVED
1.1.2.5.2	RESERVED
1.1.2.5.2.1	RESERVED
1.1.2.5.2.2	RESERVED
1.1.2.5.2.3	RESERVED
1.1.2.5.2.4	RESERVED
1.1.2.5.2.5	RESERVED

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	195

1.1.2.6	Program Performance Measurement
1.1.2.6.1	Performance Measurement Plan
1.1.2.6.2	SLA Process Support
1.1.2.6.3	SLA Performance Reports
1.1.2.7	Quality Assurance
1.1.2.7.1	Quality Assurance Plan
1.1.2.7.2	Conduct Product, Process and Quality Audits
1.1.2.7.3	Track Corrective Actions
1.1.2.7.4	Audit Reports and Recommendations
1.1.3	Business Management
1.1.3.1	Financial Management
1.1.3.1.1	Program Finance Management
1.1.3.1.1.1	ETC Report
1.1.3.1.1.2	TTO/TTR Reports
1.1.3.1.1.2.1	Ad Hoc query requests
1.1.3.1.1.2.2	Full TTO Payoff Report (Monthly)
1.1.3.1.1.2.3	Full TTO Payoff Report (On Request)
1.1.3.1.1.2.4	Expired Lease TTO Monthly Payoff Report (Monthly)
1.1.3.1.1.2.5	Expired Lease TTO Annual Payoff Report (Monthly)
1.1.3.1.1.3	Monthly Funds Status Report
1.1.3.1.1.4	Project Financial Status Report
1.1.3.1.1.4.1	85% Ceiling Price Notification (by SO)
1.1.3.1.1.4.2	Cost Element Forecast
1.1.3.1.1.4.3	Obligated Funding Report
1.1.3.1.1.5	Job Order Cost Management
1.1.3.1.1.5.1	Job Order Code Hierarchy
1.1.3.1.1.5.2	Job Order Code Establishment
1.1.3.1.1.5.3	Job Order Cost Monitoring
1.1.3.1.1.6	Invoice Management
1.1.3.1.1.6.1	Invoice Review
1.1.3.1.1.6.2	Monthly Invoice Summary Report
1.1.3.1.1.6.3	DD250 Status report
1.1.3.1.1.6.4	Travel and Per Diem Review
1.1.3.1.1.6.5	Payments
1.1.3.1.1.6.6	Invoice issue resolution
1.1.3.1.2	Financial Reporting
1.1.3.1.2.1	Funds Status Reporting
1.1.3.1.2.2	Cost Performance Reporting
1.1.3.1.2.3	Project Cost Reporting
1.1.3.1.2.4	Financial Database Management
1.1.3.2	Subcontractor Liaison
1.1.3.2.1	RESERVED
1.1.3.2.2	RESERVED
1.1.3.2.3	RESERVED
1.1.3.2.4	Small Business Management
1.1.3.3	Facilities Support
1.1.3.3.1	RESERVED
1.1.3.3.2	RESERVED

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	196

1.1.3.3.3	RESERVED
1.1.3.4	Resource Management
1.1.3.4.1	Staffing Coordination
1.1.3.4.2	Labor Conformance
1.1.3.5	Program Service Supply Chain Management
1.1.3.5.1	Solution Management
1.1.3.5.1.1	RESERVED
1.1.3.5.1.2	RESERVED
1.1.3.5.1.3	CLIN Management
1.1.3.5.1.3.1	Create / Update / Delete
1.1.3.5.1.3.2	Communicate
1.1.3.5.2	Product / Service Provisioning
1.1.3.5.2.1	Online Catalog Support (Web Ordering System - WOS)
1.1.3.5.2.2	Product and Service Fulfillment
1.1.3.5.2.2.1	Logistics
1.1.3.5.2.2.2	Order to Invoice Process
1.1.3.5.2.2.3	Material Scheduling
1.1.3.5.2.2.4	Purchase Requisitioning
1.1.3.6	RESERVED
1.1.3.7	DB Admin
1.1.3.8	Physical Security
1.2	RESERVED
1.2.1	RESERVED
1.2.2	RESERVED
1.2.2.1	RESERVED
1.2.2.2	RESERVED
1.2.2.3	RESERVED
1.2.3	RESERVED
1.3	RESERVED
1.3.1	RESERVED
1.3.1.1	RESERVED
1.3.1.2	RESERVED
1.3.1.3	RESERVED
1.3.1.3.1	RESERVED
1.3.1.3.2	RESERVED
1.3.1.3.3	RESERVED
1.3.1.3.4	RESERVED
1.3.1.3.4.1	RESERVED
1.3.2	RESERVED
1.3.2.1	RESERVED
1.3.2.2	RESERVED
1.3.2.3	RESERVED
1.3.2.4	RESERVED
1.4	RESERVED
1.4.1	RESERVED
1.4.1.1	RESERVED
1.4.1.2	RESERVED
1.4.2	RESERVED

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 197
--------------	--------------	--	---------------

1.4.2.1	RESERVED
1.4.2.2	RESERVED
1.4.3	RESERVED
1.4.3.1	RESERVED
1.4.4	RESERVED
1.4.4.1	RESERVED

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	198

APPENDIX B – ENGINEERING OPERATIONS WBS

2	Engineering Operations
2.1	Engineering Management
2.1.1	Service management - Network Monitoring
2.1.2	Command & Control (C & C)
2.1.3	RESERVED
2.1.3.1	Automated Tools to Monitor Network Performance - App Manager, Quest, ACE Licenses
2.1.3.2	RESERVED
2.2	Infrastructure Engineering
2.2.1	Server Infrastructure
2.2.1.1	RESERVED
2.2.2	Client Infrastructure
2.2.2.1	Software Monitoring Tools - Altiris CMS Licenses
2.2.2.2	RESERVED
2.2.3	Network Infrastructure
2.2.3.1	Network Infrastructure Tools
2.2.3.2	RESERVED
2.2.4	RESERVED
2.2.4.1	RESERVED
2.2.5	Infrastructure and Deployment Projects
2.2.5.1	RESERVED
2.3	Production Engineering Support
2.3.1	RESERVED
2.3.1.1	Backup and Recovery Services Support & Tools
2.3.2	RESERVED
2.3.3	Production Eng Tools/Maint - T-Support of Blackberry & Hyena
2.4	RESERVED
2.4.1	RESERVED
2.4.1.1	RESERVED
2.4.1.2	RESERVED
2.4.2	RESERVED
2.4.3	RESERVED

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 199
--------------	--------------	--	---------------

APPENDIX C – END USER SERVICES WBS

	APPENDIX C - END USER SERVICES WBS (STAFFED AT 100:1 RATIO)
3	End User Services
3.1	End User Services - Equipment Maintenance
3.1.1	End User Equipment
3.1.2	Dispatch on-site and on-call technicians
3.1.3	Provide Global reporting system Service Center
3.1.4	Maintain Service and Repair Logs on Enterprise Systems
3.1.5	Preventive Maintenance
3.1.5.1	Schedule and perform hardware PM based on OEM specifications
3.1.5.2	Schedule and perform software PM based on ITMS policies
3.1.6	Remedial Maintenance
3.1.6.1	Software remedial maintenance performed via patch management
3.1.6.2	Software patches distributed remotely
3.1.6.3	Critical Incident Support
3.1.6.3.1	Service Request
3.1.6.3.1.1	Locations
3.1.6.3.1.2	Durations
3.1.6.3.2	Submit critical incident support proposal
3.1.6.3.3	Spare Parts
3.1.6.3.3.1	Provide a plan 60 days after contract award
3.1.6.3.3.1.1	Spare parts
3.1.6.3.3.1.2	User equipment loaner pool
3.1.6.3.4	Warranty
3.1.6.3.4.1	Register products with vendors to receive SMARTNET support
3.1.6.3.4.1.1	Provide Technical support
3.1.6.3.4.1.2	Provide Software patches
3.1.6.3.4.1.3	Provide hardware technical releases
3.1.6.3.4.1.4	Provide Equipment refresh
3.1.6.3.5	Non-Warranty Maintenance Support for Desktop Workstations
3.1.6.3.5.1	Non-Warranty Maintenance Support for Laptop Workstations
3.1.6.3.5.2	Non-Warranty Maintenance Support for Local Desktop Printers
3.1.6.3.5.3	Non-Warranty Maintenance Support for Mid-Range Printers
3.1.6.3.5.4	Non-Warranty Maintenance Support for High-End Printers
3.1.6.3.5.5	Non-Warranty Maintenance Support for High-End Network Laser Printers
3.1.6.3.5.6	Non-Warranty Maintenance Support for Laptop Docking Stations
3.1.6.3.5.7	Non-Warranty Parts Only Support for Desktop Workstations
3.1.6.3.5.8	Non-Warranty Parts Only Support for Laptop Workstations
3.1.6.3.5.9	Non-Warranty Parts Only Support for Local Desktop Printers
3.1.6.3.5.10	Non-Warranty Parts Only Support for Mid-Range Printers
3.1.6.3.5.11	Non-Warranty Parts Only Support for High-End Printers
3.1.6.3.5.12	Non-Warranty Parts Only Support for High-End Network Laser Printers
3.1.6.3.5.13	Non-Warranty Parts Only Support for Laptop Docking Stations
3.1.6.3.5.14	Cisco Device Maintenance - DHS HQ Projects
3.1.6.3.5.15	Non-Warranty Maintenance Support for WINTEL Low Range Servers
3.1.6.3.5.16	Non-Warranty Maintenance Support for WINTEL Medium Range Servers
3.1.6.3.5.17	Non-Warranty Maintenance Support for WINTEL High Range Servers

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	200

3.1.6.3.5.18	Non-Warranty Maintenance Support for WINTEL Enterprise Servers
3.1.6.3.5.19	Maintenance Support for Cisco Low Range Router
3.1.6.3.5.20	Maintenance Support for Cisco Medium Range Router
3.1.6.3.5.21	Maintenance Support for Cisco High Range Router
3.1.6.3.5.22	Maintenance Support for Cisco Switch
3.1.6.3.5.23	Maintenance Support for Cisco Firewall
3.2	End User Services - Installation, Moves, Adds, Changers (IMAC)
3.2.1	Physical and Software IMAC Support - Courier Service
3.2.1.1	Remotely installs software
3.2.1.1.1	HSOC
3.2.1.1.2	DHS HQ Locations
3.2.1.2	Dispatches technicians
3.2.1.3	IMACs over quantity 10 are managed as projects
3.2.1.3.1	Scheduled
3.2.1.3.2	Procedures documented and tested
3.2.1.3.3	Lessons learned
3.2.1.4	Bulk IMAC drawdown management
3.2.1.5	Data Migration
3.2.1.6	System Re-imaging
3.2.1.6.1	Remotely re-images
3.2.1.6.1.1	HSOC
3.2.1.6.1.2	DHS HQ Locations
3.2.1.6.2	SPOC dispatches call to the IMAC team
3.2.1.6.2.1	Hard disk failures
3.2.1.6.2.2	Software CDs
3.2.1.6.2.3	Instructions
3.2.1.7	Bulk IMAC drawdown management
3.2.1.8	Installation for Desktop Workstations
3.2.1.9	Installation for Laptop Workstations
3.2.1.10	Installation for Desktop Printers
3.2.1.11	Installation for Network Printers and Multi-Functional Devices
3.2.1.12	Network Connectivity for Network Copiers
3.2.1.13	Installation for WINTEL Low Range Server
3.2.1.14	Installation for WINTEL Medium Range Server
3.2.1.15	Installation for WINTEL High Range Server
3.2.1.16	Installation for Cisco Low Range Router
3.2.1.17	Installation for Cisco Medium Range Router
3.2.1.18	Installation for Cisco High Range Router
3.2.1.19	Installation for Cisco High Switch
3.2.1.20	Installation for Cisco Medium Switch
3.2.1.21	Installation for Cisco Low Switch
3.2.1.22	Installation for Cisco Firewall
3.2.1.23	Government Property Workstation Pre-Support Inspection
3.2.1.24	Government Property Printer Pre-Support Inspection
3.2.1.25	Government Property Copier Pre-Support Inspection
3.2.1.26	Government Property Server Pre-Maintenance Inspection
3.2.1.27	Government Property Cisco Network Device Pre-Maintenance Inspection
3.3	End User Services - Headquarters

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	201

3.3.1	Management
3.3.1.1	Provide management and direction of HQ support entities
3.3.1.2	Interface with HQ IT Operations Staff
3.3.1.3	Oversee Asset Management process
3.3.2	HQ Tier II Support
3.3.2.1	Resolve complex problems
3.3.2.2	Perform On site IMAC on limited basis
3.3.3	Operations
3.3.3.1	Onsite Technical Support for VIP end users
3.3.3.2	Technical Resource coordinator for IT users
3.3.3.3	Perform individual assignments associated with maintenance and deployment of applications products or services
3.3.3.4	Close Ticket with Appropriate Detail
3.3.4	Monthly Reporting
3.3.4.1	Oral Weekly
3.3.4.2	Written weekly activity report
3.3.4.3	Written monthly status report
3.4	End User Services - Field Services Support
3.4.1	Desk side Support
3.4.1.1	Dispatch CIR
3.4.1.2	Resolve and Confirm with User
3.4.1.3	Close ticket with appropriate detail
3.5	End User Services - SPOC
3.5.1	Utilize SPOC Policies and Procedures to Resolve Customer Issues
3.5.2	Provide Daily End User Help Desk Services
3.5.3	Maintain Ticketing Management System
3.5.4	Staff and Maintain SPOC Support Teams
3.5.5	Provide Necessary Training to Support Teams
3.5.6	Maintain ACD System
3.5.7	Perform Required System Backups
3.5.8	Provide SPOC Recording Communication to End Users for Service Impacting Events
3.5.9	Develop Plan for Self-Help System
3.5.10	Call Reception and Logging
3.5.10.1	Track Calls Received
3.5.10.2	Provide Toll Free Access to SPOC
3.5.11	Route to Support Organizations
3.5.12	Perform Call Redirection
3.5.13	Perform Diagnostics
3.5.14	Resolve Customer Incidents
3.5.15	Provide How-To Support
3.5.16	Perform Password Reset
3.5.17	Incident Management
3.5.17.1	Perform Daily Alert Notification Paging (WP)
3.5.17.2	Maintain DHS Escalation/Paging Contact Lists (WP)
3.5.17.3	Attend Weekly Ticket Review Meetings
3.5.18	Reporting
3.5.18.1	Monthly SLA Call Accounting Statistics Report (WP)

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	202

3.5.18.2	Daily Open Call Tracking Report (WP)
3.5.18.3	Weekly DHS Stats Report (WP)
3.5.18.4	Monthly Help Desk Responsiveness Report (WP)
3.5.18.5	Monthly Call Abandonment Report (WP)
3.5.18.6	Monthly First Call Resolution Report (WP)
3.5.18.7	Monthly End-to-End Resolution Report (WP)
3.5.18.8	Monthly Repeat Call Incident Report (WP)
3.5.18.9	Monthly Customer Satisfaction Report (WP)
3.5.18.10	Monthly Knowledge Base Status Report (WP)
3.5.19	Incremental Service Desk Support SPOC Call
3.5.19.1	Incremental Service Desk Setup - SPOC-Trained Applications
3.5.19.2	Incremental Service Desk Setup - SPOC-Coordinated Applications
3.5.19.3	Incremental Service Desk Support - Government-owned ProSight SW Enterprise Application
3.6	Service Management - Land Mobile Radio
3.6.1	Manage Land Mobile Radio Services

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	203

APPENDIX D – APPLICATION SERVICES WBS

	APPENDIX D - APPLICATION SERVICES WBS
4	Application Services
4.1	Application Projects
4.1.1	Project Reporting System
4.1.2	RESERVED
4.2	Architect DHS Applications
4.2.1	RESERVED
4.2.2	RESERVED
4.2.3	RESERVED
4.2.4	RESERVED
4.2.5	RESERVED
4.2.6	RESERVED
4.2.7	RESERVED
4.2.8	RESERVED
4.2.9	RESERVED
4.2.10	RESERVED
4.2.11	RESERVED
4.2.12	RESERVED
4.2.13	Perform Enterprise Applications Testing
4.2.13.1	Proposed Integration Testing
4.2.13.2	Proposed System/Subsystem Testing
4.2.13.3	Proposed Acceptance testing
4.2.13.3.1	Perform Functional Testing
4.2.13.3.2	Conduct Performance Testing
4.2.13.3.3	Proposed Approach for Product/Service Acceptance
4.2.14	DHS Enterprise Application Environment
4.2.14.1	Unix Server Hosting - High
4.2.14.2	Tape Backup System Hosting - Unix Environment

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	204

APPENDIX E – SECURITY SERVICES WBS

	APPENDIX E - SECURITY SERVICES WBS
5	Security Services
5.1	Security Program Management
5.1.1	Work Order Management
5.1.1.1	Integrated Program Management Plan
5.1.1.2	Weekly Status Reports
5.2	RESERVED
5.2.1	RESERVED
5.2.1.1	RESERVED
5.2.1.2	RESERVED
5.3	Information Assurance Governance
5.3.1	Certification & Accreditation
5.3.1.1	Initiation Phase
5.3.1.1.1	LAN A Sub System Documentation
5.3.1.2	Security Certification Phase
5.3.1.2.1	LAN A Sub System Documentation
5.3.1.3	Security Accreditation
5.3.1.3.1	LAN A Sub System Documentation
5.3.1.4	Continuous Monitoring Phase
5.3.1.4.1	Auditing & Compliance
5.3.1.4.2	CAP Accreditation
5.3.2	RESERVED
5.3.2.1	RESERVED
5.3.2.1.1	RESERVED
5.3.2.1.2	RESERVED
5.3.2.1.3	RESERVED
5.3.2.2	RESERVED
5.3.2.2.1	RESERVED
5.3.2.2.2	RESERVED
5.3.2.3	RESERVED
5.3.2.3.1	RESERVED
5.3.3	S&T Certification & Accreditation
5.4	IT Security Operations
5.4.1	IT Configuration Management
5.4.1.1	Configuration Change Control
5.4.1.1.1	CR Tracking & Approval
5.4.1.1.2	Security Impact Reviews
5.4.1.2	Configuration Status Accounting
5.4.1.2.1	Configuration Definitions
5.4.1.2.1.1	Network Components Policy & Configuration
5.4.1.2.1.1.1	Network Connections (e.g PPP links/GRE Tunnels)
5.4.1.2.1.1.2	Firewalls
5.4.1.2.1.1.3	Routers
5.4.1.2.1.1.4	Network Intrusion Detection Devices
5.4.1.2.1.1.5	Switches
5.4.1.2.1.1.6	Printers

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 205
---------------------	--------------	--	---------------

5.4.1.2.1.2	System Components Policy & Configuration
5.4.1.2.1.2.1	Active Directory Architecture
5.4.1.2.1.2.2	Servers (Dell, HP, IBM)
5.4.1.2.1.2.3	Workstations
5.4.1.2.1.3	Sub-Systems Architectures
5.4.1.2.1.3.1	RESERVED
5.4.1.2.1.3.2	VOIP
5.4.1.2.1.3.3	Blackberry
5.4.1.2.1.4	SCIF/Secure Area Configs
5.4.1.2.1.4.1	Security Policy Testing
5.4.1.3	Configuration, Verification, and Audit
5.4.1.4	LAN A Security Architecture
5.4.1.4.1	Develop model for Security Ops Architecture
5.4.2	Vulnerability & Incident Management (VIM)
5.4.2.1	VIM Strategic Management
5.4.2.2	RESERVED
5.4.2.3	Intrusion Detection
5.4.2.3.1	Device Management
5.4.2.3.1.1	Intrusion Detection Systems
5.4.2.3.2	Device Monitoring
5.4.2.3.2.1	Intrusion Detection Systems
5.4.2.4	Incident Response
5.4.2.5	RESERVED
5.4.2.5.1	RESERVED
5.4.3	RESERVED
5.4.3.1	RESERVED
5.4.3.2	RESERVED
5.4.3.3	RESERVED
5.4.3.4	RESERVED
5.4.3.5	RESERVED
5.4.3.6	RESERVED
5.4.4	RESERVED
5.4.4.1	RESERVED
5.4.4.1.1	RESERVED
5.4.4.1.2	RESERVED
5.4.4.1.3	RESERVED
5.4.4.2	RESERVED
5.4.4.3	RESERVED

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	206

APPENDIX F – ASSET INVENTORY MANAGEMENT WBS

	APPENDIX F - ASSET MANAGEMENT WBS
6	Asset Management
6.1	Asset Tracking and Annual Inventory
6.1.1	Asset Tracking services (ongoing present state)
6.1.2	Annual Physical Inventory (ongoing present state)
6.1.3	Asset Management Reporting
6.1.3.1	Monthly Asset Report
6.1.3.2	Ad hoc Reports
6.2	RESERVED
6.2.1	RESERVED
6.2.1.1	RESERVED
6.2.1.2	RESERVED
6.2.1.3	RESERVED
6.3	RESERVED
6.3.1	RESERVED
6.3.2	RESERVED
6.3.2.1	RESERVED
6.3.2.2	RESERVED
6.3.2.3	RESERVED

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	207

APPENDIX G – APPLICABLE LAWS, REGULATIONS, POLICIES, AND GUIDELINES

The law, regulations, policies, and guidelines that affect the system include:

- **U.S. Congress - Public Law (PL) & United States Code (U.S.C)L:**
 - PL 107-347 Section III, *Federal Information Security Management Act (FISMA) of 2002*, 2002
 - PL 107-305, *Cyber Security Research and Development Act of 2002*
 - PL 96-456, *Classified Information Procedures Act of 1980*
 - 5 U.S.C. 552, *Freedom of Information Act; Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings*, 1967
 - 5 U.S.C. 552a, *Privacy Act; Records Maintained on Individuals*, 1974
 - 18 U.S.C. 1029, *Fraud and Related Activity in Connection with Access Devices*
 - 18 U.S.C. 1030, *Fraud and Related Activity in Connection with Computers*
 - 40 U.S.C. 1401 et seq., P.L. 104-106, *Clinger Cohen Act of 1996 (Information Technology and Management Reform Act of 1996)*
 - 44 U.S.C. 3534, *Federal Agency Responsibilities*
 - 44 U.S.C. 3535, *Annual Independent Evaluation*
 - 44 U.S.C. 3537, *Authorization of Appropriations*
 - 44 U.S.C. 3541, P.L. 107-296, *Federal Information Security Management Act of 2002 (FISMA)*
 - 44 U.S.C. 3546, *Federal Information Security Incident Center*
- **Executive Orders - Office of Management and Budget (OMB) Circular, Homeland Security Presidential Directive (HSPD), Presidential Decision Directive (PDD):**
 - OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems*, 2000
 - HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, 2004
 - PDD-63, *Critical Infrastructure Protection*, 1998
- **DHS Management Directive (MD):**
 - DHS MD 4100.1, *Wireless Management Office*

