

<b>AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT</b>		<b>1. CONTRACT ID CODE</b>	<b>PAGE OF PAGES</b>
			1   2

<b>2. AMENDMENT/MODIFICATION NO.</b> P00005	<b>3. EFF. DATE</b> 03/01/2009	<b>4. REQUISITION/PURCHASE REQ. NO.</b> 0020036725	<b>5. PROJECT NO. (If applicable)</b>
--	-----------------------------------	---	---------------------------------------

<b>6. ISSUED BY</b> Department of Homeland Security Customs & Border Protection 1300 Pennsylvania Ave. NW NP 1310 Washington	<b>CODE</b> 7014  DC 20229	<b>7. ADMINISTERED BY (If other than Item 6)</b> Dept of Homeland Security Customs and Border Protection Office of Procurement - NP 1310 1300 Pennsylvania Ave. NW Washington	<b>CODE</b>  DC 20229
---	-------------------------------------	--	-----------------------------

<b>8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and Zip Code)</b> VIATBCH SYSTEMS  7901 JONES BRANCH DR  MCLEAN VA 22102-3306  CODE 116207788 FACILITY CODE	<b>9A. AMENDMENT OF SOLICITATION NO.</b>
	<b>9B. DATED (SEE ITEM 11)</b>
	<b>10A. MODIFICATION OF CONTRACT/ORDER NO.</b> X HSBP1008C01762 /
	<b>10B. DATED (SEE ITEM 13)</b> 10/26/2007

**11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS**

The above numbered solicitation is amended as set forth in item 14. The hour and date specified for receipt of Offers  is extended,  is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing items 8 and 15, and returning \_\_\_\_\_ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

**12. ACCOUNTING AND APPROPRIATION DATA (If required)**

SEE ATTACHED

**13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.**

<input type="checkbox"/>	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
<input type="checkbox"/>	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (Such as changes in paying office, appropriation data, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103 (b).
<input type="checkbox"/>	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
X	D. OTHER (Specify type of modification and authority) FAR 43.103-(a)
E. IMPORTANT: Contractor <input type="checkbox"/> is not <input checked="" type="checkbox"/> is required to sign this document and return _____ copies to issuing office.	

**14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)**

This modification is issued to accomplish the following:

- Option Year Two (2). The period of performance is extended from 1 March 2009 through 28 February 2010 with an extended OY1 SOW Level of Effort from 1 March 2009 through 30 April 2009 and a OY2 Descoped SOW Level of Effort from 1 May 2009 through 28 February 2010.
- Option Year Two is funded in the amount of \$6,139,462.60. The total contract value is increased from \$12,230,468.76

Except as provided herein, all terms and conditions of the document referenced in item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

(b) (6)	<b>SIGNER (Type or print)</b> PRESIDENT	<b>16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)</b> Andre S. Aslen Contracting Officer
(b) (6)	<b>DATE SIGNED</b> 4/09	(b) (6) <b>CC. DATE SIGNED</b> 5/21/2009

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT - Continuation			1. CONTRACT ID CODE	
2. AMENDMENT/MODIFICATION NO. P00005	3. EFF. DATE 03/01/2009	4. REQUISITION/PURCHASE REQ. NO. 0020036725	PAGE OF 2	PAGES 2

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)  
to \$18,369,931.36

3. The Descoped Statement of Work (SOW) is attached to  
the Modification Schedule of Supplies and Services.

All other terms and conditions remain unchanged.

ATTACHMENT INFORMATION  
FOR  
AWARD/ORDER/IA HSBP1008C01762, MODIFICATION P00005

---

**SCHEDULE OF SUPPLIES/SERVICES**

---

<b>Item Number:</b>	<b>00130</b>	<b>Line Item (Priced/Information/Option):</b>	<b>P</b>
<b>Supplies/Services:</b>	Onsite Tech Svcs - USV		
<b>Qty</b>	<b>Unit</b>	<b>Unit Price</b>	<b>Ext. Price</b>
1	AU	(b) (4)	(b) (4)
<b>Item Number:</b>	<b>00140</b>	<b>Line Item (Priced/Information/Option):</b>	<b>P</b>
<b>Supplies/Services:</b>	Critical Maintenance -USV		
<b>Qty</b>	<b>Unit</b>	<b>Unit Price</b>	<b>Ext. Price</b>
1	AU	(b) (4)	(b) (4)
<b>Item Number:</b>	<b>00150</b>	<b>Line Item (Priced/Information/Option):</b>	<b>P</b>
<b>Supplies/Services:</b>	Standard Maint. - USV		
<b>Qty</b>	<b>Unit</b>	<b>Unit Price</b>	<b>Ext. Price</b>
1	AU	(b) (4)	(b) (4)
<b>Item Number:</b>	<b>00160</b>	<b>Line Item (Priced/Information/Option):</b>	<b>P</b>
<b>Supplies/Services:</b>	Standard Maint. -Base		
<b>Qty</b>	<b>Unit</b>	<b>Unit Price</b>	<b>Ext. Price</b>
1	AU	(b) (4)	(b) (4)
<b>Item Number:</b>	<b>00170</b>	<b>Line Item (Priced/Information/Option):</b>	<b>P</b>
<b>Supplies/Services:</b>	OEM Service - USV		
<b>Qty</b>	<b>Unit</b>	<b>Unit Price</b>	<b>Ext. Price</b>
1	AU	(b) (4)	(b) (4)
<b>Item Number:</b>	<b>00180</b>	<b>Line Item (Priced/Information/Option):</b>	<b>P</b>
<b>Supplies/Services:</b>	Spares/Replacements - Base		
<b>Qty</b>	<b>Unit</b>	<b>Unit Price</b>	<b>Ext. Price</b>
1	AU	(b) (4)	(b) (4)
<b>Item Number:</b>	<b>00190</b>	<b>Line Item (Priced/Information/Option):</b>	<b>P</b>
<b>Supplies/Services:</b>	Travel -Base		
<b>Qty</b>	<b>Unit</b>	<b>Unit Price</b>	<b>Ext. Price</b>
1	AU	(b) (4)	(b) (4)
<b>Item Number:</b>	<b>00200</b>	<b>Line Item (Priced/Information/Option):</b>	<b>P</b>
<b>Supplies/Services:</b>	WHTI- TAG Warranty		
<b>Qty</b>	<b>Unit</b>	<b>Unit Price</b>	<b>Ext. Price</b>
1	AU	(b) (4)	(b) (4)
<b>Item Number:</b>	<b>00210</b>	<b>Line Item (Priced/Information/Option):</b>	<b>P</b>
<b>Supplies/Services:</b>	WHTI		
<b>Qty</b>	<b>Unit</b>	<b>Unit Price</b>	<b>Ext. Price</b>
1	AU	(b) (4)	(b) (4)
<b>Item Number:</b>	<b>00220</b>	<b>Line Item (Priced/Information/Option):</b>	<b>P</b>
<b>Supplies/Services:</b>	OEM Svc -Base		
<b>Qty</