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	208

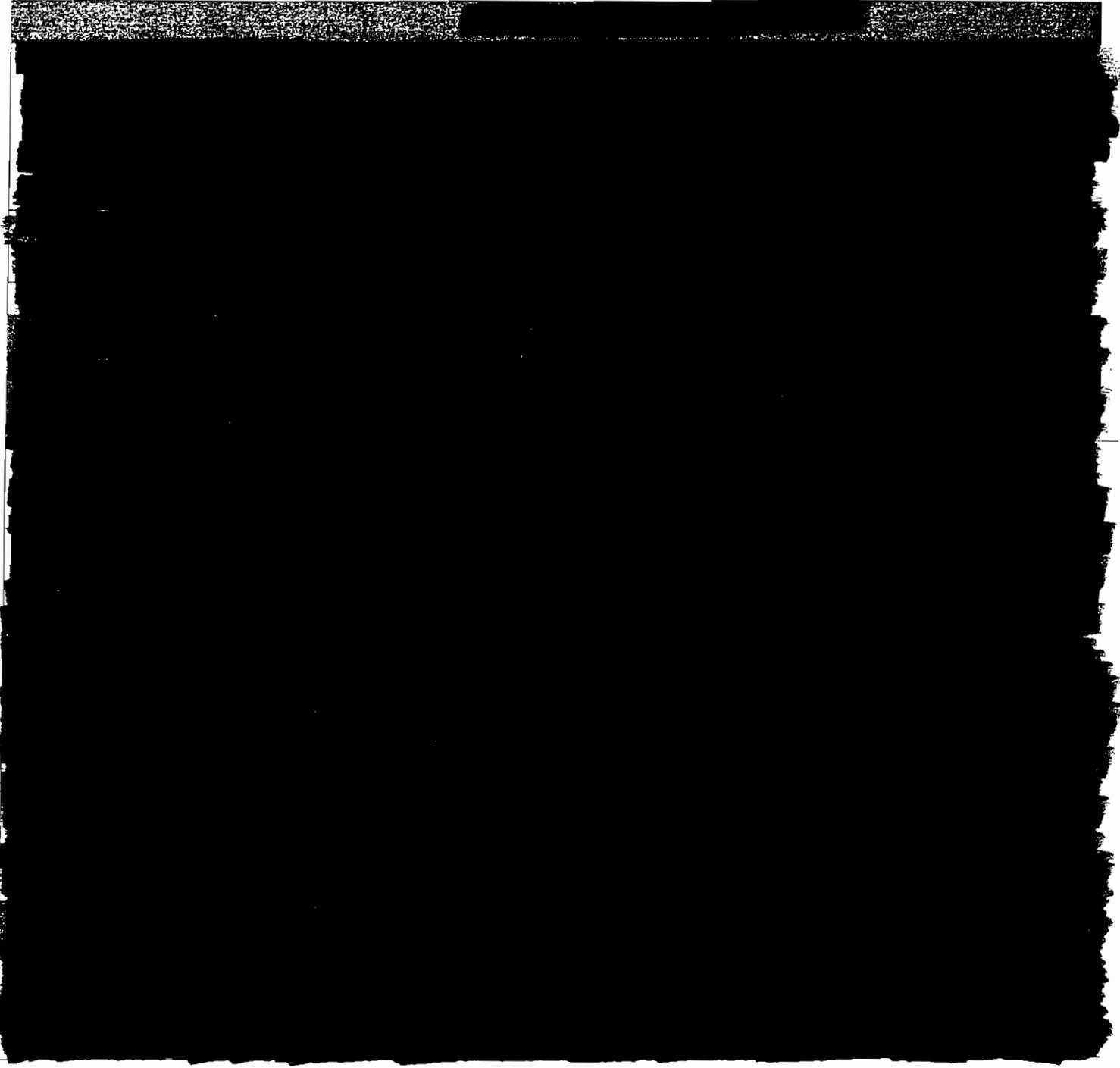
- DHS MD-4300A, DHS Policy Guide for Sensitive Systems
- DHS MD 4900, Individual Use and Operation of DHS Information Systems/Computers
- DHS MD 11030.1, Physical Protection of Facilities and Real Property
- DHS MD 11053, Security Education, Training, and Awareness Program Directive
- **National Institute of Standards and Technology (NIST) - Special Publications (SP) and Federal Information Processing Standards Publications (FIPS PUBS):**
 - FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, 2003
 - 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, 2004
 - 800-34, Contingency Planning Guide for Information Technology Systems, 2002
 - 800-30, Risk Management Guide for Information Technology Systems, 2002
 - 800-26, Revised NIST SP 800-26 System Questionnaire with NIST SP 800-53 References and Associated Security Control Mappings, 2005
 - 800-18, Guide for Developing Security Plans for Information Technology Systems, 1998
- **Additional NIST Guidelines:**
 - 800-70, The NIST Security Configuration Checklists Program
 - 800-68, Draft NIST Special Publication 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist, 2004
 - 800-65, Integrating Security into the Capital Planning and Investment Control Process, 2005
 - 800-64, Security Considerations in the Information System Development Life Cycle, 2004
 - 800-61, Computer Security Incident Handling Guide, 2004
 - 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, 2004
 - 800-59, Guideline for Identifying an Information System as a National Security System, 2003
 - 800-55, Security Metrics Guide for Information Technology Systems, 2003
 - 800-53, Recommended Security Controls for Federal Information Systems, 2005

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	209

- 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, 2002
- 800-50, Building an Information Technology Security Awareness and Training Program, 2003
- 800-47, Security Guide for Interconnecting Information Technology Systems, 2002
- 800-45, Guidelines on Electronic Mail Security, 2002
- 800-42, Guideline on Network Security Testing, 2003
- 800-41, Guidelines on Firewalls and Firewall Policy, 2002
- 800-40, Procedures for Handling Security Patches, 2002
- 800-36, Guide to Selecting Information Security Products, 2003
- 800-35, Guide to Information Technology Security Services, 2003
- 800-31, Intrusion Detection Systems (IDS), 2001
- 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, 2004
- 800-23, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, 2000

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 210
--------------	--------------	--	---------------

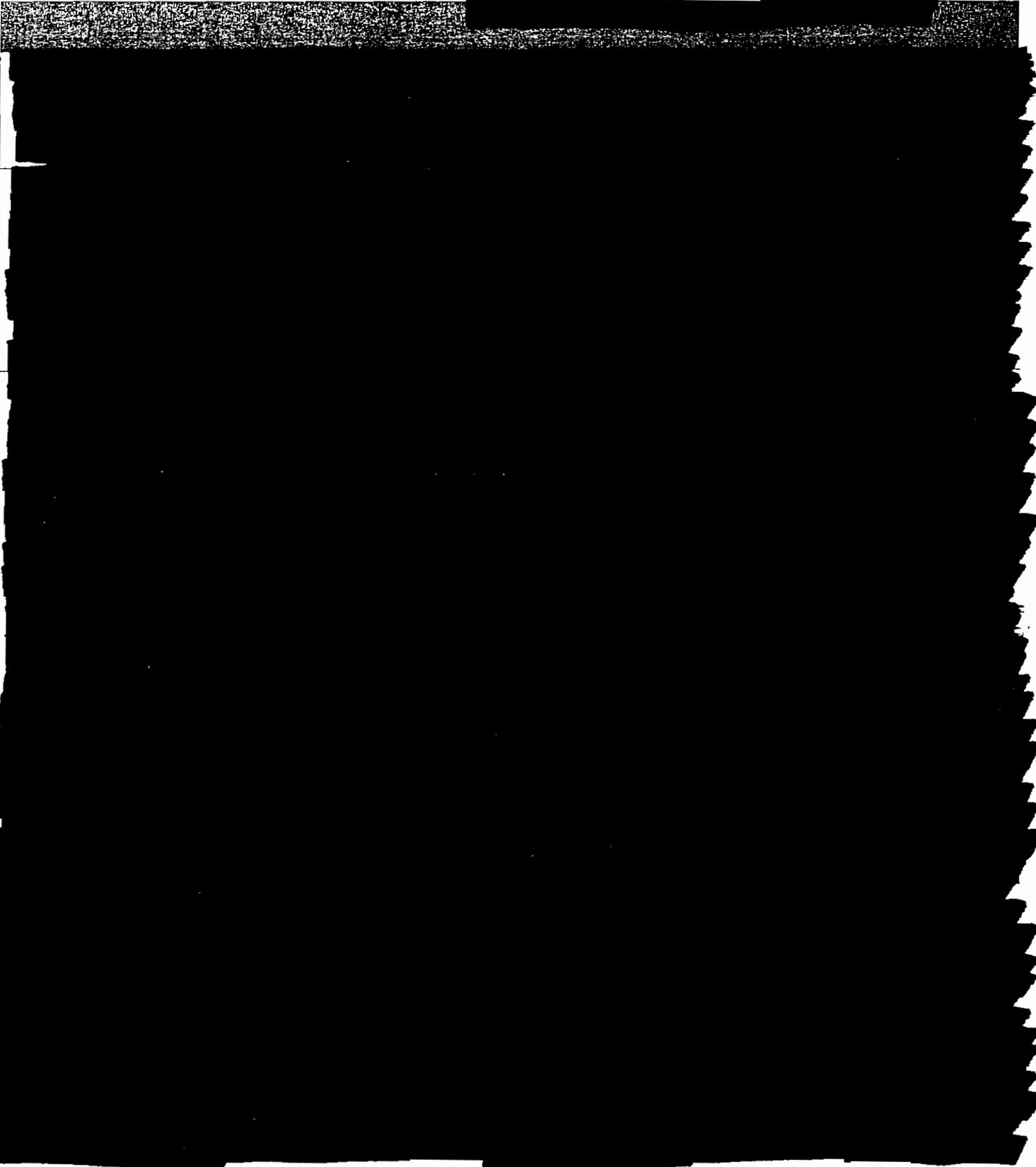
APPENDIX H – SERVICE LEVEL AGREEMENTS



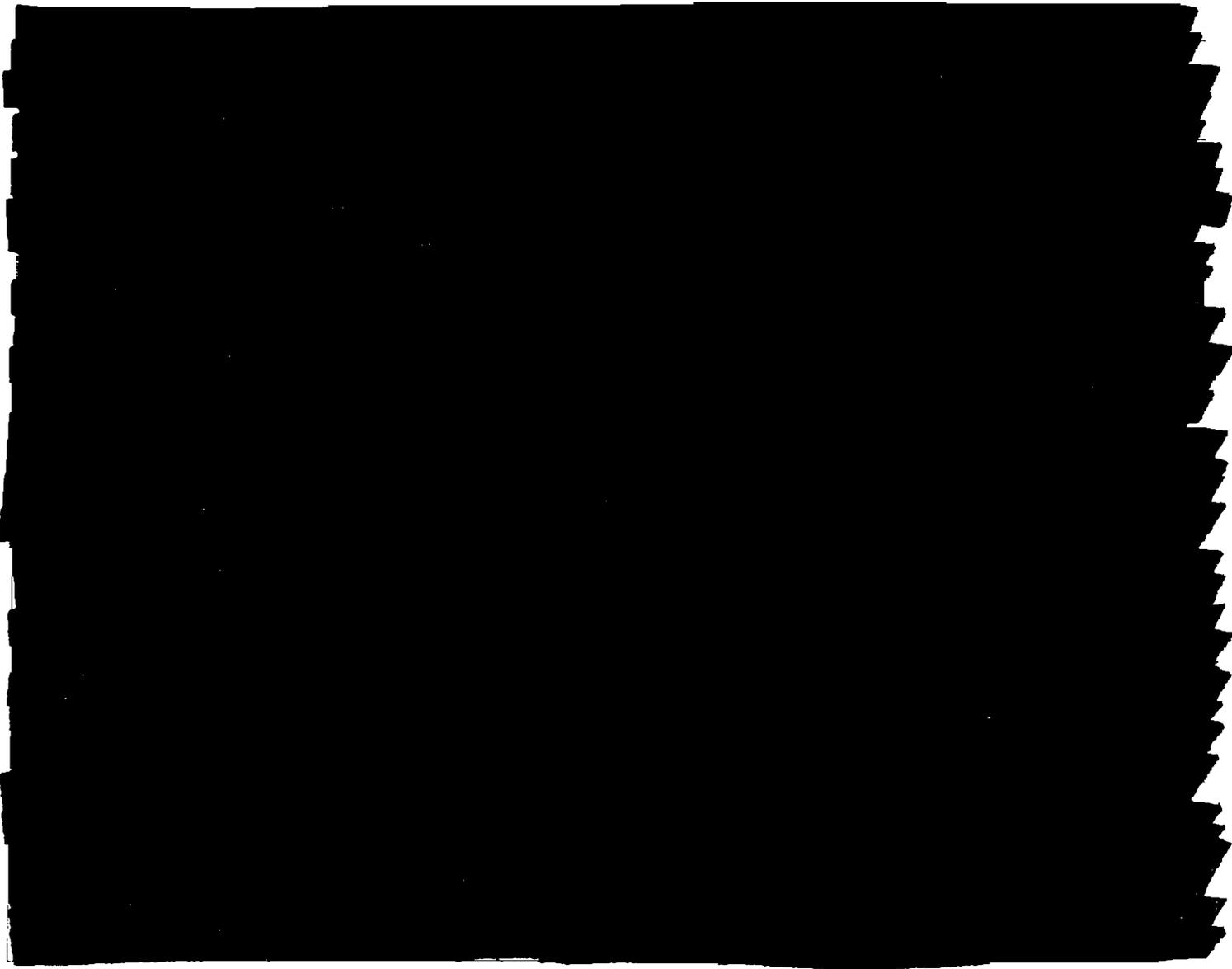
b4

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 211
--------------	--------------	--	---------------

b4



Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 212
--------------	--------------	--	---------------



b4

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	213

[Redacted]

[Redacted]

b4

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 214
--------------	--------------	--	---------------

b4



Solicitation

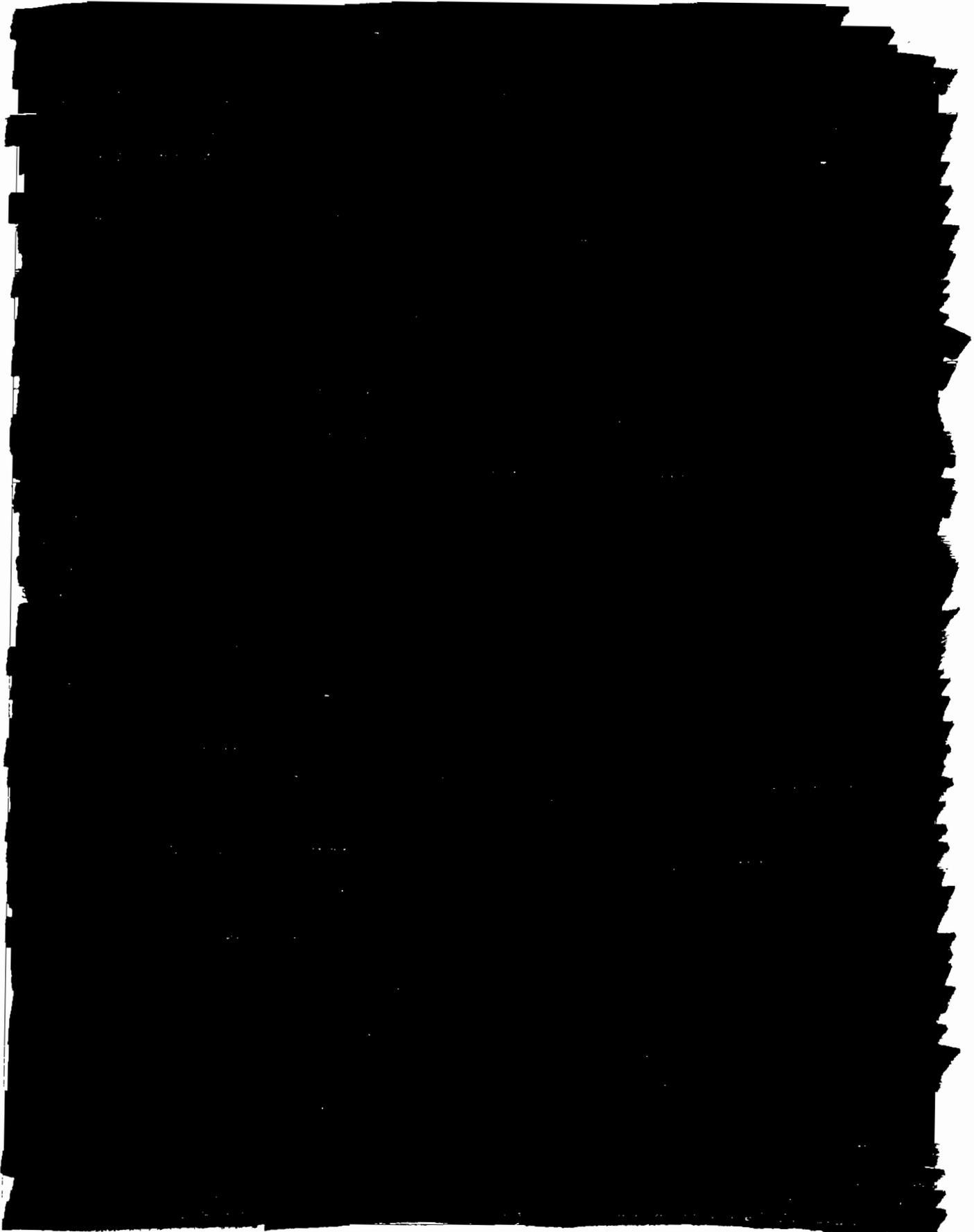
Document No.

Document Title

ITMS Bridge Contract

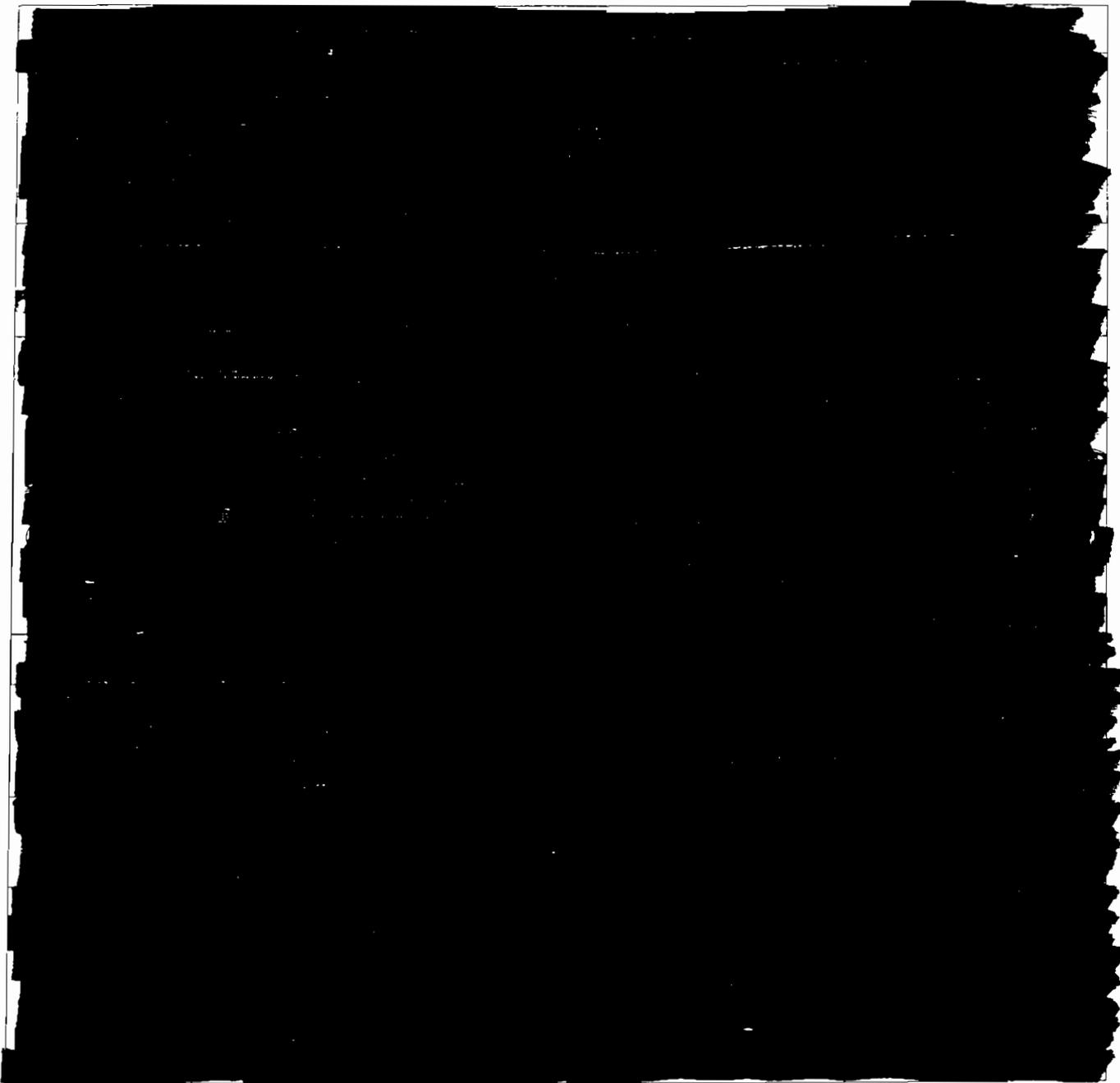
Page #

215



b4

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 216
--------------	--------------	--	---------------



b4

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	217

[Redacted]

[Redacted]

b4

Solicitation

Document No.

Document Title

Page #

ITMS Bridge Contract

218

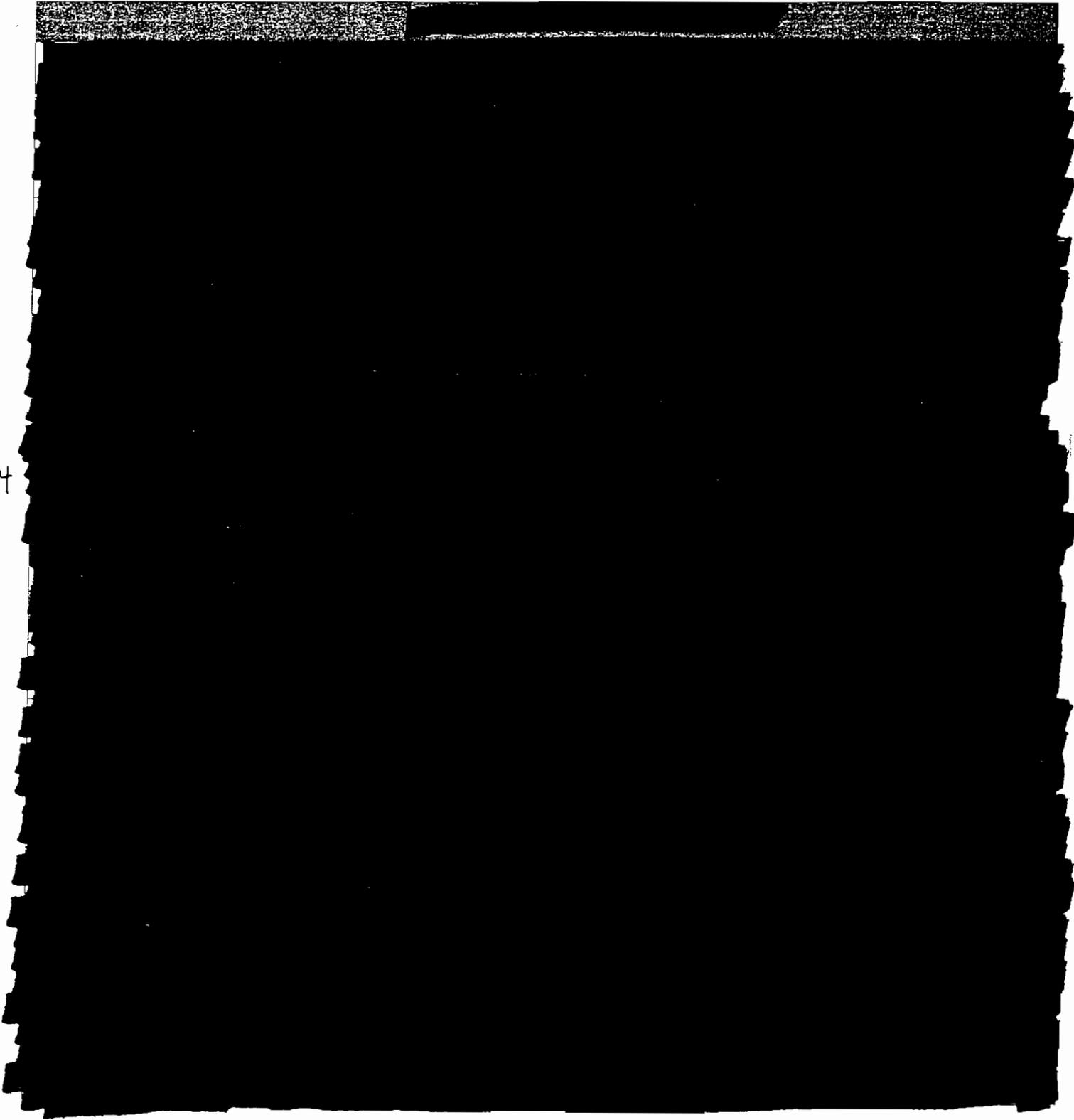
[Redacted]

[Redacted]

b4

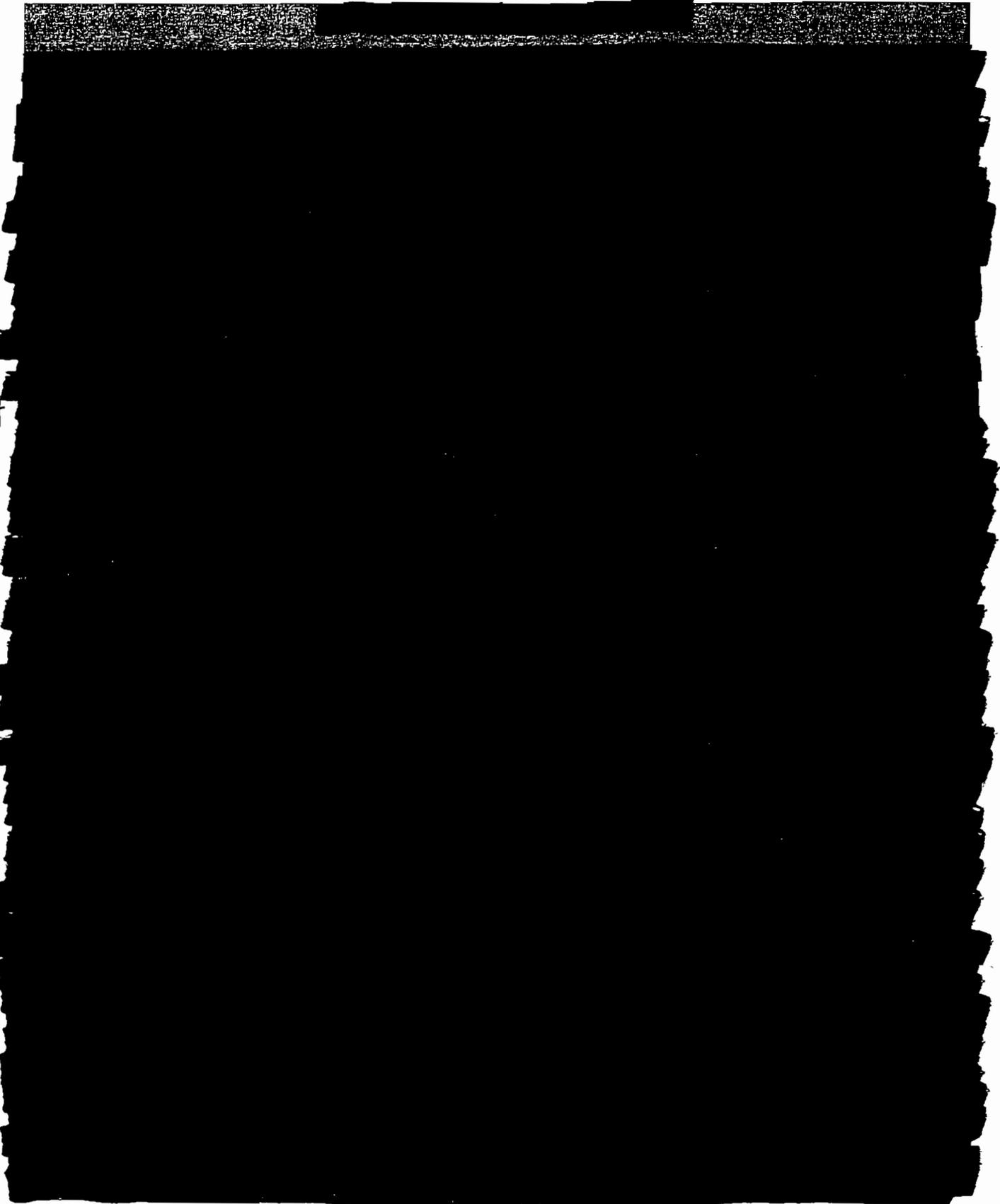
Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	219

b4



Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 220
--------------	--------------	--	---------------

b7

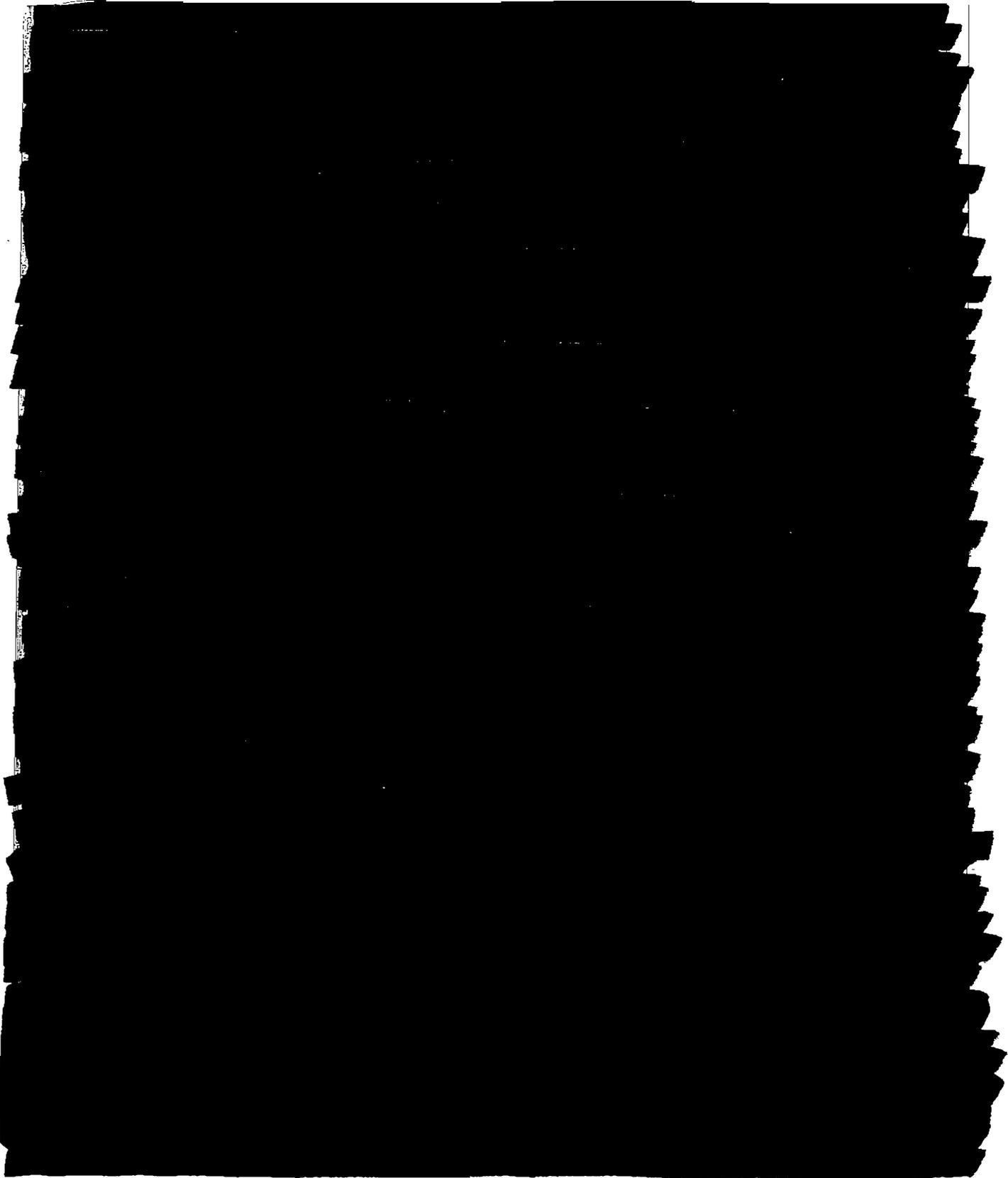


Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 221
--------------	--------------	--	---------------

b4



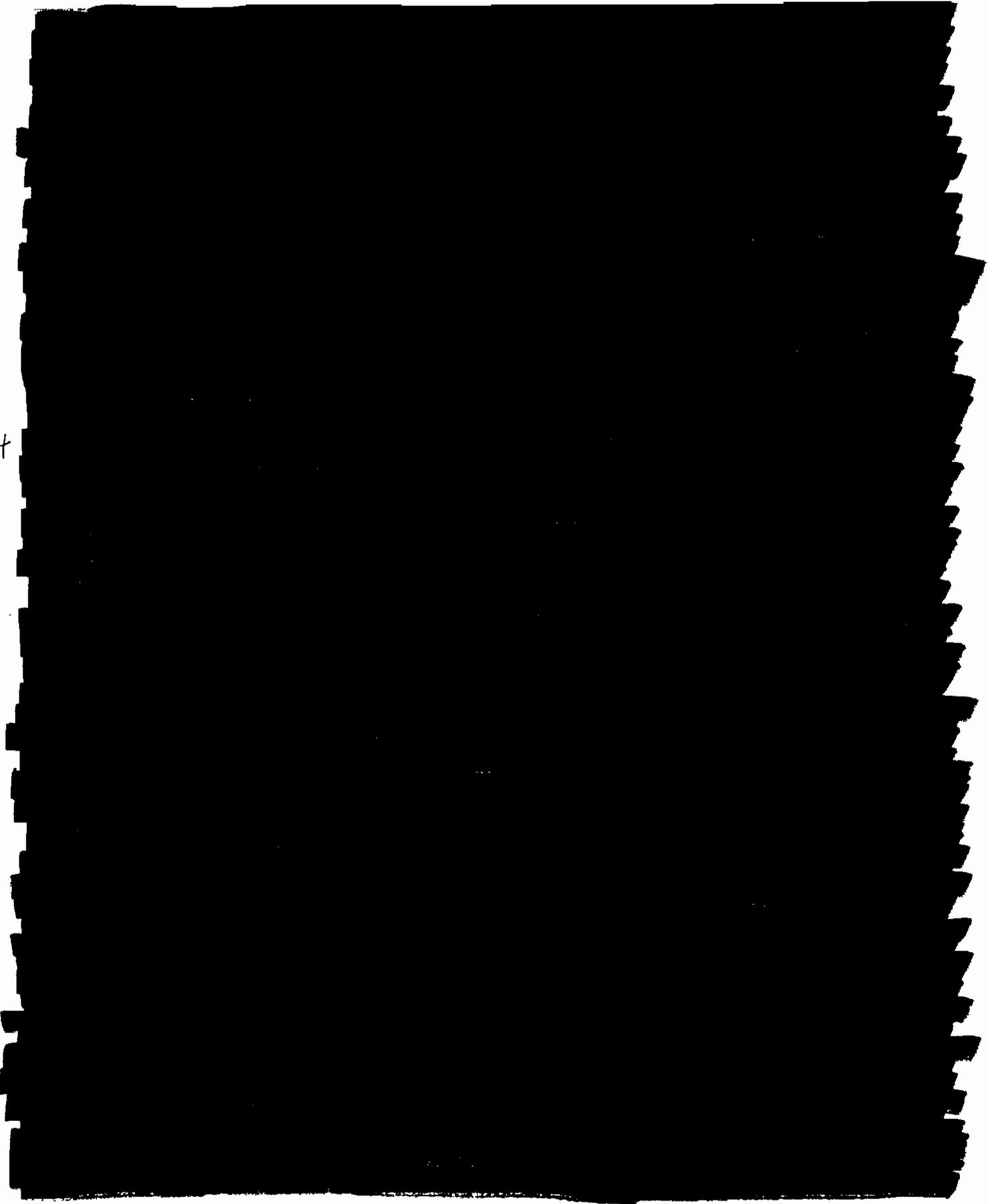
Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 222
--------------	--------------	--	---------------



b4

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 223
--------------	--------------	--	---------------

b4



Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 224
--------------	--------------	--	---------------

b4



Solicitation

Document No.

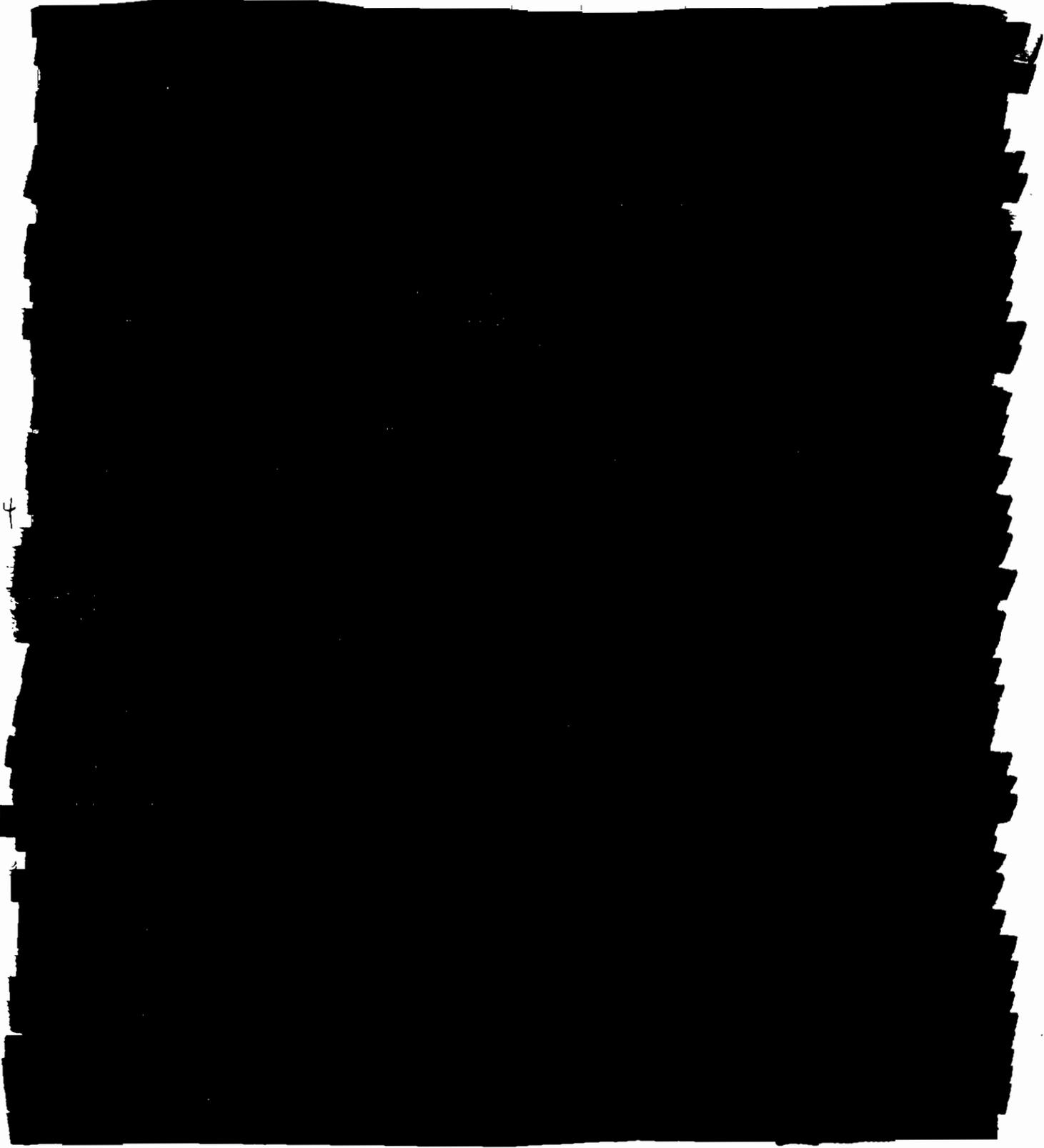
Document Title

Page #

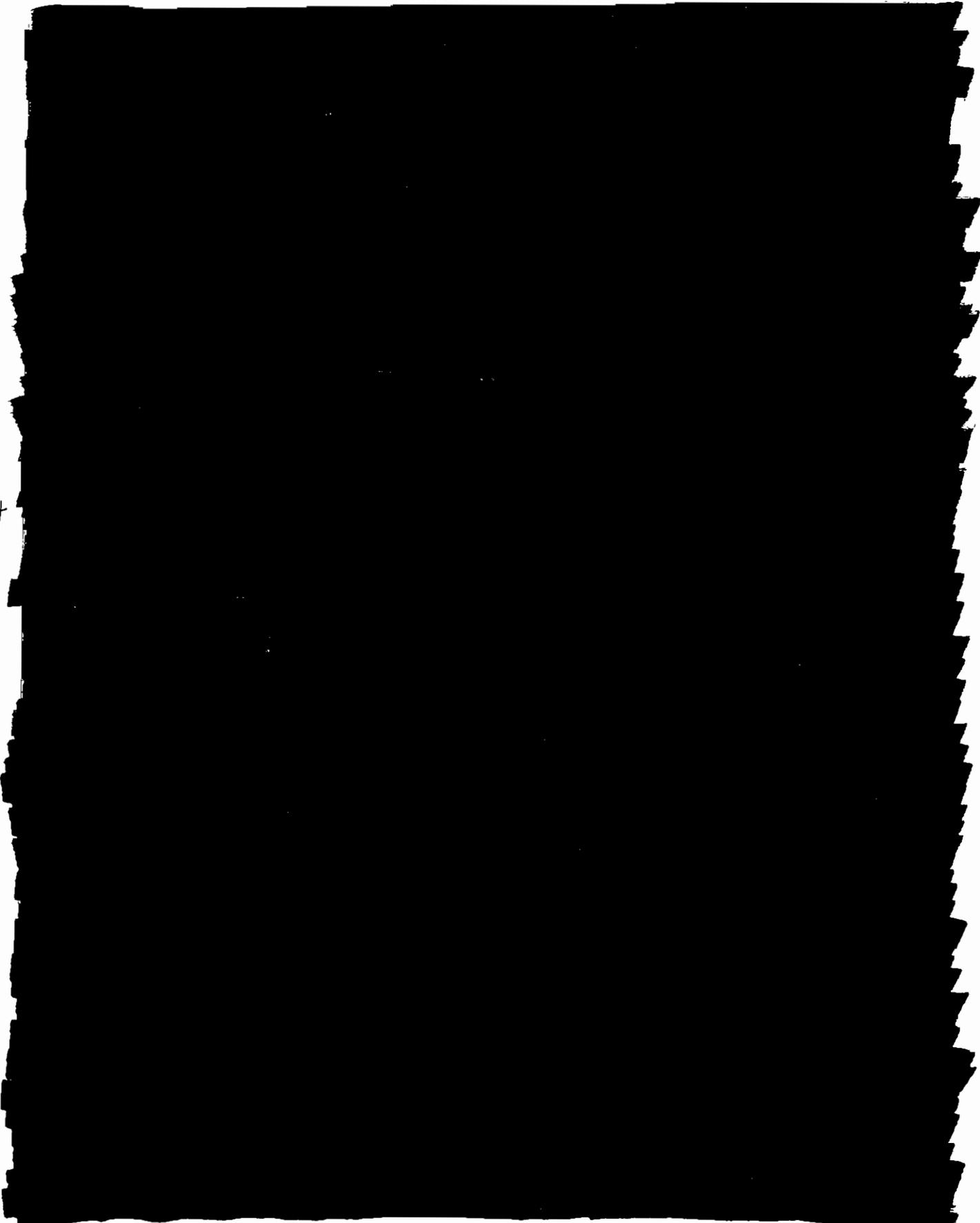
ITMS Bridge Contract

225

b4



Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 226
--------------	--------------	--	---------------



b4

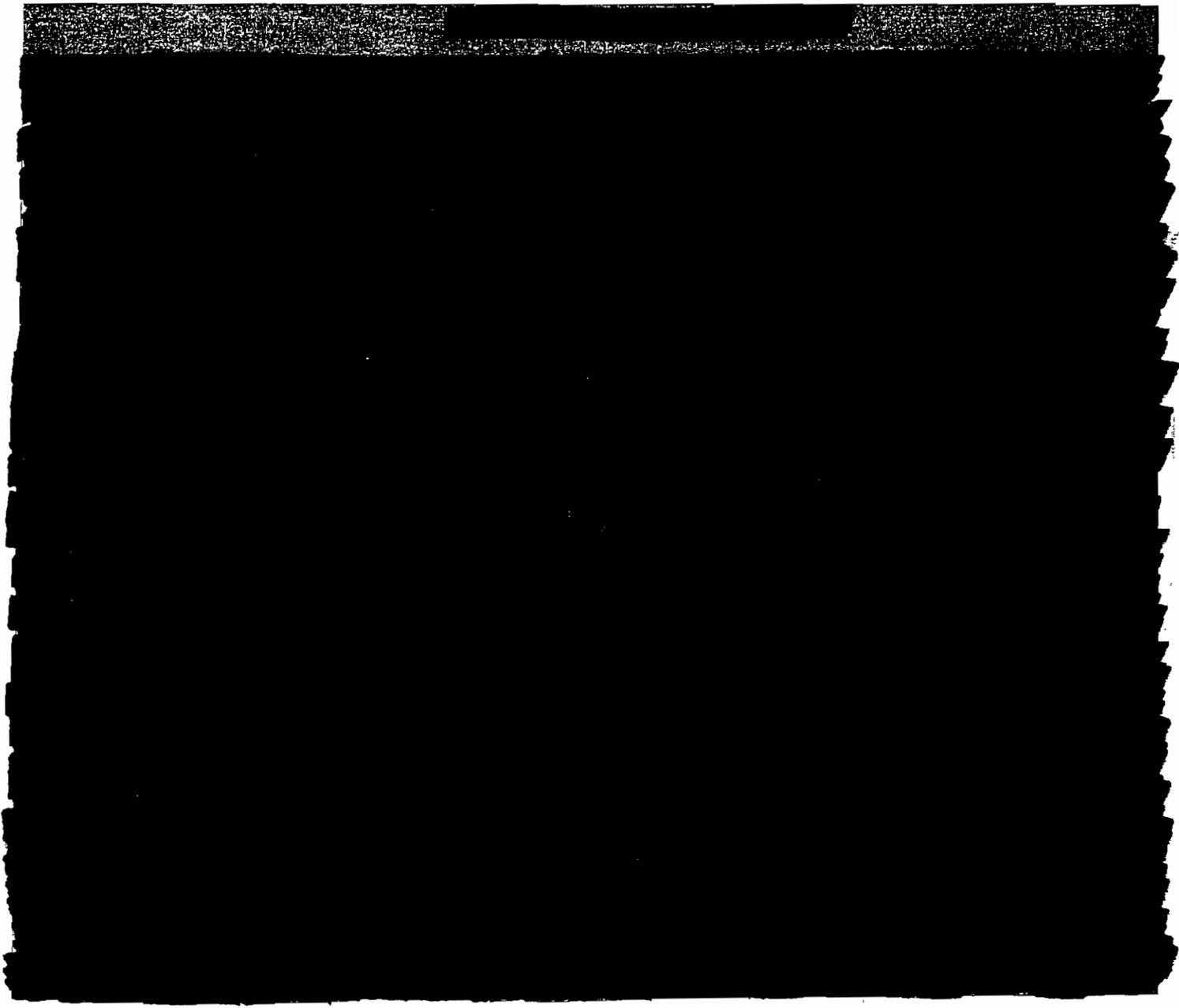
Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 227
--------------	--------------	--	---------------

b4



Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 228
--------------	--------------	--	---------------

b4



Solicitation

Document No.

Document Title
ITMS Bridge Contract

Page #
229

[REDACTED]

b4

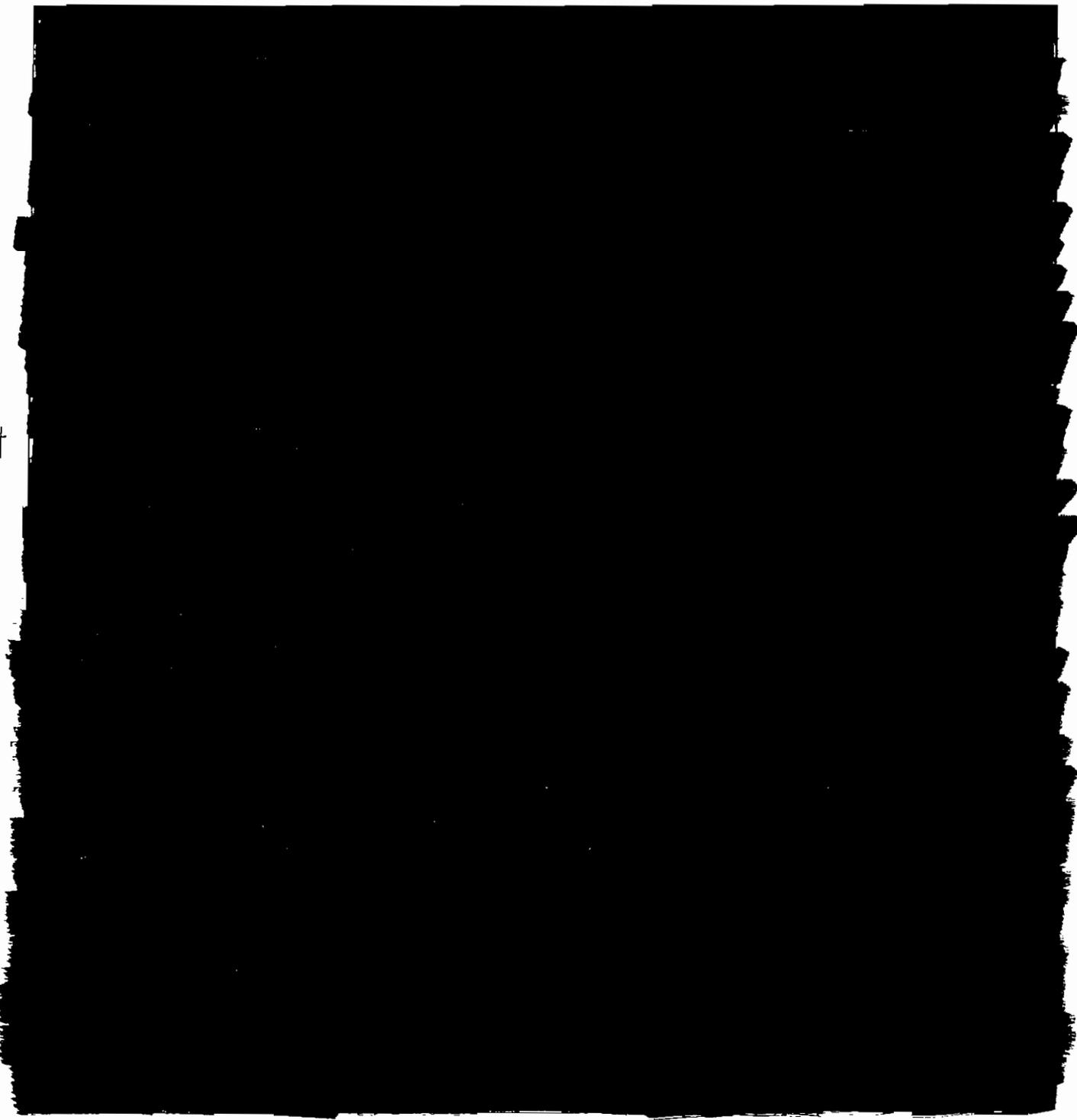
Solicitation

Document No.

Document Title
ITMS Bridge Contract

Page #
230

b4



Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 231
--------------	--------------	--	---------------

b4



Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 232
--------------	--------------	--	---------------

SECTION D—PACKAGING AND MARKING

D.1 PACKAGING AND MARKING

The Contractor shall preserve, pack, and mark for shipment items for delivery under this contract in accordance with good commercial practices and adequate to ensure both acceptance by common carrier and safe transportation at the most economical rate(s).

Containers shall be clearly marked as follows:

- Name of Contractor
- Contract Number
- Task Order Number
- Description of Items Contained Therein
- Consignee's Name and Address
- Date of Document

The Contractor shall place identical requirements on all subcontracts; however for direct delivery from 3rd party vendors the Contractor shall follow standard commercial practices.

The Contractor pricing shall include FOB Destination charges for delivery within 30 days after receipt of an accepted, funded Service Order. FOB Destination pricing shall be provided for the 48 contiguous United States only. The Contractor shall address OCONUS (to include Hawaii and Alaska) on a case-by-case basis as required. This applies to non-premium services; specifically, the Contractor shall acknowledge and include in their proposed pricing the expedited delivery requirements as provided for premium and premier service levels. If the Government requires expedited delivery for standard service levels, the Contractor shall provide a separate submission and handle these on a case-by-case basis.

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	233

SECTION E—INSPECTION AND ACCEPTANCE

E.1 GENERAL

This section sets forth requirements for inspection and acceptance. This section also applies to all replacement systems and equipment, substitute equipment, or other individual items of equipment ordered throughout the term of the contract.

E.2 TSA 3.1.1 CLAUSES INCORPORATED BY REFERENCE

This contract incorporates by reference one or more provisions or clauses listed below with the same force and effect as if they were given in full text. The clauses are located on the internet at: <http://www.tsa.gov/public/display?theme=84&content=0900051980013479>

TSA Clause No.	Title	Date
3.10.4.16	Responsibility for Supplies.	FEB 2003
3.10.4.2	Inspection of Supplies-Fixed-Price.	FEB 2003
3.10.4.4	Inspection of Services-Both Fixed-Price and Cost Reimbursement	FEB 2003
3.10.4.5	Inspection-Time-and-Material and Labor-Hour.	FEB 2003

Additional inspection and acceptance requirements may be identified in future delivery or task orders.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 234
---------------------	--------------	--	---------------

SECTION F—DELIVERIES OR PERFORMANCE

F.1 CLAUSES INCORPORATED BY REFERENCE (TSA 3.1.1)

This RFP or contract, as applicable, incorporates by reference one or more provisions or clauses listed below with the same force and effect as if they were given in full text.

TSA Clause No.	Title	Date
3.10.1.11	Government Delay of Work	FEB 2003
3.10.1.9	Stop-Work Order	FEB 2003
3.10.1.24	Notice of Delays	FEB 2003
3.11.34	F.O.B. Destination	FEB 2003

F.2 PERIOD OF PERFORMANCE

The period of performance shall be a one-year base period from effective date of award with two one-year option periods.

F.3 PLACE OF PERFORMANCE

The Contractor shall perform the work under this contract at locations specified in Section C.

F.4 DELIVERY OF REPORTS

Unless otherwise specified, deliverables as specified herein shall be addressed to: the Transportation Security Administration, TSA-11, Attn: [COTR], 601 South 12th Street, Arlington, VA 22202, marked with the contract number, to the attention of the appropriate Contracting Office recipient.

F.5 DELIVERABLES

F.5.1 This section identifies the items that the Contractor shall deliver to the Government. In this section, the items the Contractor delivers are called "deliverables." Deliverables shall be provided via electronic mail, and or in hard copy, as specified in table F-1 Deliverables. Deliverables shall be submitted in accordance with dates and timeframes identified in Section F, Table of Deliverables and the format prescribed in Section F.5.2. The Contractor shall provide a preliminary deliverable in accordance with the date specified in Section F, Table of Deliverables and as referenced in Section C. The Government has up to 3 cycles to review and comment on such deliverables. After such review processes the deliverables shall be finalized and submitted as a final and accepted deliverable.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 235
--------------	--------------	--	---------------

The Government will review and accept/reject deliverables within ten (10) working days. The Contractor records responses gathered from the customer feedback forms that are provided to TSA upon formal delivery of documents. The Contractor shall track acceptance of deliverables.

Work products are due as specified in Section F, but may not be subject to the deliverable review process:

F.5.2 The following standards apply with the creation, formatting, and delivery of documentation:

- For deliverables specified in Section F, the Contractor shall deliver electronic copies, in the named electronic formats, at version levels compatible with the current release of the stated formats.
- Textual materials shall be provided in Microsoft Word (current release).
- Graphical Material shall be provided in Microsoft PowerPoint (current release).
- Statistical related charts, graphs and other spreadsheet material shall be provided in Microsoft Excel (current release).
- Hardcopy documentation of 50 pages or more shall be bound in a suitable manner.
- Be clear, concise and understandable.
- Specifically define what is required to be accomplished in performance-based, quantitative terms, for each sub-task applicable to include—assumption of existing services, transition services and implementation of managed services and interrelationship consistent with this Performance Work Statement.
- Fully demonstrate understanding of objectives, mandates, coordination activities and requirements necessary to accomplish TSA objectives.
- Softcopy documentation shall be delivered on CD ROM media.
- The Contractor shall deliver three (3) hard copies and one (1) electronic media for all deliverables unless specified otherwise by the Government.

F.6 DATA ITEMS

In addition to deliverables and work products produced by the Contractor, the Contractor shall deliver data items as defined in Section J hereto.

The following standards apply with the creation, formatting, and delivery of data item documentation:

- Textual materials shall be provided in Microsoft Word (current release).
- Graphical Material shall be provided in Microsoft PowerPoint (current release).
- Statistical related charts, graphs and other spreadsheet material shall be provided in Microsoft Excel (current release).
- Hardcopy documentation of 50 pages or more shall be bound in a three ring binder.
- Visio

F.7 SUBCONTRACT REPORTS

F.7.1 The Contractor shall submit a subcontracting report for this contract on Standard Form 294 and 295 (see Attachment 11, Section J). The report shall be submitted semi-annually in accordance with the General Instructions on the reverse side of the form. The original report shall be submitted to the

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 236
---------------------	--------------	--	---------------

TSA, Small & Disadvantaged Business Utilization Program Manager with a copy to the Contract Officer.

F.7.2 An electronic subcontracting reporting system (eSRS) is being developed which will allow Contractors to enter both SF 294 and SF 295 into a single website that is part of eSRS (see <http://www.esrs.gov/>). Training will be provided for both industry and Government before the system is implemented. After eSRS is implemented, the Contractor is expected to submit all their reports electronically to eSRS. The Contractor shall be responsible for inputting accurate and complete reports.

F.7.3 The Contractor's Small Business Subcontracting Plan dated July 18, 2006 and the goals established therein are hereby incorporated by reference.

F.8 MONTHLY SUBCONTRACTING ACTIVITY REPORT (MSAR)

F.8.1 The Contractor shall report on a monthly basis all subcontracting activity related to the contract. The MSAR supplements, but does not replace, the SF294 and 295 small business reporting requirements. At a minimum, the MSAR should include the following information for each Subcontractor regardless of size: Subcontractor Name, DUNS Number, point of contact, phone number, city and state, business type code, NAICS, anticipated value of subcontract, amount spent (paid) this month, and amount spent (paid) to date. A summary sheet rolling the data should also be submitted with the report.

F.8.2 The MSAR is required when due, regardless of whether there has been any subcontracting activity since the inception of the contract or since the previous report.

F.8.3 Purchase from a corporation, company, or subdivision that is an affiliate of the prime are not included in this report.

F.8.4 MSAR data reported by prime Contractors shall be limited to awards made to their immediate Subcontractor(s). Credit cannot be taken for awards made to lower tier Subcontractor(s).

F.8.5 This report shall be transmitted electronically to the TSA, Small & Disadvantaged Business Utilization Program Manager with copies to the Contract Officer and COTR.

F.9 VENDOR REPORT: CONTRACTUAL FINANCIAL OPERATIONS AND PROJECTIONS

The Transportation Security Administration (TSA) Office of the Chief Information Officer (OCIO) will be responsible for monitoring the performance of projects performed by the selected vendor. In this section, costs represent the total costs, inclusive of fee, to the Government. The OCIO will evaluate projects and programs with regard to cost to the Government, schedule, and performance to assure customers and stakeholders of the successful operation and subsequent completion of all activities performed under the contract. The Contractor shall be responsible for reporting, on a monthly basis, the financial status of all projects (new, recurring, and/or completed) in an Estimate To Complete Report (ETC). Project status reports require delineation by the elements composing the project scope. The financial status reports shall be tracked in unison with the scope developed in the cost and technical proposal submitted by the Contractor. The cost elements proposed for each project

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 237
--------------	--------------	--	---------------

shall be tracked individually to allow for TSA to complete an independent cost analysis. The cost/price (as applicable) element line items are defined below:

- Recurring Equipment
- One-Time/Purchase
- Time and Materials Labor
- Firm Fixed Price Tasks
- Other Direct Charges

The Contractor shall provide estimated costs/price projections for each line item under a project for each month of the fiscal year. The line items shall be rolled up into quarterly projections for that period of estimate, and subsequently rolled up into a yearly estimate. As each report is submitted, the cost for months/quarters prior to the reporting period shall be updated with current costs to date.

Funding obligated/applied to the contract throughout the fiscal year shall also be included in the report. All funds placed on contract shall be assigned to the appropriate project as specified in the contract or contract modification. The report shall capture a cumulative total of all funding placed on contract for each project. Once a new fiscal year begins, any/all unliquidated obligations or costs are to be posted as the beginning balance for the following fiscal year.

F.10

[REDACTED]

[REDACTED]

[REDACTED]

b4

[REDACTED]

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	238

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b4

[REDACTED]

b4

[REDACTED]

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 240
--------------	--------------	--	---------------

b4

[REDACTED]
[REDACTED] can be provided in one consolidated report under the requirements of the Asset Management Solution.

Table F-1 Deliverables/Work Products

See Section J, Attachments.

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	241

SECTION G—CONTRACT ADMINISTRATION DATA

G.1 CONTRACT OFFICER (CO)

The Contract Officer is the only person authorized to make any changes, approve any changes in the requirements of this contract, issue service orders, obligate funds and authorize the expenditure of funds, and notwithstanding any provisions contained elsewhere in this contract, the said authority remains solely in the Contract Officer. In the event, the Contractor makes any changes at the direction of any person other than the Contract Officer, the change will be considered to have been without authority and no adjustment will be made in the contract price to cover any increase in costs occurred as a result thereof. It is incumbent on the Contractor to make sure that this requirement is enforced, or work performed will be performed at the Contractor's own risk.

The following Primary Contracting Officers are assigned to this contract. Alternate Contracting Officers may be assigned:

TSA Contracting Officer:

NAME: Christopher E. Zeleznik
PHONE NO.: 571-227-1605
EMAIL: Christopher.Zeleznik@dhs.gov

DHS Contracting Officer:

NAME: Tina Honey
PHONE NO.: (202) 772-0904
EMAIL: Tina.Honey@dhs.gov

G.2 CONTRACT OFFICER'S TECHNICAL REPRESENTATIVE (COTR) AND TECHNICAL MONITORS

G.2.1 The principle role of the COTR is to support the Contract Officer in managing the business agreement. This is done through furnishing technical direction within the confines of the agreement, monitoring performance, ensuring requirements are met within the terms of the contract, and maintaining a strong relationship with the Contract Officer. As a team the Contract Officer and COTR must ensure that program requirements are clearly communicated and that the agreement is performed to meet them. The principle role of the TM is to support the COTR on all work orders, tasks, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.

G.2.2 The Contract Officer hereby designates the individual(s) named below as the Contract Officer's Technical Representative(s) and Technical Monitor(s). Such designations(s) shall specify the scope and limitations of the authority so delegated.

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	242

TSA COTRs:

NAME: Boris DeSouza
PHONE NUMBER: (571) 227-3003
EMAIL: Boris.Desouza@dhs.gov

NAME: Jim Workman
PHONE NUMBER: (571) 227-4180
EMAIL: James.Workman@dhs.gov

NAME: Gerald Voorhies
PHONE NUMBER: (571) 227-1557
EMAIL: George.Voorhies@dhs.gov

ALTERNATIVE TSA COTR (FOR SUBMISSION OF INVOICES):

NAME: Marthanne Kleinhample
PHONE NUMBER: (571) 227-3830
EMAIL: Marthan.kleinhample@dhs.gov

DHS HQ COTR:

NAME: Beth Killoran
PHONE NUMBER: (571) 227-4319
EMAIL: Beth.Killoran@dhs.gov

G.2.3 The COTR(s) AND TM(s) may be changed at any time by the Government without prior notice to the Contractor, but notification of the change, including the name and phone number of the successor COTR, will be promptly provided to the Contractor by the Contract Officer in writing.

G.2.4 The responsibilities and limitations of the COTR are as follows:

- The COTR is responsible for the technical aspects of the project and technical liaison with the Contractor. The COTR is also responsible for the final inspection and acceptance of all reports and such other responsibilities as may be specified in the contract.
- The COTR may designate assistant COTR(s) to act for him/her by naming such assistant in writing and transmitting a copy of such designation through the Contracting Officer to the Contractor.
- The COTR will maintain communications with the Contractor and the Contracting Officer. The COTR must report any observed fraud, waste, or opportunities to improve performance of cost efficiency to the Contracting Officer.
- The COTR will immediately alert the Contracting Officer to any possible Contractor deficiencies or questionable practices so that corrections can be made before the problems become significant.
- The COTR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes which affect the Contract price, terms or conditions. Any Contractor request for changes shall be referred to the Contracting Officer directly or through the COTR. No such changes shall be made without the expressed prior authorization of the Contracting Officer.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 243
--------------	--------------	--	---------------

- The COTR is not authorized to direct the Contractor on how to perform the work.
- The COTR is not authorized to issue stop-work orders. The COTR must inform the Contracting Officer of the recommendation to stop work, but the Contracting Officer is the only person authorized to issue the order.
- The COTR is not authorized to discuss new proposed efforts or encourage the Contractor to perform additional efforts on an existing contract or order.

G.2.5 The responsibilities and limitations of the TM are as follows:

- Coordinating with the COTR on all work order, task, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action
- Monitoring the Contractor's performance in relation to the technical requirements of the assigned functional area of the contract to ensure that the Contractor's performance is strictly within the contract's scope and obligated funding
- Ensuring that all recommended changes in any work under the contract are coordinated and submitted in writing to the COTR for consideration
- Ensuring that the Contractor does not begin unauthorized work
- Informing the COTR if the Contractor is not attaining the schedule or meeting cost milestones
- Performing technical reviews of the Contractor's proposals as directed by the COTR
- Performing acceptance of the Contractor's deliverables as directed by the COTR
- Reviewing invoices and certify them for payment as directed by the COTR
- Reporting any threats to the health and safety of persons or potential for damage to Government property or critical national infrastructure which may result from the Contractor's performance or failure to perform the contract's requirements

G.3 ORDERING (TSA 3.2.4.16) (JUN 2005)

Any supplies and services to be furnished under this contract shall be ordered by issuance of task orders and delivery orders. Such orders may be issued from date of contract award through 36 months from date of contract award (if all options are exercised).

All orders are subject to the terms and conditions of this contract. In the event of conflict between an order and this contract, the contract shall control.

If mailed, an order is considered "issued" when the Government deposits the order in the mail. Orders may also be issued by facsimile, or by electronic methods.

Only warranted Contract Officers are authorized to issue task orders and service orders. Ordering Officers may only order equipment or services covered in Sections B and C as represented by existing CLINs.

G.4 ACCOUNTABILITY OF COSTS/SEGREGATION OF TASK ORDERS

For Time and Materials orders costs incurred by the Contractor under this contract shall be segregated in accordance with proper accounting procedures. The Contractor shall, therefore, establish separate job order accounts and numbers for each task and shall record all incurred costs in

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 244
--------------	--------------	--	---------------

the appropriate job order account assigned each task. There shall be no commingling of costs between options.

G.5 INVOICE REQUIREMENTS

G.5.1 It is the responsibility of the TSA to ensure that all services/products have been delivered by the Contractor prior to acceptance and payment. The Contractor shall submit original TSA invoices to the Coast Guard Finance Center in accordance with the address listed in section G.6 below.

G.5.2 The Contractor shall separate the type of support billed to TSA into three categories: Equipment; Time and Materials Labor, and Firm Fixed Price Tasks. Individual vouchers (under the categories listed above) shall be prepared and submitted to TSA using the same criteria employed to obligate funding on the delivery or task order. A separate invoice should be provided each month for the support billed to TSA. In addition, a fully completed Standard Form (SF) 1034 (See Section J, Attachment 2) shall accompany each separate Contractor invoice. As applicable the invoice shall have a valid Material Inspection and Receiving Report (DD250) signed by an authorized TSA Government representative for all elements contained in the invoice. A copy of each signed DD250 shall be sent to the designated COTR authorized to evaluate contractual obligations on behalf of the TSA.

G.5.3 A report of all material billed to TSA is required each month to track outstanding equipment in the "field" or residing at TSA HQ. The report shall include a status of the DD250, a Government Point-of-Contact (POC), the equipment delivery location, equipment operational location, price of each unit, lease duration, date of acquisition, and type of equipment. The data must be provided in an application that is consistent with TSA approved software, preferably Microsoft Excel or Microsoft Access format. A detailed list of invoice requirements is included in Table G-1 below. The list provides TSA required data elements for all invoices as well as individual requirements by a specific type of invoice (i.e. T&M).

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 245
--------------	--------------	--	---------------

INVOICE REQUIREMENTS---TABLE G-1

All invoices submitted to TSA shall include the information outlined in Column 1. All Time and Materials invoices shall include the information outlined in Columns 1 and 2. All Firm Fixed Price invoices shall include the information outlined in Columns 1 and 3.

Column 1	Column 2	Column 3
1. Vendor Name	1. Labor Categories	1. Price per Period
2. Invoice Number	2. Contractors Name	2. Number of Periods
3. Invoice Date	3. Number of Hours Billed	3. Site Location of Deliverables
4. Date of Service/Equipment Provided	4. Cost per Period by Labor Category	4. Description of Billed Services/Equipment
5. Payment/Vendor Address, Telephone Number, Other Contact Information	5. Site Location of Deliverables	5. Contract Line Item Number (CLIN)
6. Contract Month	6. Contract Line Item Number (CLIN)	
7. Fiscal Year	7. Description of Equipment	
8. Payment Due Date	8. Unit Cost of Equipment)	
9. Contract Number	9. Quantity	
10. Task Order Number	10. Total Direct Labor Charges	
11. Work Order Number (if applicable)	11. Total Other Direct Costs	
12. TSA Functional/Budget Code (appropriation code)	12. Subtotal per Deliverable	
13. Cumulative Value to Date (not applicable to FFP)		
14. Total Amount Invoiced		
15. Vendor Point-of-Contact		
16. TSA Point-of-Contact (COTR as identified in G.2.2)		
17. Grand Total per Invoice		
18. Page Numbers		
19. Payment terms		

The Table above is an illustration of invoicing requirements. Specific invoicing requirements will be mutually agreed to by the parties and included by contract modification within thirty (30) days after the effective date for award.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 246
---------------------	--------------	--	---------------

G.6 INVOICE SUBMISSION

G.6.1 Original invoices must be submitted to the following address:

U.S. Coast Guard Finance Center
TSA Invoices (OPC5D)
P.O. 4111
Chesapeake, VA 23326-4111

G.6.2 Duplicate TSA invoices must be submitted to the following address (COTR or Technical Monitors POC will be provided by the TSA Contracting Officer):

Transportation Security Administration
Attn: [COTR]
701 South 12th Street
Arlington, Virginia 22202

G.7 METHOD OF PAYMENT

G.7.1 Payments under this contract will be made either by check or by wire transfer through the Treasury Financial Communications System at the option of the Government.

G.7.2 The Contractor must forward the following information in writing to the CO no later than seven (7) days after receipt of notice of award:

- Full name (where practical), title, telephone number, and complete mailing address of responsible official(s):
To whom check payments are to be sent, and
 - Who may be contracted concerning the bank account information requested below.
- The following bank account information required to accomplish wire transfers:
 - Name, address, and telegraphic abbreviation of the receiving financial institution.
 - Receiving financial institution's 9-digit American Bankers Association (ABA) identifying number for routing transfer of funds. (Only provide if the receiving financial institution has access to the Federal Reserve Communication System).
 - Recipient's name and account number at the receiving financial institution to be credited with the funds.

G.8 PRICING OF ADJUSTMENTS

When costs are a factor in any determination of a contract price adjustment pursuant to the "changes" clause, or any other clause of this contract, such costs must be in accordance with the contract cost principles and procedures in the AMS in effect on the date of the contract.

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	247

G.9 TRAVEL AND PER DIEM (APPLICABLE TO T&M ORDERS ONLY)

G.9.1 The Contractor shall be reimbursed for travel costs associated with this contract. The reimbursement for those costs shall be as follows:

- Travel subsistence reimbursements will be authorized under the rates and conditions under the Federal Travel Regulations.
- Per diem will be reimbursed, at actual costs, not to exceed, the per diem rates set forth in the Federal Travel Regulations prescribed by General Services Administration and when applicable, Standardized Regulations Section 925 – Maximum Travel Per Diem Allowances for Foreign Areas – prescribed by the Department of State.
- Travel of more than 10 hours, but less than 24 hours, when no lodging is required, per diem shall be one-half of the Meals and Incidental Expenses (M&IE) rate applicable to the locations of temporary duty assignment. If more than one temporary duty point is involved, the allowance of one-half of the M&IE rate is prescribed for the location where the majority of the time is spent performing official business. The per diem allowance shall not be allowed when the period of official travel is 10 hours or less during the same calendar day.
- Airfare costs in excess of the lowest rate available, offered during normal business hours are not reimbursable.
- All reimbursable Contractor travel shall be authorized through the issuance of a task order executed by the Contract Officer.

G.9.2 Local Travel Costs will not be reimbursed under the following circumstances:

- Travel at Government installations where Government transportation is available
- Travel performed for personnel convenience/errands, including commuting to and from work; and
- Travel costs incurred in the replacement of personnel when such replacement is accomplished for the Contractor's or employee's convenience.

G.10 IMPLEMENTATION OF TASK/DELIVERY ORDERS

All work/projects shall be initiated only by issuance of a fully executed task or delivery orders issued by the Contracting Officer. Specific ordering requirements will be mutually agreed to by the parties and included by contract modification within thirty (30) days after the effective date for award.

G.11 PURCHASE AGENT AUTHORITY

The Contracting Officer may issue the Contractor a purchase agent authorization to use Government supply sources or other Government-issued contract vehicles in the performance of this contract. Title or applicable licensing rights to all property acquired by the Contractor under such an authorization shall vest in the Government unless otherwise specified in the contract. Such property shall be considered Government Property.

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	248

"Approval Authority" will be given by the Acquisition Office by letter stating the guidelines and any limitation to act on behalf of the Government and/or bind the Government.

G.12 GOVERNMENT-FURNISHED FACILITIES AND EQUIPMENT

TSA will provide administrative supplies and onsite office facilities for Contractor on-site support personnel, to include, but not limited to, a workspace, workstation, desk, and phone. Dedicated TSA-provided laptops(s) and telephone(s) will be provided for support personnel requiring TSA imaged equipment.

The Contractor shall use the Government-furnished facilities and equipment only in connection with this contract.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 249
--------------	--------------	--	---------------

SECTION H—SPECIAL CONTRACT REQUIREMENTS

H.1 TYPE OF CONTRACT (TSA 3.2.4.1) (FEB 2003)

TSA contemplates award of a Fixed Price, Indefinite Delivery/Indefinite Quantity and Time and Materials contract resulting from this contract.

H.2 EQUAL OPPORTUNITY PREAWARD CLEARANCE OF SUBCONTRACTS (TSA 3.6.2.10) (FEB 2003)

Notwithstanding the clause of this contract titled TSA 3.10.2-1, Subcontracts (Fixed-Price Contracts), the Contractor shall not enter into a first-tier subcontract for an estimated or actual amount of \$10 million or more without obtaining in writing from the Contracting Officer a clearance that the proposed Subcontractor is in compliance with equal opportunity requirements and therefore is eligible for award.

H.3 INSURANCE (TSA 3.4.1.12) (FEB 2003)

H.3.1 During the term of this contract and any extension, the Contractor shall maintain at its own expense the insurance required by this clause. Insurance companies shall be acceptable to the Transportation Security Administration. Policies that apply to covered contract work shall include all terms and provisions required by the Transportation Security Administration.

H.3.2 The Contractor shall maintain and furnish evidence of the following insurance, with the stated minimum limits:

- **Worker's Compensation and Employer's Liability.** The Contractor shall comply with applicable Federal and State workers' compensation and occupational disease statutes. The Contractor shall maintain employer's liability coverage of at least \$100,000, except in States with exclusive or monopolistic funds that do not permit worker's compensation to be written by private carriers.
- **General Liability.** The Contractor shall maintain bodily injury general liability insurance written on a comprehensive form of policy of at least \$100,000 per person and \$500,000 per occurrence. Property damage limits, if any, will be set forth elsewhere in the "Schedule."
- **Automobile Liability.** For automobiles used in connection with performance of this contract, the Contractor shall maintain automobile liability insurance written on a comprehensive form of policy with coverage of at least \$200,000 per person and \$500,000 per occurrence for bodily injury and \$20,000 per occurrence for property damage, unless higher limits are required by airport management and state law.
- **Aircraft Liability.** If aircraft will be used in connection with performance of this contract, the Contractor shall maintain aircraft public and passenger liability insurance with coverage of at least \$200,000 per person and \$500,000 per occurrence for bodily injury other than passenger liability, and \$200,000 per occurrence for property damage. Coverage for passenger liability bodily injury shall be at least \$200,000 multiplied by the number of seats or passengers, whichever is greater.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 250
---------------------	--------------	--	---------------

- **Watercraft Liability** When watercraft will be used in connection with performing the contract, the Contractor shall provide watercraft liability insurance. Limits shall be at least \$1,000,000 per occurrence. The policy shall include coverage for owned, non-owned and hired watercraft.
- **Environmental Impairment Liability.** When the contract involves hazardous wastes, the Contractor shall provide environmental impairment liability insurance with coverage of at least \$1,000,000 bodily injury per occurrence and \$1,000,000 property damage per occurrence. Such insurance shall include coverage for the clean up, removal, storage, disposal, transportation, and use of pollutants and hazardous waste.
- **Medical Malpractice.** When the contract will involve health care services, the Contractor shall maintain medical malpractice liability insurance with coverage of at least \$500,000 per occurrence.

H.3.3 Each policy shall substantially include the following provision: "It is a condition of this policy that the issuing company furnishes written notice to the Transportation Security Administration 30 days in advance of the effective date of any reduction in or cancellation of this policy."

H.3.4 The Contractor shall furnish a certificate of insurance or, if required by the Contracting Officer, true copies of liability policies and manually countersigned endorsements of any changes, including the TSA's contract number to ensure proper filing of documents. Insurance shall be effective, and evidence of acceptable insurance furnished, before beginning performance under this contract. Evidence of renewal shall be furnished not later than five days before a policy expires.

H.3.5 The maintenance of insurance coverage as required by this clause is a continuing obligation. The lapse or termination of insurance coverage without replacement coverage being obtained will be grounds for termination for default. *Unless modified in the "Schedule"

H.4 INSURANCE-WORK ON A GOVERNMENT INSTALLATION (TSA 3.4.1.10)

H.4.1 The Contractor shall, at its own expense, provide and maintain during the entire performance of this contract, at least the kinds and minimum amounts of insurance required in the "Schedule" or elsewhere in the contract.

H.4.2 Before commencing work under this contract, the Contractor shall certify to the Contracting Officer in writing by letter or certificate of insurance, reflecting TSA's contract number, that the required insurance has been obtained. The policies evidencing required insurance shall contain an endorsement to the effect that any cancellation or any material change adversely affecting the Transportation Security Administration's interest shall not be effective: (1) for such period as the laws of the State in which this contract is to be performed prescribe, or (2) until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer, whichever period is longer.

H.4.3 The Contractor shall insert the substance of this clause, including this paragraph I, in subcontracts under this contract that require work on a Government installation and shall require Subcontractors to provide and maintain the insurance required in the "Schedule" or elsewhere in the contract. The Contractor shall maintain a copy of all Subcontractors' proofs of required insurance, and shall make copies (reflecting the TSA's contract number to ensure proper filing of documents) available to the Contracting Officer upon request.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 251
---------------------	--------------	--	---------------

H.5 AUTHORIZED USERS

This contract is for the use of the Transportation Security Administration (TSA) as well as to provide select services and connectivity to other DHS organizational elements and external law enforcement entities.

H.6 DISCLOSURE OF INFORMATION

Information furnished under this solicitation may be subject to disclosure under the Freedom of Information Act (FOIA). Therefore, all items that are confidential to business, or contain trade secrets, proprietary, or personnel information must be clearly marked.

Any information made available to the Contractor by the Government must be used only for the purpose of carrying out the provisions of this contract and must not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract.

In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and information and must ensure that all work performed by its Subcontractors shall be under the supervision of the Contractor or the Contractor's employees.

H.7 STANDARD CONDUCT AT GOVERNMENT INSTALLATIONS

The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance and integrity and shall be responsible for taking such disciplinary action with respect to his employees as may be necessary. The Contractor is also responsible for ensuring that the Contractor's employees do not disrupt the work activities or materials of Federal staff in the workplace.

H.8 SUBSTITUTION OF KEY MANAGEMENT PERSONNEL

Individuals proposed as key management personnel and accepted for this contract are expected to remain with this contract. However, in the event that the Contractor deems it necessary to replace any of the individuals designated as key management personnel, the Contractor shall request the substitution in writing to the Contract Officer.

H.8.1 All substitutes must have at least equal qualifications to those of the individual being replaced.

H.8.2 All appointments of key management personnel shall be approved by the Contract Officer, and no substitutions of such personnel shall be made without the advance written approval of the Contract Officer.

H.8.3 Except as provided otherwise in this clause, at least thirty (30) days (sixty (60) days if security clearance is required) in advance of the proposed substitution, all proposed substitutions of key management personnel must be submitted in writing to the Contract Officer, including the information required otherwise in this provision.

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	252

H.8.4 Where individuals proposed as key management personnel become unavailable between the submission of the final proposal revisions and contract award, within five (5) days following contract award, the Contractor shall notify the Contract Officer in writing of such unavailability and who will be performing, if required, as the temporary substitute. Within fifteen (15) days following contract award, the Contractor shall submit in writing to the Contract Officer proposed substitutions for the unavailable individuals.

H.8.5 Request for substitution of key management personnel must provide a detailed explanation of the circumstances necessitating substitution, a resume of the proposed substitute, and any other information requested by the Contract Officer to make a determination as to the appropriateness of the proposed substitute's qualifications. All resumes shall be signed by the proposed substitute and his/her formal direct supervisor or higher authority.

H.8.6 The Contract Officer shall promptly notify the Contractor in writing of his/her approval or disapproval of all requests for substitution of key management personnel. All disapprovals will require resubmission of another substitution by the Contractor within fifteen (15) days.

H.9 SUBSTITUTION OF KEY PERSONNEL FOR DELIVERY AND TASK ORDERS

If the Government determines that certain personnel are key to successful completion of a delivery or task order or special project, they will be designated as "key personnel" in the delivery or task order. Key personnel are defined as:

- Personnel identified in the proposal as key individuals to be assigned for participation in the performance of the service order/special project and who may, at the discretion of the Government, be interviewed to verify resume representations;
- Personnel whose resumes were submitted with the proposal; or
- Individuals who are designated as key personnel by agreement between the Government and the Contractor during negotiations.

The Contractor shall notify the Contract Officer and the Contract Officer's Technical Representative (COTR) prior to making any changes in key personnel. No changes in key personnel will be made unless the Contractor can demonstrate that the qualifications of prospective personnel are equal to or better than the qualifications of the personnel being replaced. All requests for approval of substitutions in key personnel shall be in writing and provide a detailed explanation of the circumstances necessitating the proposed substitution. They must contain a complete resume for the proposed substitute and other information requested by the Contract Officer to approve or disapprove the proposed substitution. The COTR will evaluate such requests and promptly notify in writing the Contractor of the approval or disapproval. All disapprovals will require resubmission of another substitution by the Contractor within fifteen (15) days.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 253
---------------------	--------------	--	---------------

H.10 ORGANIZATIONAL CONFLICT OF INTEREST

The Contractor warrants that, to the best of the Contractor's knowledge and belief, there are no relevant facts or circumstances which could give rise to an Organizational Conflict of Interest (OCI), as defined in AMS procedures, or that the Contractor has disclosed all relevant information.

The Contractor agrees that if an actual or potential OCI is discovered after award, the Contractor shall make a full disclosure in writing to the Contract Officer. This disclosure must include a description of actions, which the Contractor has taken or proposes to take, after consultation with the Contract Officer, to avoid, mitigate, or neutralize the actual or potential conflict.

The Contract Officer may terminate this contract for convenience, in whole or in part, if it deems such termination necessary to avoid an OCI. If the Contractor was aware of a potential OCI prior to award or discovered an actual or potential conflict after award and did not disclose or misrepresent relevant information to the Contracting Office, the Government may terminate the contract for default, debar the Contractor from Government contracting, or pursue such other remedies as may be permitted by law or this contract.

The Contractor must include this clause in all subcontracts and in lower tier subcontracts unless a waiver is requested from, and granted by, the Contracting Officer.

In the event that changes to a requirement are in such a way as to create a potential conflict of interest for the Contractor, the Contractor must:

- Notify the Contracting Officer of a potential conflict.
- Recommend to the Government an alternate approach which would avoid the conflict.
- Present for approval a conflict of interest mitigation plan that will describe in detail the change requirement that creates the potential conflict of interest; outline in detail the actions the Contractor or Government in performance of the task to mitigate the conflict will take.
- Not commence work on a changed requirement related to a potential conflict of interest until specifically notified by the Contracting Officer to proceed.

If the Contracting Officer determines that it is in the best interest of the Government to proceed with work, notwithstanding a conflict of interest, a request for waiver must be submitted in accordance with FAR 9.503 and AMS procedures.

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	254

H.11 CONTRACTOR'S RESPONSIBILITY FOR ASSIGNED SPACE, EQUIPMENT, AND SUPPLIES

If, due to the fault or neglect of the Contractor, his agents, or employees, damages are caused to any Government property, equipment, stock or supplies, during the performance of this contract, the Contractor shall be responsible for such loss or damage and the Government, at its option, may either require the Contractor to replace all property or to reimburse the Government for the full value of the lost or damaged property. The Contractor is responsible for maintaining all assigned space(s) in a clean and orderly fashion during the course of this contract. All telephones are for conducting official Government business only.

H.12 WARRANTY PERIOD

The Contractor warrants that (1) it has, or can obtain, the appropriate knowledge and skills to perform the agreed Services; and (2) it will use commercially reasonable efforts to provide the Services on a timely basis and in the manner described.

The warranty for materials furnished by the Contractor under this contract shall be for a period of ninety (90) days or if equipment is involved, the Original Equipment Manufacturer's warranty (OEM).. In the case of equipment (hardware or software, as appropriate), the Original Equipment Manufacturer's warranty will be provided as specified in the B-Tables, and shall be the only warranty applicable thereto.

H.13 PUBLICITY AND DISSEMINATION OF CONTRACT INFORMATION

Publicity releases in connection with this contract shall not be made by the Contractor unless prior written approval has been received from the Contract Officer.

The Contractor shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contract Officer. Two copies of any material proposed to be published or distributed shall be submitted to the Contracting Officer.

A minimum of five days notice is required for requests made in accordance with this provision.

H.14 PROCEDURES FOR CORRESPONDENCE

All correspondence shall be subject to the following procedures:

- o Technical correspondence shall be addressed to the COTR or his designated representative with information copies to the Contract Officer, as appropriate.
- o All other correspondence, e.g., request for waivers, deviations, or modifications to the requirements, and terms and conditions of this contract, shall be addressed to the Contract Officer with an information copy to the COTR or his designated representative (see Section G).

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 255
---------------------	--------------	--	---------------

H.15 PERSONNEL ACCESS

All Contractor personnel requiring access to the Government's sites will be subject to the security clearance procedures set forth in this contract.

H.16 INTERRELATIONSHIP OF ASSOCIATE CONTRACTORS

The TSA may enter into contractual agreements with other Contractors (i.e., "Associate Contractors") in order to provide information technology requirements separate from the work to be performed under this contract, yet having links and interfaces to this contract. The Contractor may be required to coordinate with other such Contractor(s) through the cognizant CO and/or designated representative in providing suitable, non-conflicting technical and/or management interfaces and in avoidance of duplication of effort. Information on deliverables provided under separate contracts may, at the discretion of the TSA and/or other Government agencies, be provided to such other Contractor(s) for the purpose of such work.

Where the Contractor and an associate Contractor fail to agree upon action to be taken in connection with their respective responsibilities, each Contractor shall promptly bring the matters to the attention of the cognizant CO and furnish the Contractor's recommendations for a solution. The Contractor shall not be relieved of its obligations to make timely deliveries or be entitled to any other adjustment because of failure of the Contractor and its associate to promptly refer matters to the CO or because of failure to implement CO directions.

Where the Contractor and Associate Contractors are required to collaborate to deliver a service; the Government will designate, in writing and prior to the definition of the task, to both Contractors, a "lead Contractor" for the project. In these cases the Associate Contractors shall also be contractually required to coordinate and collaborate with the Contractor. TSA will facilitate the mutual execution of Non-Disclosure Agreements.

Compliance with this Special Contract Requirement is included in the contract price and shall not be a basis for equitable adjustment.

H.17 PERMITS

The Contractor shall be responsible for obtaining any necessary licenses and permits, and for complying with any applicable Federal, state, and municipal laws, codes, and regulations, and any applicable foreign work permits, authorizations, etc., in connection with the performance of the contract.

H.18 PRODUCT SUBSTITUTIONS

Product Substitutions is addressed in C.4.3.11.

H.19 SPECIAL PROJECTS

Upon request by the Government the Contractor shall provide a proposal for any Special Projects by way of the ordering process (see Section G.10). The intent of a Special Project may be to allow the Government to acquire services and meet requirements relating to support of the mission of TSA not

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 256
---------------------	--------------	--	---------------

specifically quantified and priced in the Performance Work Statement, e.g., site relocations, etc. These services are to be provided and priced individually. The Government will have the option of accepting the Contractor's offer or performing the work using another Contractor or Government resources.

Site surveys, site walkthroughs or site preparation, such as the installation and maintenance of structured cabling, air conditioning (HVAC) systems and/or electrical circuits, performed by the Contractor for the purpose of implementing a connectivity solution at a TSA controlled airport or TSA office location, will be separately priced. HVAC systems installed during site preparation are not supported by the Contractor's managed services.

The Contractor shall not proceed with any work under a Special Project unless authorized in writing by the Contract Officer. A request for a technical and price proposal will be sent to the Contractor and shall be submitted at a time and date mutually agreed to by the Government and the Contractor. proposals shall be evaluated for timeliness and completeness as well as from a technical and price reasonableness perspective. A firm-fixed price may be negotiated along with T&M, as appropriate, for the Special Project and a delivery order may be issued by the Contract Officer. The delivery order will indicate a start date and a completion date for the Special Project as well as other terms and conditions of the order.

H.20 ENHANCEMENTS OR SPECIALIZED EQUIPMENT TO ACCOMMODATE USERS WITH DISABILITIES (SECTION 508 OF THE REHABILITATION ACT)

An amendment to Section 508 of the Rehabilitation Act prohibits federal agencies from procuring, developing, maintaining, or using electronic and information technology (EIT) that is inaccessible to people with disabilities, subject to an undue burden defense.

The Contractor is reminded that once finalized, the applicable standards in Section 508 of the Rehabilitation Act, as amended, shall apply to this contract and any items, if any, or services covered by or provided in connection with this requirement. The Government and the Contractor shall negotiate as necessary, to add contract clauses that will allow for the acquisition of such covered products and services at prices that can be determined by the Government to be fair and reasonable. A contract modification may be issued to cover any such actions.

H.21 COMMERCIALLY AVAILABLE ITEMS

Except as specifically stated in this contract all hardware and software components, and products used in the performance of this contract shall be commercially available.

H.22 LABOR CATEGORIES – DELETED, (DELETE TABLE)

The labor categories listed in Section J, Attachment 9 of the contract represent the Government's best estimate of some personnel necessary for the successful performance of the contract. Although the Contractor is expected to map from the contract categories to the Contractor's own categories, for the purpose of matching resources to requirements, the use of additional labor categories not currently contemplated may be necessary over the life of the contract. Certain unique labor categories may be required under specific delivery/task orders.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 257
--------------	--------------	--	---------------

Labor rates for exempt positions shall be based on the locality of where the work is performed. The Contractor shall use the geographic Differential Formula for the DC metropolitan area for services provided in the DC area. For services such as the SPOC performed out of area, the Contractor shall use rates from that locality.

- Labor Area of Operations. Contractor proposed labor rates are for use within the United States, including Alaska and Hawaii. Other OCONUS requirements will be reviewed on a case-by-case basis, as requested.
- Travel Requirements. Due to the sensitive nature of select locations, the Contractor shall include "CONUS" travel and specify the location within this document as "Omaha, Nebraska". For the estimation purposes, the Contractor shall use "Omaha, Nebraska" to estimate travel to and from these security sensitive locations. "Omaha, Nebraska" is approximately the geographic center of the United States and shall be the Contractor's basis for establishing travel estimates to these localities.
- Security Clearance Requirements for Labor Category Rate Structure. The basic labor category rate structure addresses up to Secret clearance requirements. The Contractor shall address other additional security clearance requirements on a case-by-case basis, as requested by the Government.
- Contractor and Subcontractor T&M Government Site Rates. Government site labor category rates are applicable when employees are provided, at the Government's expense, all facilities, equipment and supplies necessary to execute their assigned responsibilities. Government Site Rates shall be utilized when the place and duration of task performance can be reasonably predicted to eliminate employee's need for contractor facility support.
- Subcontractor T&M Contractor Site Rates. The effort requires subcontractors to be resident in a Contractor facility; or alternatively, to be resident on a government site, as appropriate to the work effort. As such, the Contractor may add a facility burden to the subcontractor T&M rates for contractor site locations. As applicable, the Contractor may use a four (4%) percent annual escalation applied to the one year quotations received.

H.23 NON-PERSONAL SERVICES

As stated in the Federal Register, Volume 57, No. 190, page 45096, dated September 30, 1992, Policy Letter on Inherently Government Functions, no personal services shall be performed under this contract. No Contractor employee will be directly supervised by a Government employee. All individual Contractor employee assignments, and daily work direction, shall be given by the applicable employee supervisor. If the Contractor believes any Government action or communication has been given that would create a personal services relationship between the Government and any Contractor employee, the Contractor shall promptly notify the Contracting Officer of this communication or action.

The Contractor shall not perform any inherently Governmental actions as defined by FAR 7.500. No Contractor employee shall hold him or herself out to be a Government employee, agent, or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications with third parties in connection with this contract, Contractor employees shall identify themselves as Contractor employees and specify the name of the company for which they work. In all communications with other Government Contractors in connection with this contract, the Contractor employee shall state that they have no authority to in any way change the contract and that if the other Contractor believes this communication to be a

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 258
---------------------	--------------	--	---------------

direction to change their contract, they should notify the Contracting Officer for that contract and not carry out the direction until a clarification has been issued by the Contracting Officer.

The Contractor shall ensure that all of its employees working on this contract are informed of the substance of this clause. Nothing in this clause shall limit the Government's rights in any way under any other provision of the contract, including those related to the Government's right to inspect and accept the services to be performed under this contract. The substance of this clause shall be included in all subcontracts at any tier.

H.24 CONTRACTOR RESPONSIBILITIES

The Contractor shall provide all management, administrative, clerical, and supervisory functions required for the effective and efficient performance of this contract.

The Government shall not be liable for any injury to the Contractor's personnel or damage to the Contractor's property unless such injury or damage is due to negligence on the part of the Government and is recoverable under the Federal Torts Claims Act, or pursuant to another Federal statutory authority.

A smooth and orderly transition between the Contractor and a predecessor or successor Contractor is necessary to ensure minimum disruption to vital Government business. The Contractor shall cooperate fully in the transition.

The Contractor shall adhere to the same professional and ethical standards of conduct required of Government personnel. The Contractor shall not:

- Discuss with unauthorized persons any information obtained in the performance of work under this contract.
- Conduct business not directly related to this contract on Government premises.
- Use computer systems and/or other Government facilities for company or personal business other than work related; or
- Recruit on Government premises or otherwise act to disrupt official Government business.

H.25 QUALIFICATIONS OF EMPLOYEES

The Contracting Officer may require dismissal from work of those employees which he/she deems incompetent, careless, insubordinate, unsuitable or otherwise objectionable, or whose continued employment he/she deems contrary to the public interest or inconsistent with the best interest of national security. The Contractor shall fill out, and cause each of its employees on the contract work to fill out, for submission to the Government, such forms as may be necessary for security or other reasons. Upon request of the Contracting Officer, the Contractor's employees shall be fingerprinted. Each employee of the Contractor shall be a citizen of the United States of America.

H.26 NON-DISCLOSURE AGREEMENTS

Non-Disclosure Agreements are required to be signed by all Contractor personnel when their role requires them to come into contact with Government procurement sensitive information, other

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 259
---------------------	--------------	--	---------------

sensitive information, or proprietary business information from other Contractors (e.g., cost data, plans, and strategies). The recipient certifies in writing that they will take the necessary steps to prevent the unauthorized disclosure and use of information. The Contractor shall maintain the file of the signed Non-Disclosure Agreements which will be made available to the Government upon request.

H.27 TSA DATA PROTECTED BY THE PRIVACY ACT

Data collected under this contract that pertains to individuals will belong solely to the Government and the Contractor shall have no property rights to this data whatsoever. In addition, information pertaining to individuals gathered under any resulting contract shall only be disclosed in accordance with the terms of the Privacy Act, 5 U.S.C.552a.

H.28 TSA REQUIREMENTS AND DUTIES FOR HANDLING SENSITIVE SECURITY INFORMATION (SSI)

Requirements for Safeguarding and Control of SSI—For purposes of this Contract, all information that the TSA provides or causes to be provided to the Contractor as SSI in connection with its duties under this contract shall be covered by TSA policies and procedures for safeguarding and control of SSI until TSA specifically authorizes the Contractor in writing to treat any such information as public. This requirement shall be applicable to all subcontracting on the contract.

Definition of Confidential Information—In addition to the SSI defined by TSA, SSI on this contract shall also include: (1) any specifications, know-how, strategies or technical data, processes, business documents or information, marketing research and other data, customer or client lists, or sources of information which are owned, used or possessed exclusively by or for the benefit of the TSA and based on SSI; (2) SSI-derived work product(s); (3) all SSI obtained by the Contractor from a third party in connection with performance under this contract,

Duty to Maintain SSI—Except as required by any law, court order, subpoena, or by the TSA, or as required to perform Contractor's duties under this Contract, neither Contractor nor its related entities shall disclose SSI to anyone without a valid need to know, nor shall they use or allow the use of SSI to further any private interest other than those within the scope of this Contract. The Contractor shall immediately notify the TSA Contracting Officer in writing of any subpoena or court order requiring disclosure of SSI.

H.29 PRE-EMPLOYMENT INVESTIGATIVE STANDARDS FOR CONTRACTORS

The Contractor staff supporting TSA, DHS, and stakeholder tasks shall be in compliance with the U.S. DHS Management Directive No. 11055 and the TSA Management Directive No. 2800.71 and all updated versions of these documents.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 260
---------------------	--------------	--	---------------

H.30 DHS MENTOR-PROTÉGÉ PROGRAM (DEC 2003)

Large businesses are encouraged to participate in the DHS Mentor-Protégé program for the purpose of providing developmental assistance to eligible small business protégé entities to enhance their capabilities and increase their participation in DHS contracts.

The program consists of:

- Mentor firms, which are large prime Contractors capable of providing developmental assistance;
- protégé firms, which are small businesses, veteran-owned small businesses, service-disabled veteran-owned small businesses, HUBZone small businesses, small disadvantaged businesses, and women-owned small business concerns; and
- Mentor-Protégé agreements, approved by the DHS OSDDBU.

Mentor participation in the program means providing business developmental assistance to aid protégés in developing the requisite expertise to effectively compete for and successfully perform DHS contracts and subcontracts.

Large business prime Contractors, serving as mentors in the DHS mentor-protégé program, are eligible for a post-award incentive for subcontracting plan credit by recognizing costs incurred by a mentor firm in providing assistance to a protégé firm and using this credit for purposes of determining whether the mentor firm attains a subcontracting plan participation goal applicable to the mentor firm under a DHS contract. The amount of credit given to a mentor firm for these protégé developmental assistance costs shall be calculated on a dollar for dollar basis and reported via the SF-295; for example, the mentor/large business prime Contractor reports a \$10,000 subcontract to the protégé/small business Subcontractor and \$5,000 of developmental assistance to the protégé/small business Subcontractor as \$15,000 (\$10,000 traditional subcontract plus \$5,000 in developmental assistance for a total of \$15,000).

Contractors interested in participating in the program are encouraged to contact the DHS OSDDBU for more information.

H.31 OPTION TO EXTEND THE TERM OF THE CONTRACT (TSA 3.2.4-35) (FEB 2003)

The Government may extend the term of this contract by written notice to the Contractor within the timetable defined below; provided, that the Government shall give the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

Option 1, if exercised, shall be exercised within 12 months from date of contract award.

Option 2, if exercised, shall be exercised within 24 months from date of contract award.

If the Government exercises this option, the extended contract shall be considered to include this option Clause.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 261
--------------	--------------	--	---------------

H.32 OBSERVANCE OF LEGAL HOLIDAYS

The Government observes the following holidays:

New Year's Day
Martin Luther King Birthday
President's Day
Memorial Day
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day

In addition to the days designated as holidays, the Government observes also the following days:

- Any other day designated by Federal Statute,
- Any other day designated by Executive Order, and
- Any other day designated by President's Proclamation.

Observance of such holidays by Government personnel shall not be a reason for the Contractor to request an extension of the period of performance, or entitlement of compensation except as set forth within the contract. In the event the Contractor's personnel work during the holiday, they may be reimbursed by the Contractor, however, no form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost, other than their normal compensation for the time worked. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.

When the Government grants excused absence to its employees, assigned Contractor personnel may also be dismissed. The Contractor agrees to continue to provide sufficient personnel to perform critical tasks already in operation or scheduled, and shall be guided by the instructions issued by the Contracting Officer or the Contracting Officer's Technical Representative.

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	262

H.33 ORDER OF PRECEDENCE

Any inconsistency in this contract with the Government's requirements and the Contractor's proposal shall be resolved by giving precedence in the following order:

- (a) The Performance Work Statement (Section C)
- (b) Other documents, exhibits, and attachments to Section C (Section J)
- (c) The Schedule (Sections B and D through H)
- (c) Contract clauses (Section I)

H.34 COST DISCLOSURE

The Contractor shall provide a narrative description of the justification of their pricing methodology. If the level of effort is not fully exposed, the Contractor shall describe in quantifiable terms the number of FTEs and the level of risk represented by the cost. The Contractor shall include all estimates of work hours and labor categories. The Contractor's proposed description of risk shall include any mention of additional labor hours to cover exceptional work requirements such as unpredictable mission related requirements.

H.35 USE OF PRICING TOOLS

The Government reserves the right to seek certification of costs associated with a pricing model. In addition, the Government may seek a hands-on demonstration of the pricing tool that includes validation based on input samples provided by the Government.

In instances where a tool is utilized to develop a price for shared services, the Government shall receive, at minimum, a specific price discount for these services off our GSA Schedule standard pricing.

H.36 BILLING AND PRICING

The Contractor shall expense charges under this contract following the Contractor's disclosure statement practices.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 263
--------------	--------------	--	---------------

PART II – CONTRACT CLAUSES

SECTION I – CONTRACT CLAUSES

I.1 TSA 3.1.1 CLAUSES INCORPORATED BY REFERENCE

This contract incorporates by reference one or more provisions or clauses listed below with the same force and effect as if they were given in full text. The clauses are located on the internet at: <http://www.tsa.gov/public/display?theme=84&content=0900051980013479>

TSA Clause No.	Title	Date
3.1.8.1	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	FEB 2003
3.1.8.2	Price or Fee Adjustment for Illegal or Improper Activity	FEB 2003
3.2.2.3.25	Price Reduction for Defective Cost or Pricing Data - Modifications	FEB 2003
3.2.2.3.26	Price Reduction for Defective Cost or Pricing Data- Modifications	FEB 2003
3.2.2.3.27	Subcontractor Cost or Pricing Data	JULY 2004
3.2.2.3.28	Subcontractor Cost or Pricing Data-Modifications	FEB 2003
3.2.2.3.30	Termination of Defined Benefit Pension Plans	FEB 2003
3.2.2.3.33	Order of Precedence	FEB 2003
3.2.2.3.36	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other Than Pensions	JULY 2004
3.2.2.3.38	Requirements for Cost or Pricing Data or Information Other Than Cost or Pricing Data	FEB 2003
3.2.2.3.39	Requirements for Cost or Pricing Data or Information Other Than Cost or Pricing Data-Modifications	JULY 2004
3.2.2.7.6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment	FEB 2003
3.2.3.2	Cost Accounting Standards	FEB 2003
3.2.4.34	Option to Extend Services	FEB 2003
3.2.5.4	Contingent Fees	FEB 2003
3.2.5.5	Anti-Kickback Procedures	FEB 2003
3.2.5.6	Restrictions on Subcontractor Sales to the TSA	FEB 2003
3.3.1.1	Payments	FEB 2003
3.3.1.11	Availability of Funds for the Next Fiscal Year	FEB 2003
3.3.1.5	Payments under Time-and-Materials and Labor-Hour Contracts	FEB 2003
3.3.1.6	Discounts for Prompt Payment	FEB 2003
3.3.1.7	Limitation on Withholding of Payments	FEB 2003
3.3.1.8	Extras	FEB 2003
3.3.1.9	Interest	FEB 2003
3.3.1.15	Assignment of Claims	FEB 2003
3.3.1.17	Prompt Payment.	JAN 2003

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	264

3.3.1.25	Mandatory Information for Electronic Funds Transfer (EFT- Payment - Central Contractor Registration (CCR)	FEB 2003
3.4.2.7	Federal, State, and Lo-I Taxes -- Fixed Price (Noncompetitive Contract)	FEB 2003
3.4.2.8	Federal, State, and Local Taxes --Fixed Price Contract	FEB 2003
3.5.1	Authorization and Consent	FEB 2003
3.5.13	Rights in Data-General	FEB 2003
3.5.16	Rights in Data-Special Works	FEB 2003
3.5.18	Commercial Computer Software-Restricted Rights	FEB 2003
3.6.1.3	Use of Small Business Concerns	FEB 2003
3.6.1.4	Small, Small Disadvantaged, Women-Owned and Service-Disabled Veteran Owned Small Business Subcontracting Plan	AUG 2002
3.6.1.6	Liquidated Damages-Subcontracting Plan	FEB 2003
3.6.2.2	Convict Labor	FEB 2003
3.6.2.3	Walsh-Healey Public Contracts Act Representation	FEB 2003
3.6.2.5	Prohibition of Segregated Facilities	FEB 2003
3.6.2.9	Equal Opportunity	FEB 2003
3.6.2.14	Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans	FEB 2003
3.6.2.16	Notice to the Government of Labor Disputes	FEB 2003
3.6.2.28	Service Contract Act of 1965, As Amended	FEB 2003
3.6.2.31	Fair Labor Standards Act and Service Contract Act-Price Adjustment	FEB 2003
3.6.3.16	Drug-Free Workplace	JAN 2004
3.6.4.2	Buy American Act-Supplies	FEB 2003
3.6.4.10	Restrictions on Certain Foreign Purchases	FEB 2003
3.7.1	Privacy Act Notification	FEB 2003
3.7.2	Privacy Act	FEB 2003
3.8.2.10	Protection of Government Buildings, Equipment, and Vegetation	FEB 2003
3.8.2.11	Continuity of Services	FEB 2003
3.8.4.5	Government Supply Sources	FEB 2003
3.9.1.1	Contract Disputes	FEB 2003
3.9.1.2	Protest After Award	FEB 2003
3.10.1.7	Bankruptcy	FEB 2003
3.10.1.12	Changes-Fixed Price (Alternate II)	FEB 2003
3.10.1.14	Changes-Time-and-Materials or Labor-Hours	FEB 2003
3.10.1.25	Notification and Change-Of-Name Agreements	
3.10.2.1	Subcontracts (Fixed Price Contracts)	FEB 2003
3.10.2.5	Competition in Subcontracting	FEB 2003
3.10.4.21	Requirements for Software Measures	FEB 2003
3.10.6.1	Termination for Convenience of the Government (Fixed-Price)	AUG 2002
3.10.6.4	Default (Fixed-Price Supply and Service)	FEB 2003
3.10.6.7	Excusable Delays	FEB 2003
3.13.2	Security Requirements --Classified Contract	FEB 2003

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	265

3.13.3	Printed or Copied Double-Sided on Recycled Paper	FEB 2003
3.14.3	Foreign Nationals as Contractor Employees	AUG 2002

I.2 RESERVED

I.3 NOTIFICATION OF OWNERSHIP CHANGES (TSA 3.2.2.3.37) (FEB 2003)

(a) The Contractor shall make the following notifications in writing.

(1) When the Contractor becomes aware that a change in its ownership has occurred or is certain to occur which could result in changes in the valuation of its capitalized assets in the accounting records, the Contractor shall notify the Contracting Officer within 30 days.

(2) The Contractor shall also notify the Contracting Officer within 30 days whenever changes to asset valuations or any other cost changes have occurred or are certain to occur as a result of a change in ownership.

(b) The Contractor shall:

(1) Maintain current, accurate, and complete inventory records of assets and their costs;

(2) Provide the Contracting Officer or designated representative ready access to the records upon request;

(3) Ensure that all individual and grouped assets, their capitalized values, accumulated depreciation or amortization, and remaining useful lives are identified accurately before and after each of the Contractor's ownership changes; and

(4) Retain and continue to maintain depreciation and amortization schedules based on the asset records maintained before each Contractor ownership change.

(c) The Contractor shall include the substance of this clause in all subcontracts under this contract when it is anticipated that cost or pricing data will be required or for which any pre-award or post-award cost determination will be subject to the contract.

I.4 REQUESTS FOR CONTRACT INFORMATION (TSA 3.2.2.3.75) (FEB 2003)

Any contract resulting from this SIR will be considered a public document, subject to release under the Freedom of Information Act (FOIA), 5 U.S.C. Section 552. Unless covered by an exemption described in the Act, all information contained in the contract, including unit price, hourly rates and their extensions, may be released to the public upon request. Offerors are therefore urged to mark any sensitive documents submitted as a result of this Screening Information Request SIR that may be deemed as trade secrets, proprietary information, or privileged or confidential financial information.

I.5 OFFICIALS NOT TO BENEFIT (TSA 3.2.5.1) (FEB 2003)

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 266
---------------------	--------------	--	---------------

No member of or delegate to Congress, or resident commissioner, shall be admitted to any share or part of this contract, or to any benefit arising from it. However, this clause does not apply to this contract to the extent that this contract is made with a corporation or the corporation's general benefit.

I.6 RESERVED

I.7 WHISTLEBLOWER PROTECTION FOR CONTRACTOR EMPLOYEES (TSA 3.2.5.8) (FEB 2003)

The Contractor agrees not to discharge, demote or otherwise discriminate against an employee as a reprisal for disclosing information to a Member of Congress, or an authorized official of an agency or of the Department of Justice, relating to a violation of law related to this contract (including the competition for or negotiation of a contract)“ Definitions: (1) "Authorized official of the agency" means an employee responsible for contracting, program management, audit, inspection, investigation, or enforcement of any law or regulation relating to TSA procurement or the subject matter of the contract. (2) "Authorized official of the Department of Justice" means any person responsible for the investigation, enforcement, or prosecution of any law or regulation:

I.8 TSA COST PRINCIPLES (TSA 3.3.2.1) (FEB 2003)

(a) Transportation Security Administration (TSA) "Contracting Cost Principles" shall be used for:

- (1) The pricing of contracts, subcontracts, and modifications to contracts and subcontracts whenever cost analysis is performed; and
- (2) The determination, negotiation, or allowance of cost when required by a contract clause.

(b) TSA Cost Principles are incorporated by reference in this contract as the basis for:

- (1) Determining reimbursable costs under: (i) Cost-reimbursement contracts and cost-reimbursement subcontracts under these contracts performed by commercial organizations, and (ii) The cost-reimbursement portion of time-and -materials contracts except when material is priced on a basis other than at cost;
- (2) Negotiating indirect cost rates, when: (i) TSA has division or corporate contract administration responsibilities; (ii) Quick Close-out procedures are used; or (iii) Indirect rate caps are negotiated in the contract.
- (3) Proposing, negotiating, or determining costs under terminated contracts;
- (4) Price revision of fixed-price incentive contracts;
- (5) Price re-determination of contracts; and (6) Pricing changes and other contract modifications.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 267
--------------	--------------	--	---------------

(c) When contract administration responsibilities rest with another Government agency, the TSA will apply the cost principles of the administering agency for the determination or negotiation of indirect rates not covered by (2)(ii) or (2)(iii) above.

(d) Upon request, the Contracting Officer will provide a copy of the TSA "Contract Cost Principles." Until TSA develops its own Contract Cost Principles, TSA will adopt FAA's Contract Cost Principles, available at: <http://fast.faa.gov/procurement-guide/html/3-3-2.htm>.

I.9 ERRORS AND OMISSIONS (TSA 3.4.1.13) (FEB 2003)

(a) The Contractor warrants that it is insured for \$200,000 (unless another amount is set forth in the "Schedule") for errors and omissions per claim in an amount in excess of the minimum set forth in the "Schedule" in the performance of this contract.

(b) Unless the Contractor's policy is prepaid, non-cancelable, and issued for a period at least equal to the term of this contract on an occurrence basis, the Contractor must have the policy amended to include substantially the following provision: "It is a condition of this policy that the company furnish written notice to the U.S. Transportation Security Administration 30 days in advance of the effective date of any reduction in or cancellation of this policy."

(c) The Contractor must furnish a certificate of insurance or, if required by the Contracting Officer, true copies of liability policies and manually countersigned endorsements of any changes, including the TSA's contract number to ensure proper filing of documents. Insurance must be effective, and evidence of acceptable insurance furnished, before beginning performance under this contract. Evidence of renewal must be furnished not later than five days before a policy expires.

I.10 UTILIZATION OF SMALL BUSINESS CONCERNS (TSA 3.6.1.3) (FEB 2003)

(a) It is the policy of the Transportation Security Administration (TSA) that small business concerns, small disadvantaged business concerns, HUBZone small business concerns, veteran-owned small business concerns, service-disabled veteran owned small business concerns, and women-owned small business concerns shall be provided the opportunities to participate in performing TSA contracts, including contracts and subcontracts for subsystems, assemblies, components, and related services for major systems. It is further the policy of the TSA that its prime Contractors establish procedures to ensure the timely payment of amounts due pursuant to the terms of their subcontracts with these small business concerns.

(b) The Contractor hereby agrees to carry out this policy in the awarding of subcontracts to the fullest extent consistent with efficient contract performance. The Contractor further agrees to cooperate in any studies or surveys conducted by the TSA as may be necessary to determine the extent of the Contractor's compliance with this clause.

(c) Definitions. As used in this contract: "HUBZone small business concern" means a small business concern that appears on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration. "Service-disabled veteran-owned small business concern" – (1) Means a small business concern – (i) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veteran; and (ii) The management and

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 268
---------------------	--------------	--	---------------

daily business operations of which are controlled by one or more service-disabled veterans, or in the case of a veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran. (2) Service-disabled veteran means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16). "Small business concern" means a small business as defined pursuant to Section 3 of the Small Business Act, and relevant regulations promulgated pursuant thereto. "Small disadvantaged business concern" means a small business concern that represents, as part of its offer that – (1) It has received certification as a small disadvantaged business concern consistent with 13 CFR part 124, Subpart B; (2) No material change in disadvantaged ownership and control has occurred since its certification; (3) Where the concern is owned by one or more individuals, the net worth of each individual upon whom the certification is based does not exceed \$750,000 after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); and (4) It is identified, on the date of its representation, as a certified small disadvantaged in the database maintained by the Small Business Administration (PRO-Net). "Veteran-owned small business concern" means a small business concern – (1) Not less than 51 percent of which is owned by one or more veterans (as defined in 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and (2) The management and daily business operations of which are controlled by one or more veterans. "Women-owned small business concern" means a small business concern – (1) That is at least 51 percent owned by one or more women, or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and (2) Whose management and daily business operations are controlled by one or more women.

(d) Contractors acting in good faith may rely on written representations by their Subcontractors regarding their status as a small business concern, a small disadvantaged business concern, a veteran-owned small business concern, a service-disabled veteran owned small business concern, a HUBZone small business concern or a women-owned small business concern.

I. 11 RESERVED

I.12 LIQUIDATED DAMAGES – SUBCONTRACTING PLAN (TSA 3.6.1.6) (FEB 2003)

(a) Failure to make a good faith effort to comply with the subcontracting plan, as used in this clause, means the lack of a good faith effort to perform in accordance with the requirements of the subcontracting plan approved under the clause in this contract titled "Small, Small Disadvantaged, Women-Owned, Veteran-Owned, and Service-Disabled Veteran Owned Small Business Subcontracting Plan," are willful or intentional action to frustrate the plan.

(b) If, at contract completion, or in the case of a commercial product plan, at the close of the fiscal year for which the plan is applicable, the Contractor has failed to meet its subcontracting goals and the Contracting Officer decides in accordance with paragraph (c) of this clause that the Contractor failed to make a good faith effort to comply with its subcontracting plan, established in accordance with the clause in this contract titled "Small, Small Disadvantaged, Women-Owned, and Service-Disabled Veteran Owned Small Business Subcontracting Plan," the Contractor shall pay the Government liquidated damages in an amount stated. The amount of damages attributable to the Contractor's failure to comply shall be an amount equal to the actual dollar amount by which the Contractor failed to achieve each subcontract goal or, in the case of a commercial products plan, that portion of the dollar amount allocable to Government contracts by which the Contractor failed to achieve each subcontract goal.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 269
---------------------	--------------	--	---------------

(c) Before the Contracting Officer makes a final decision that the Contractor has failed to make such good faith effort, the Contracting Officer shall give the Contractor written notice specifying the failure and permitting the Contractor to demonstrate what good faith efforts have been made. Failure to respond to the notice may be taken as an admission that no valid explanation exists. If, after consideration of all the pertinent data, the Contracting Officer finds that the Contractor failed to make a good faith effort to comply with the subcontracting plan, the Contracting Officer shall issue a final decision to that effect and require that the Contractor pay the Government liquidated damages as provided in paragraph (b) of this clause.

(d) With respect to commercial product plans; i.e., company-wide or division-wide subcontracting plans approved under paragraph (g) of the clause in this contract titled "Small, Small Disadvantaged, Women-Owned, and Service-Disabled Veteran Owned Small Business Subcontracting Plan," the Contracting Officer of the agency that originally approved the plan will exercise the functions of the Contracting Officer under this clause on behalf of all agencies that awarded contracts covered by that commercial product plan.

(e) The Contractor shall have the right of appeal from any final decision of the Contracting Officer.

(f) Liquidated damages shall be in addition to any other remedies that the Government may have.

I.13 AFFIRMATIVE ACTION FOR SPECIAL DISABLED AND VIETNAM ERA VETERANS – (TSA 3.6.2.12) (FEB 2003)

(a) Definitions.

(1) "Appropriate office of the State employment service system," as used in this clause, means the local office of the Federal-State national system of public employment offices assigned to serve the area where the employment opening is to be filled, including the District of Columbia, Guam, Puerto Rico, Virgin Islands, American Samoa, and the Trust Territory of the Pacific Islands.

(2) "Openings that the Contractor proposes to fill from within its own organization," as used in this clause, means employment openings for which no one outside the Contractor's organization (including any affiliates, subsidiaries, and the parent companies) will be considered and includes any openings that the Contractor proposes to fill from regularly established recall lists.

(3) Openings that the Contractor proposes to fill under a customary and traditional employer-union hiring arrangement, as used in this clause, means employment openings that the Contractor proposes to fill from union halls, under their customary and traditional employer-union hiring relationship.

(4) "Suitable employment openings" as used in this clause includes, but is not limited to, openings that occur in jobs categorized as—

- (i) Production and non-production;
- (ii) Plant and office;
- (iii) Laborers and mechanics;

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	270

(iv) Supervisory and non-supervisory;
(v) Technical; and
(vi) Executive, administrative, and professional positions compensated on a salary basis of less than \$25,000 a year; and (2) Includes full-time employment, temporary employment of over 3 days, and part-time employment, but not openings that the Contractor proposes to fill from within its own organization or under a customary and traditional employer-union hiring arrangement, nor openings in an educational institution that are restricted to students of that institution.

(b) General.

(1) Regarding any position for which the employee or applicant for employment is qualified, the Contractor shall not discriminate against the individual because the individual is a special disabled or Vietnam Era veteran. The Contractor agrees to take affirmative action to employ, advance in employment and otherwise treat qualified special disabled and Vietnam Era veterans without discrimination based upon their disability or veteran's status in all employment practices such as—

- (i) Employment;
- (ii) Upgrading;
- (iii) Demotion or transfer;
- (iv) Recruitment;
- (v) Advertising;
- (vi) Layoff or termination;
- (viii) Rates of pay or other forms of compensation; and
- (viii) Selection for training, including apprenticeship.

(2) The Contractor agrees to comply with the rules, regulations, and relevant orders of the Secretary of Labor (Secretary) issued under the Vietnam Era Veterans' readjustment Assistance Act of 1972 (the Act), as amended.

(c) Listing openings.

(1) The Contractor agrees to list all suitable employment openings existing at contract award or occurring during contract performance, at an appropriate office of the State employment service system in the locality where the opening occurs. These openings include those occurring at any Contractor facility, including one not connected with performing this contract. An independent corporate affiliate is exempt from this requirement.

(2) State and local Government agencies holding Federal contracts of \$10,000 or more shall also list all their suitable openings with the appropriate office of the State employment service.

(3) The listing of suitable employment openings with the State employment service system is required at least concurrently with using any other recruitment source or effort and involves the obligations of placing a bona fide job order, including accepting referrals of veterans and non-veterans. This listing does not require hiring any particular job applicant or hiring from any particular group of job applicants and is not intended to relieve the Contractor from any requirements of Executive orders or regulations concerning nondiscrimination in

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 271
--------------	--------------	--	---------------

employment.

(4) Whenever the Contractor becomes contractually bound to the listing terms of this clause, it shall advise the State employment service system, in each State where it has establishments, of the name and location of each hiring location in the State. As long as the Contractor is contractually bound to these terms and has so advised the State system, it need not advise the State system of subsequent contracts. The Contractor may advise the State system when it is no longer bound by this contract clause.

(5) Under the most compelling circumstances, an employment opening may not be suitable for listing, including situations when:

- (i) The Government's needs cannot reasonably be supplied,
- (ii) Listing would be contrary to national security, or
- (iii) The requirement of listing would not be in the Government's interest.

(d) Applicability.

(1) This clause does not apply to the listing of employment openings which occur and are filled outside the 50 States, the District of Columbia, Puerto Rico, Guam, Virgin Islands, American Samoa, and the Trust Territory of the Pacific Islands.

(2) The terms of paragraph (c) above of this clause do not apply to openings that the Contractor proposes to fill from within its own organization or under a customary and traditional employer-union hiring arrangement. This exclusion does not apply to a particular opening once an employer decides to consider applicants outside of its own organization or employer-union arrangement for that opening.

(e) Postings.

(1) The Contractor agrees to post employment notices stating:

- (i) the Contractor's obligation under the law to take affirmative action to employ and advance in employment qualified special disabled veterans and veterans of the Vietnam era, and
- (ii) the rights of applicants and employees.

(2) These notices shall be posted in conspicuous places that are available to employees and applicants for employment. They shall be in a form prescribed by the Director, Office of Federal Contract Compliance Programs, Department of Labor (Director), and provided by or through the Contracting Officer.

(3) The Contractor shall notify each labor union or representative of workers with which it has a collective bargaining agreement or other contract understanding, that the Contractor is bound by the terms of the Act, and is committed to take affirmative action to employ, and advance in employment, qualified special disabled and Vietnam Era veterans.

(f) Noncompliance. If the Contractor does not comply with the requirements of this clause,

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	272

appropriate actions may be taken under the rules, regulations, and relevant orders of the Secretary issued pursuant to the Act.

(g) Subcontracts. The Contractor shall include the terms of this clause in every subcontract or purchase order of \$10,000 or more unless exempted by rules, regulations, or orders of the Secretary. The Contractor shall act as specified by the Director to enforce the terms, including action for noncompliance.

1.14 AFFIRMATIVE ACTION FOR WORKERS WITH DISABILITIES (TSA 3.6.2-13) (FEB 2003)

(a) General.

(1) Regarding any position for which the employee or applicant for employment is qualified, the Contractor shall not discriminate against any employee or applicant because of physical or mental disability. The Contractor agrees to take affirmative action to employ, advance in employment, and otherwise treat qualified individuals with disabilities without discrimination based upon their physical or mental disability in all employment practices such as--

- (i) Recruitment, advertising, and job application procedures;
- (ii) Hiring, upgrading, promotion, award of tenure, demotion, transfer, layoff, termination, right of return from layoff, and rehiring;
- (iii) Rates of pay or any other form of compensation and changes in compensation;
- (iv) Job assignments, job classifications, organizational structures, position descriptions, lines of progression, and seniority lists;
- (v) Leaves of absence, sick leave, or any other leave;
- (vi) Fringe benefits available by virtue of employment, whether or not administered by the Contractor;
- (vii) Selection and financial support for training, including apprenticeships, professional meetings, conferences, and other related activities, and selection for leaves of absence to pursue training;
- (viii) Activities sponsored by the Contractor, including social or recreational programs; and
- (ix) Any other term, condition, or privilege of employment.

(2) The Contractor agrees to comply with the rules, regulations, and relevant orders of the Secretary of Labor (Secretary) issued under the Rehabilitation Act of 1973 (29 U.S.C. 793) (the Act), as amended.

(b) Postings.

(1) The Contractor agrees to post employment notices stating--

- (i) The Contractor's obligation under the law to take affirmative action to employ and advance in employment qualified individuals with disabilities; and
- (ii) The rights of applicants and employees.

(2) These notices shall be posted in conspicuous places that are available to employees and applicants for employment. The Contractor shall ensure that applicants and employees with disabilities are informed of the contents of the

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 273
--------------	--------------	--	---------------

notice (e.g., the Contractor may have the notice read to a visually disabled individual, or may lower the posted notice so that it might be read by a person in a wheelchair). The notices shall be in a form prescribed by the Deputy Assistant Secretary for Federal Contract Compliance of the U.S. Department of Labor (Deputy Assistant Secretary) and shall be provided by or through the Contracting Officer.

(3) The Contractor shall notify each labor union or representative of workers with which it has a collective bargaining agreement or other contract understanding, that the Contractor is bound by the terms of Section 503 of the Act and is committed to take affirmative action to employ, and advance in employment, qualified individuals with physical or mental disabilities.

(c) Noncompliance. If the Contractor does not comply with the requirements of this clause, appropriate actions may be taken under the rules, regulations, and relevant orders of the Secretary issued pursuant to the Act.

(d) Subcontracts. The Contractor shall include the terms of this clause in every subcontract or purchase order in excess of \$10,000 unless exempted by rules, regulations, or orders of the Secretary. The Contractor shall act as specified by the Deputy Assistant Secretary to enforce the terms, including action for noncompliance.

I.15 NOTICE OF DELAY (TSA 3.10.1.24) (FEB 2003)

If the Contractor becomes unable to complete the contract work at the time(s) specified because of technical difficulties, notwithstanding the exercise of good faith and diligent efforts in the performance of the work called for hereunder, the Contractor shall give the Contracting Officer written notice of the anticipated delay and the reasons therefore. Such notice and reasons shall be delivered promptly after the condition creating the anticipated delay becomes known to the Contractor, but in no event less than forty-five (45) days before the completion date specified in this contract, unless otherwise directed by the Contracting Officer. When the notice is required, the Contracting Officer may extend the time specified in the Schedule for the period determined in the best interest of the Government.

I.16 SUBCONTRACTS FOR COMMERCIAL ITEMS (TSA 3.10.2.6) (FEB 2003)

I. Definition.

(a) "Commercial item" as used in this clause, means: (1) Any item, other than real property, that is of a type customarily used for non-governmental purposes and that— (i) Has been sold, leased, or licensed to the general public; or (ii) Has been offered for sale, lease, or license to the general public; (2) Any item that evolved from an item described in paragraph I(a)(1) of this clause through advances in technology or performance and that is not yet available in the commercial marketplace, but will be available in the commercial marketplace in time to satisfy the delivery requirements under a pending Government contract; (3) Any item that would satisfy a criterion expressed in paragraphs I(a)(1) or I(a)(2) of this clause, but for— (i) Modifications of a type customarily available in the commercial marketplace; or (ii) Minor modifications of a type not customarily available in the commercial marketplace made to meet Federal Government requirements. Minor modifications means modifications that do not significantly alter the non-governmental function or essential physical

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 274
--------------	--------------	--	---------------

characteristics of an item or component, or change the purpose of a process. Factors to be considered in determining whether a modification is minor include the value and size of the modification and the comparative value and size of the final product. Dollar values and percentages may be used as guideposts, but are not conclusive evidence that a modification is minor. (4) Any combination of items meeting the requirements of paragraphs I(a)(1), (2), (3), or (5) of this clause that are of a type customarily combined and sold in combination to the general public; (5) Installation services, maintenance, services, repair services, training services, and other services if such services are procured for support of an item referred to in paragraphs I(a)(1), (2), (3), or (4) of this clause, and if the source of such services—) Offers such services to the general public and the Federal Government contemporaneously and under similar terms and conditions; and (ii) Offers to use the same work force for providing the Federal Government with such services as the source uses for providing such services to the general public; (6) Services of a type offered and sold competitively in substantial quantities in the commercial marketplace based on established catalog or market prices for specific tasks performed, under standard commercial terms and conditions. This does not include services that are sold based on hourly rates without an established catalog or market price for a specific service performed; (7) Any item, combination of items, or service referred to in subparagraphs I(a)(1) through (a)(6), notwithstanding the fact that the item, combination of items, or service is transferred between or among separate divisions, subsidiaries, or affiliates of a Contractor; or (8) A non-developmental item, if the procuring agency determines the item was developed exclusively at private expense and sold in substantial quantities, on a competitive basis, to multiple State and local Governments.

(b) "Subcontract" as used in this clause, includes a transfer of commercial items between divisions, subsidiaries, or affiliates of the Contractor or Subcontractor at any tier. II. To the maximum extent practicable, the Contractor shall incorporate, and require its Subcontractors at all tiers to incorporate, commercial items or non-developmental items as components of items to be supplied under this contract. III. Notwithstanding any other clause of this contract, the Contractor is not required to include any TSA Acquisition Management System provision or clause, other than those listed below to the extent they are applicable and as may be required to establish the reasonableness of prices, in a subcontract at any tier for commercial items or commercial components: (a) Equal Opportunity (E.O. 11246); (2) Affirmative Action for Special Disabled and Vietnam Era Veterans (38 U.S.C. 4212(a)); (b) Affirmative Action for Handicapped Workers (29 U.S.C. 793); and (c) Preference for Privately Owned U.S.-Flagged Commercial Vessels (46 U.S.C. 1241) (flow down not required for subcontracts awarded beginning May 1, 1996). IV. The Contractor shall include the terms of this clause, including this paragraph IV, in subcontracts awarded under this contract.

I.17 DEFINITIONS - --GOVERNMENT PROPERTY (TSA 3.10.3.1) (FEB 2003)

(a) Accessory item - --an item that facilitates or enhances the operation of plant equipment but which is not essential for its operation.

(b) Agency-peculiar property - --Government-owned personal property that is peculiar to the mission of an agency (e.g., military or space property). It excludes Government material, special test equipment, special tooling, and facilities.

(c) Auxiliary item - --an item without which the basic unit of plant equipment cannot operate.

(d) Common item -- material that is common to the applicable Government contract and the Contractor's other work.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 275
---------------------	--------------	--	---------------

(e) Contractor-acquired property (CAP) - property acquired or otherwise provided by the Contractor for performing a contract and to which the Government has title.

(f) Contractor inventory - --(1) Any property acquired by and in the possession of a Contractor or Subcontractor under a contract for which title is vested in the Government and which exceeds the amounts needed to complete full performance under the entire contract; (2) Any property that the Government is obligated or has the option to take over under any type of contract as a result either of any changes in the specifications or plans hereunder or of the termination of the contract (or subcontract hereunder), before completion of the work, for the convenience or at the option of the Government; and (3) Government-furnished property that exceeds the amounts needed to complete full performance under the entire contract.

(g) Custodial records – written memoranda of any kind, such as requisitions, issue hand receipts, tool checks, and stock record books, used to control items issued from tool cribs, tool rooms, and stockrooms.

(h) Discrepancies incident to shipment - deficiencies incident to shipment of Government property to or from a Contractor's facility whereby differences exist between the property purported to have been shipped and property actually received. Such deficiencies include loss, damage, destruction, improper status and condition coding, errors in identity or classification, and improper consignment.

(i) Facilities - --hen used in other than a facilities contract, means property used for production, maintenance, research, development, or testing. It includes plant equipment and real property. It does not include material, special test equipment, special tooling, or agency-peculiar property.

(j) Facilities contract - -- contract under which Government facilities are provided to a Contractor or Subcontractor by the Government for use in connection with performing one or more related contracts for supplies or services. A "related contract" is used in this clause, means a Government contract or subcontract for supplies or services under which the use of the facilities is or may be authorized. It is used occasionally to provide special tooling or special test equipment. Facilities contracts may take any of the following forms: (1) Facilities acquisition contract providing for the acquisition, construction, and installation of facilities. (2) Facilities use contract providing for the use, maintenance, accountability, and disposition of facilities. (3) A consolidated facilities contract, which is a combination of facilities acquisition and a facilities use contract.

(k) Government-furnished property (GFP) - property in the possession of, or directly acquired by, the Government and subsequently made available to the Contractor.

(l) Government production and research property - Government-owned facilities, Government owned special test equipment, and special Blank Sidetooling to which the Government has title or the right to acquire title.

(m) Government property - property owned by or leased to the Government or acquired by the Government under the terms of the contract. It includes both Government-furnished property and Contractor-acquired property as defined in this section.

(n) Individual item record - separate card, form, document or specific line(s) of computer data used to account for one item of property.

(o) Line item - single line entry on a reporting form that indicates a quantity of property having the same description and condition code from any one contract at any one reporting location.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 276
--------------	--------------	--	---------------

(p) Material - property that may be incorporated into or attached to a deliverable end item or that may be consumed or expended in performing a contract. It includes assemblies, components, parts, raw and processed materials, and small tools and supplies that may be consumed in normal use in performing a contract.

(q) Nonprofit organization - corporation, foundation, trust, or institution operated for scientific, educational, or medical purposes, not organized for profit, and no part of the net earnings of which inures to the benefit of any private shareholder or individual.

(r) Non-severable - when related to Government production and research property, means property that cannot be removed after erection or installation without substantial loss of value or damage to the property or to the premises where installed.

(s) Personal property - property of any kind or interest in it, except real property, records of the Federal Government, and naval vessels of the following categories: battleships, cruisers, aircraft carriers, destroyers, and submarines.

(t) Plant clearance - actions relating to the screening, redistribution, and disposal of Contractor inventory from a Contractor's plant or work site. The term 'Contractor's plant' includes a Contractor-operated Government facility.

(u) Plant clearance officer - authorized representative of the Contracting Officer assigned responsibility for plant clearance.

(v) Plant clearance period - the period beginning on the effective date of contract completion or termination and ending 90 days (or such longer period as may be agreed to) after receipt by the Contracting Officer of acceptable inventory schedules for each property classification. The final phase of the plant clearance period means that period after receipt of acceptable inventory schedules.

(w) Plant equipment - personal property of a capital nature (including equipment, machine tools, test equipment, furniture, vehicles, and accessory and auxiliary items) for use in manufacturing supplies, in performing services, or for any administrative or general plant purpose. It does not include special tooling or special test equipment.

(x) Precious metals - common and highly valuable metals characterized by their superior resistance to corrosion and oxidation. Included are silver, gold, and the platinum group metals-platinum, palladium, iridium, osmium, rhodium, and ruthenium.

(y) Property - property, both real and personal. It includes facilities, material, special tooling, special test equipment, and agency-peculiar property.

(z) Property Administrator (PA) - an authorized representative of Contracting Officer assigned to administer the contract requirements and obligations relating to Government property.

(aa) Public body - any State, Territory, or possession of the United States, any political subdivision thereof, the District of Columbia, the Commonwealth of Puerto Rico, any agency or instrumentality of any of the foregoing, any Indian tribe, or any agency of the Federal Government.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 277
--------------	--------------	--	---------------

(bb) Real property - and rights in land, ground improvements, utility distribution systems, and buildings and other structures. It does not include foundations and other work necessary for installing special tooling, special test equipment, or plant equipment.

(cc) Reportable property - --Contractor inventory that must be reported for screening in accordance with this subpart before disposition as surplus, to a separate contract or to a special contract requirement governing their use or disposition.

(dd) Reporting activity - --he Government activity that initiates the Standard Form 120, Report of Excess Personal Property (or when acceptable to GSA, by data processing output).

(ee) Salvage - property that because of its worn, damaged, deteriorated, or incomplete condition or specialized nature, has no reasonable prospect of sale or use as serviceable property without major repairs, but has some value in excess of its scrap value.

(ff) Scrap - personal property that has no value except for its basic material content.

(gg) Screening completion date - --he date on which all screening required by this subpart is to be completed. It includes screening within the Government and the donation screening period.

(hh) Serviceable or usable property - property that has a reasonable prospect of use or sale either in its existing form or after minor repairs or alterations.

(ii) Special test equipment - either single or multipurpose integrated test units engineered, designed, fabricated, or modified to accomplish special purpose testing in performing a contract. It consists of items or assemblies of equipment including standard or general purpose items or components that are interconnected and interdependent so as to become a new functional entity for special testing purposes. It does not include material, special tooling, facilities (except foundations and similar improvements necessary for installing special test equipment), and plant equipment items used for general plant testing purposes.

(jj) Special tooling - --rigs, dies, fixtures, molds, patterns, taps, gauges, other equipment and manufacturing aids, all components of these items, and replacement of these items, which are of such a specialized nature that without substantial modification or alteration their use is limited to the development or production of particular supplies or parts thereof or to the performance of particular services. It does not include material, special test equipment, facilities (except foundations and similar improvements necessary for installing special tooling), general or special machine tools, or similar capital items.

(kk) Stock record - perpetual inventory record which shows by nomenclature the quantities of each item received and issued and the balance on hand.

(ll) Summary Record - -- separate card, form, document or specific line(s) of computer data used to account for multiple quantities of a line item of special tooling, special test equipment, or plant equipment costing less than \$5,000 per unit.

(mm) Surplus property - --Contractor inventory not required by any Federal agency.

(nn) Surplus release date (SRD) - --he date on which screening of personal property for Federal use is completed and the property is not needed for any Federal use. On that date, property becomes surplus and is eligible for donation

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 278
--------------	--------------	--	---------------

(oo) Termination inventory - any property purchased, supplied, manufactured, furnished, or otherwise acquired for the performance of a contract subsequently terminated and properly allocable to the terminated portion of the contract. It includes Government-furnished property. It does not include any facilities, material, special test equipment, or special tooling that are subject to a separate contract or to a special contract requirement governing their use or disposition.

(pp) Utility distribution system - includes distribution and transmission lines, substations, or installed equipment forming an integral part of the system by which gas, water, steam, electricity, sewerage, or other utility services are transmitted between the outside building or structure in which the services are used and the point of origin, disposal, or connection with some other system. It does not include communication services.

(qq) Work-in-process - material that has been released to manufacturing, engineering, design or other services under the contract and includes undelivered manufactured parts, assemblies, and products, either complete or incomplete.

1.18 SEGREGATION OF GOVERNMENT PROPERTY (TSA 3.10.3.13) (FEB 2003)

The Contractor shall physically separate Government property from Contractor-owned property. However, when advantageous to the TSA and consistent with the Contractor's authority to use such property, the property may be commingled:

- (a) When the Government property is special tooling, special test equipment, or plant equipment clearly identified and recorded as Government property;
- (b) When approved by the TSA Property Administrator in connection with research and development contracts;
- (c) When material is included in a multi-contract cost and material control system;
- (d) When scrap of a uniform nature is produced from both Government-owned and Contractor-owned material and physical segregation is impracticable;
- (e) When scrap produced from TSA-owned material is insignificant in consideration of the cost of segregation and control;
- (f) When TSA contracts involved are fixed-price and provide for the retention of the scrap by the Contractor; or
- (g) When otherwise approved by the TSA Property Administrator.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 279
--------------	--------------	--	---------------

I.19 INVENTORIES (TSA 3.10.3.14) (FEB 2003)

(a) Monthly Inventories

(1) The Contractor shall provide to the TSA's Property Administrator a quarterly (or other time frame as agreed to by the Contractor and the Contracting Officer) listing of all Government property in their possession (this includes GFP and CAP).

(2) The Contractor may electronically reproduce standard inventory schedule forms provided no change is made to the name, content or sequence of the data elements. All essential elements of data must be included and the form must be signed.

(3) The Contractor shall use inventory schedule to report all transaction of Government property in Contractor's possession or control and shall cause Subcontractors to do likewise.

(b) Physical Inventories. The Contractor shall annually physically inventory all Government property (except materials issued from stock for manufacturing, research, design, or other services required by the contract) in its possession or control and shall cause Subcontractors to do likewise. These may include electronic reading, recording and reporting or other means of reporting the existence and location of the property and reconciling the records. Type and frequency of inventory shall be based on the Contractor's established practices, the type and use of the Government property involved, or the amount of Government property involved and its monetary value, and the reliability of the Contractor's property control system. Type of physical inventories normally shall not vary between contracts being performed by the Contractor, but may vary with the type of property being controlled. Personnel who perform the physical inventory should not be the same personnel who prepare the monthly inventories.

(c) Inventories upon termination or completion.

(1) General. Immediately upon termination or completion of a contract, the Contractor shall perform and cause each Subcontractor to perform a physical inventory, adequate for disposal purposes, of all Government property applicable to the contract, unless the requirement is waived as provided in paragraph (2) below.

(2) Exception. The requirement for physical inventory at the completion of a contract may be waived by the Property Administrator when the property is authorized for use on a follow-on contract; provided, that:

(i) Experience has established the adequacy of property controls and an acceptable degree of inventory discrepancies; and

(ii) The Contractor provides a statement indicating that record balances have been transferred in lieu of preparing a formal inventory list and that the Contractor accepts responsibility and accountability for those balances under the terms of the follow-on contract.

(3) Listings for disposal purposes. (Note: This paragraph (3) applies only to nonprofit organizations.)

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 280
--------------	--------------	--	---------------

(i) Standard items that have been modified may be described on listings for disposal purposes as standard items with a general description of the modification.

(ii) Items that have been fabricated, such as test equipment, shall be described in sufficient detail to permit a potential user to determine whether they are of sufficient interest to warrant further inspection.

(d) Reporting results of inventories. The Contractor shall, as a minimum, submit the following to the TSA Property Administrator promptly after completing the physical inventory:

(1) A listing that identifies all discrepancies disclosed by a physical inventory.

(2) A signed statement that physical inventory of all or certain classes of Government property was completed on a given date and that the official property records were found to be in agreement except for discrepancies reported.

(e) Quantitative and monetary control. When requested by the Property Administrator, the Contractor's reports of results of physical inventory shall be prepared on a quantitative and monetary basis and segregated by categories of property. (End of clause)

I.20 DISPOSITION OF GOVERNMENT PROPERTY (TSA 3.10.3.15) (FEB 2003)

(a) Submission of inventory schedules.

(1) When property is no longer needed to perform the contract, the Contractor shall prepare inventory schedules in accordance with the contract and instructions from the plant clearance officer or TSA Property Administrator and shall promptly submit the schedules to the TSA Property Administrator. Inventory schedules may also be used for screening with other Federal agencies.

(2) The certificate on the inventory schedule must be executed when Contractor inventory is reported. The prime Contractor shall execute this certificate, except that for Subcontractor termination inventory the Subcontractor shall execute the certificate.

(3) The Contractor's inventory schedules shall not include any items that the Contractor can reasonably use on other Government work without financial loss. However, the schedules shall include common items specified by the Contracting Officer for delivery to the Government or which are Government-furnished property.

(4) The contract may authorize the Contractor to electronically reproduce inventory schedules provided no change is made in the name, content or sequence of the data elements. All essential elements of data must be included and the form must be signed.

(b) Acceptance. Within 15 days after receipt of inventory schedules, the plant clearance officer or Property Administrator should review them, determine their acceptability, and request the Contractor to correct any inadequate listings. Inventory schedules should not be rejected if the information is adequate for disposal purposes, even if complete cost data on work-in-process are not available. Rejection should be limited, when possible, to specific items and should not necessarily render the entire schedule unacceptable. If substantial errors are discovered that were not apparent on termination inventory schedules previously found acceptable, the final phase of a plant clearance

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	281

period should not begin until corrected schedules have been submitted, unless the plant clearance officer or Property Administrator determines otherwise.

(c) Excess inventories.

(1) Contractors shall report Contractor inventory promptly after determining it to be excess, unless a later date is authorized by the Contracting Officer or Property Administrator.

(2) Unless contract provisions or agency regulations prescribe otherwise, 12 copies of inventory schedules listing serviceable or salvable items and 6 copies of inventory schedules listing scrap items shall be presented to the Property Administrator.

(3) The Contractor shall not submit partial schedules unless authorized by the TSA Property Administrator. The first page of each schedule submitted shall be identified as partial or final in the title block of the schedule.

I.21 SEAT BELT USE BY CONTRACTOR EMPLOYEES (TSA 3.13.5) (FEB 2003)

In accordance with Executive Order 13043 entitled "Increasing Seat Belt Use in the U.S.," the Contractor is encouraged to implement, communicate and enforce on the job seat belt policies and programs for their employees and Subcontractors when operating company-owned, rented or personally-owned vehicles in the performance of this contract.

I.22 CONTRACTOR PERSONNEL SUITABILITY REQUIREMENTS, as per U.S. DHS Management Directive No. 11055 and TSA Management Directive No. 2800.71 and all updates

(a) This clause applies to the extent that this contract requires Contractor employees, Subcontractors, or consultants to have unescorted access to TSA: (1) facilities, (2) sensitive information, and/or (3) resources regardless of the location where such access occurs.

(b) TSA Servicing Security Element (SSE) has approved designated risk levels for the following positions under the contract: Position Risk Level: High Risk, Moderate Risk, or Low Risk.

(c) Not later than 30 calendar days after contract award (or date of modification, if this provision is included by modification to an existing contract), for each employee in a listed position, provided no previous background investigations can be supported as described below, the Contractor shall submit the following documentation to the SSE for an employment suitability determination: Standard Form (SF) 85P, Questionnaire for Public Trust Positions, revised September 1995. The SF 85P shall be completed in accordance with the instruction sheet and fingerprint card (FD-258). Fingerprinting facilities are available through the SSE and local police department. All fingerprint cards shall be written in black ink or typewritten with all answerable question blocks completed and shall be signed and dated within the 60 calendar day period preceding the submission. The type of investigation conducted will be determined by the position risk level designation for all duties, functions, and/or tasks performed and shall serve as the basis for granting a favorable employment suitability authorization. If an employee has had a previous Government-directed background investigation, it may be accepted by the TSA. However, the TSA reserves the right to conduct further investigations, if necessary. For each Contractor employee for which a previous background investigation was

Solicitation	Document No.	Document Title	Page #
		ITMS Bridge Contract	282

completed, the Contractor shall provide, in writing to the SSE, the name, date of birth, place of birth, and social security number of the employee, the name of the investigating entity, type of background investigation conducted, and approximate date the previous background investigation was completed in addition to the documents required above. The Contractor shall submit the required information with a transmittal letter referencing the contract number and this request to: TSA Office of Investigations: [CO insert current information here or enter "N/A" if not applicable] The transmittal letter shall also include a list of all of the names of Contractor employees and their positions for which completed forms will be submitted to the SSE pursuant to this Clause. A copy of the transmittal letter shall also be provided to the Contracting Officer.

(d) The Contractor shall submit the information required by Section (c) of this Clause for any new employee not listed in the Contractor's 'initial thirty (30) day submission who is hired into any position identified in Section (c) of this Clause.

(e) The contracting officer will provide notice to the Contractor when any Contractor employee is found to be unsuitable or otherwise objectionable, or whose conduct appears contrary to the public interest, or inconsistent with the best interest of national security. The Contractor shall take appropriate action, including the removal of such employee from working on this TSA contract, at their own expense.

(f) No Contractor employee shall work in a high, moderate, or low risk position unless the SSE has received all forms necessary to conduct any required investigation and has authorized the Contractor employee to begin work. However, if this provision is added by modification to an existing contract, Contractor employees performing in the positions listed above may continue work on the contract pending: (1) the submittal of all necessary forms within 30 calendar days, and (2) completion of a suitability investigation by the SSE, subject to the following conditions: (State any SSE conditions such as restricted access to sensitive information or facilities. Specify information or facilities. If the SSE imposes no conditions, state "N/A") If the necessary forms are not submitted by the Contractor to the SSE within 30 days of the effective date of the modification, the Contractor employee shall be denied access to TSA facilities, sensitive information and/or resources until such time as the forms are submitted and the SSE has authorized the Contractor employee to begin work.

(g) As applicable, the Contractor shall submit quarterly reports providing the following information to the Contracting Officer with a copy to the SSE and the Operating Office on or before the fifth (5th) day following each report period: A complete listing by full name in alphabetical order with the social security number, of all Contractor personnel who had access to an TSA facility, sensitive information and/or resources anytime during the report period (date of birth and social security number shall be omitted from CO and Operating Office copies of report(s). Additionally, the Contractor shall submit to the SSE and CO on or before the fifth (5th) day of each month, any employment changes made during the reporting period. Examples of such changes are terminations (to include name, SSN, hire date), and name changes. All lists must be in alphabetical order and have the name of the Contractor and the contract number.

(h) The Contractor shall notify the CO within one (1) day after any employee identified pursuant to Section (c) of this Clause is terminated from performance on the contract.

(i) The Contracting Officer may also, after coordination with the SSE and other security specialists, require Contractor employees to submit any other security information (including additional fingerprinting) deemed reasonably necessary to protect the interests of the TSA. In this event, the Contractor shall provide, or cause each of its employees to provide such security information to the SSE, and the same transmittal letter requirements of Section (c) of this Clause shall apply.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 283
--------------	--------------	--	---------------

(j) The Contactor and/or Subcontractor(s) will immediately contact the Contracting Officer in the event an employee is arrested (detained by law enforcement for any offenses, other than minor traffic offenses) or is involved in theft of Government property or the Contractor becomes aware of any information that may raise a question about the suitability of a Contractor employee.

(k) Failure to submit information required by this clause within the time required may be determined by the Contracting Officer to be a material breach of the contract.

(l) If subsequent to the effective date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in direct contract costs or otherwise affect any other terms or condition of this contract, the contract shall be subject to an equitable adjustment.

(m) The Contractor agrees to insert terms that conform substantially to the language of this clause, including paragraph (l) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to TSA facilities, sensitive information, and/or TSA IT Systems.

1.23 SENSITIVE UNCLASSIFIED INFORMATION (SUI) (TSA 3.14.5) (FEB 2003)

(a) Sensitive information shall be restricted to specific Contractors who:

- (1) have a need to know to perform contract tasks;
- (2) meet personnel suitability security requirements to access sensitive information; and
- (3) successfully complete a non-disclosure agreement (NDA).

(b) The Contractor shall develop and implement procedures to ensure that sensitive information is handled in accordance with FAA requirements and at a minimum, will address:

- (1) steps to minimize risk of access by unauthorized persons during business and non-business hours to include storage capability;
- (2) procedures for safeguarding during electronic transmission (voice, data, fax) mailing or hand carrying;
- (3) procedures for protecting against co-mingling of information with general Contractor data system/files;
- (4) procedures for marking documents with both the protective marking and the distribution limitation statement as needed;
- (5) procedures for the reproduction of subject material;
- (6) procedures for reporting unauthorized access; and
- (7) procedures for the destruction and/or sanitization of such material.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 284
--------------	--------------	--	---------------

I.24 PUBLIC COMMUNICATION (TSA 3.14.7) (JAN 2005)

TSA and the Contractor shall work together to assure that accurate and complete information is provided to the public regarding this contract. When communicating to the public (through press releases, etc.), the Contractor shall submit to the contracting officer a copy of the communication at least three days prior to its issuance. Upon receipt, TSA will provide to the Contractor comments and suggestions to improve the communication. In the event that the Contractor has been provided or has access to sensitive and secure information (SSI), then the Contractor shall wait for the contracting officer's approval prior to issuing the public communication, so that TSA can assure that SSI will not be released to the public. TSA may require the removal of any SSI from the Contractor's public communication. The Contractor also agrees not to use TSA or any TSA official in endorsements of its goods or services. TSA does not provide endorsements.

Solicitation	Document No.	Document Title ITMS Bridge Contract	Page # 285
--------------	--------------	--	---------------

PART II – PART III – LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

SECTION J – LIST OF ATTACHMENTS

The following attachments are available as shown in the table below:

Attachment Number	Title
Attachment 1	Program Documentation: Configuration Management Plan
Attachment 2	Standard Form (SF) 1034
Attachment 3	Quality Assurance Surveillance Plan (QASP) template
Attachment 4	Program Documentation: Risk Management Plan
Attachment 5	Performance Management and Incentive Plan (PMIP) with Service Level Agreements (SLAs) <i>(applicable only to the Transportation Security Administration) shall begin upon Contractor acceptance of Service Orders/Tasks</i>
Attachment 6	Offeror Table of Prices Template (CLINs)
Attachment 7	Performance Requirements Summary Template
Attachment 8	Intentionally Left Blank, See Attachment 6
Attachment 9	Labor Categories
Attachment 10	Systems Development Life Cycle Guidance Document (SDLC)
Attachment 11	Standard Form (SF) 294 and 295
Attachment 12	Reserved
Attachment 13	Reserved
Attachment 14	Enterprise Architecture Technical Reference Model
Attachment 15	TSA ITMS Application List
Attachment 16	TSA Enterprise Architecture model
Attachment 17	Other Reference Documents
Attachment 18	ODC and Travel Requirements <i>(SSS, SSP Completion Criteria, and OCIO Policy Directive 2005-1, which were provided with the initial RFP release)</i>
Attachment 19	Time and Material Labor Rates
Attachment 20	TTO/TTR Table B 7.2
Attachment 21	TTO/TTR Table B 8.1
Attachment 22	Deliverables/Work Products (Section F Table)

LABOR CATEGORIES/QUALIFICATIONS

ITOP II Program Manager - Serves as the Contractor counterpart to the Government program/technical manager for ITOP II. Manages substantial program/technical support operations involving multiple ITOP II projects/task orders and personnel at diverse locations. Organizes, directs, and coordinates planning and execution of all program/technical support activities. Shall have demonstrated information technology expertise and communications skills to be able interface with all levels of management. Simultaneously plans and manages the transition of several highly technical projects. Establishes and alters (as necessary) management structure to effectively direct program/technical support activities. Meets and confers with Government management officials regarding the status of specific Contractor program/technical activities and problems, issues or conflicts regarding resolution.

TO Project Manager - Provides competent leadership and responsible program direction through successful performance of a variety of detailed, diverse elements of project transitioning. Directs completion of tasks within estimated timeframes and budget constraints. Schedules and assigns duties to subordinates and subcontractors and ensures assignments are completed as directed. Enforces work standards and reviews/resolves work discrepancies to ensure compliance with contract requirements. Interfaces with the Contractor's ITOP II Program Manager as well as Government management personnel including, but not limited to, the Contracting Officer and the Contracting Officer's Technical Representative. Reports in writing and orally to contractor management and Government representatives.

Computer Systems Analyst - Analyzes, develops, and/or reviews computer software possessing a wide range of capabilities, including numerous engineering, business, and records management functions. Develops and/or oversees plans for automated data processing systems from project inception to conclusion: Analyzes information to be processed. Defines and analyzes problems and develops system requirements and program specifications, from which programmers prepare detailed flow charts, programs, and tests. Coordinates closely with programmers to ensure proper implementation of program and system specifications. Develops, in conjunction with functional users, system alternative solutions. Provides support for the installation, testing, implementation, and ongoing maintenance of the hardware/software to support EC/EDI functions and provides expertise in the area of EC/EDI translation software and systems.

Applications Programmer - Analyzes functional business applications and design specifications for functional areas such as payroll, logistics, and contracts. Develops block diagrams and logic flow charts. Translates detailed design into computer software. Tests, debugs, and refines the computer software to produce the required product. Prepares required documentation, including both program-level and user-level documentation. Enhances software to reduce operating time or improve efficiency. Provides technical direction to programmers as required to ensure program deadlines are met.

System Programmer - Creates and/or maintains operating systems, communications software, data base packages, compilers, assemblers, and utility programs. Modify existing software as well as create special-purpose software to ensure efficiency and integrity between systems and applications.

Functional [Subject Matter] Expert - Analyzes user needs to determine functional requirements. Performs functional allocation to identify required tasks and their interrelationships. Identifies resources required for each task. Possesses requisite knowledge and expertise so recognized in the professional community that the Government is able to qualify the individual as an expert in the field for an actual TO. Demonstrates exceptional oral and written communication skills.

Quality Assurance Specialist - Develops and implements quality control methodologies to ensure compliance with quality assurance standards, guidelines, and procedures in a large computer-based organization. Develops and defines major and minor characteristics of quality including quality metrics and scoring parameters and determines requisite quality control resources for an actual TO. Establishes and maintains a process for evaluating hardware, software, and associated documentation and/or assists in the evaluation. Conducts and/or participates in formal and informal reviews at pre-determined points throughout the development life cycle.

Data Base Analyst - Manages and/or develops data base projects. Provides highly technical expertise in the use of Data Base Management Systems (DBMS) concepts. Evaluates and recommends available DBMS products and services to support validated user requirements. Defines file organization, indexing methods, and security procedures for specific user applications.

System Administrator/Operator - Supervises and manages the daily activities of configuration and operation of business/computer systems. Optimizes system operations and resource utilization and performs system capacity analysis and planning. Provides assistance to users in accessing and using business/computer systems. Monitors and supports computer processing. Coordinates input, output, and file media. Distributes output and controls computer operation.

Systems Engineer - Applies software, hardware, and standards information technology skills in the analysis, specification, development, integration, and acquisition of systems for information management applications. Ensures these systems and applications are compliant with standards for open systems architectures, reference models, and profiles of standards -- such as the IEEE Open Systems Environment reference model -- as they apply to the implementation and specification of information management solutions on the application platform, across the application program interface, and the external environment/software application. Evaluates and recommends COTS applications and methodologies that can be acquired to provide interoperable, portable, and scalable information technology solutions. Performs analysis and validation of reusable software/hardware components to ensure the integration of these components into interoperable information management designs.

Information Systems Engineer - Analyzes information requirements. Evaluates analytically and systematically problems of workflow, organization, and planning and develops appropriate corrective action. Applies business process improvement practices to re-engineer methodologies/principles and business process modernization projects. Applies, as appropriate, activity and data modeling, transaction flow analysis, internal control and risk analysis and modern business methods and performance measurement techniques. Assist in establishing standards for information systems procedures. Develops and applies organization-wide information models for use in designing and building integrated, shared software and database management systems.

Constructs sound, logical business improvement opportunities consistent with the configuration information management guiding principles, cost savings, and open architecture objectives.

Software Engineer - Analyzes and studies complex system requirements. Designs software tools and subsystems to support software reuse and domain analyses and manages their implementation. Manages software development and support using formal specifications, data flow diagrams, other accepted design techniques, and Computer Aided Software Engineering (CASE) tools. Interprets software requirements and design specifications to code, and integrates and tests software components. Estimates software development costs and schedule. Reviews existing programs and assists in making refinements, reducing operating time, and improving current techniques. Supervises software configuration management.

Software Systems Specialist - Performs moderately complex analysis, design, development, testing, and implementation of computer software in support of a range of functional and technical environments. Develops solutions to problems involving telecommunications, network design analysis, database design, etc.

ADP Hardware Specialist - Reviews computer systems in terms of machine capabilities and man-machine interface. Prepares reports and studies concerning hardware. Prepares functional requirements and specifications.

Communications Hardware Specialist - Analyzes network and computer communications hardware characteristics and recommends equipment procurement, removals, and modifications. Adds, deletes, and modifies, as required, host, terminal, and network devices. Assists and coordinates with communications network specialists in the area of communication software. Analyzes and implements communications standards and protocols according to site requirements.

Communications Software Specialist - Analyzes network and computer communications software characteristics and recommends software procurement, removals, and modifications. Adds, deletes, and modifies, as required, host, terminal, and network devices in light of discerned software needs/problems. Assists and coordinates with communications network specialists in the area of communications software.

Communications Network Specialist - Analyzes network characteristics (e.g., traffic, connect time, transmission speeds, packet sizes, and throughput) and recommends procurement, removals, and modifications to network components. Designs and optimizes network topologies and site configurations. Plans installations, transitions, and cutovers of network components and capabilities. Ensures maintenance of systems. Coordinates requirements with users and suppliers. Provides support on all phases of analysis, design, testing, and implementation of networks and the telecommunications infrastructure to support EC/EDI functions.

Operations Manager - Manages computer operations, including at Government facilities. Schedules machine time and directs data entry efforts. Provides users with computer output. Oversees all operations to ensure downtime is minimized, necessary supplies are restocked in a timely manner, customer requests/complaints are readily resolved, etc.

Technical Writer - Gathers, analyzes, and composes technical information required for preparation of user manuals, training materials, installation guides, proposals, reports, etc. Edits functional descriptions, system specifications, user manuals, special reports, or any other customer deliverables and documents. Conducts research and ensures the use of proper technical terminology. Translates technical information into clear, readable documents to be used by technical and non-technical personnel.

Computer/Telecommunications Security Systems Specialist - Analyzes and defines security requirements for a variety of computer and telecommunications issues. Designs, develops, engineers, and implements solutions to requirements. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs. Performs risk analyses which also include risk assessment. Develops, analyzes, and implements security architecture(s) as appropriate.

IRM Analyst - Ensures problem resolution and customer satisfaction for individual TOs. Performs technical and administrative efforts for tasks, including review of work products for correctness, compliance with industry accepted standards, federal government legislative and regulatory requirements, and user standards specified in TOs. Develops requirements of IT product/service (including specifications, feasibility studies, requirements analysis, etc.) from inception to conclusion on simple to complex projects.

Training Specialist - Conducts the research necessary to develop and revise training courses and prepares appropriate training catalogs. Prepares all instructor materials (course outline, background material, and training aids). Prepares all student materials (course manuals, workbooks, handouts, completion certificates, and course critique forms). Trains personnel by conducting formal classroom courses, workshops, and seminars.

Procurement Product Specialist - Provides analysis, design, development, testing, and implementation of computer software in support of a range of functional and technical requirements to provide support for procurement software development tasks. Provides expertise in procurement processing to develop automated systems.

Imaging Specialist - Provides highly technical and specialized solutions to complex imaging problems. Performs analyses, studies, and reports related to imaging.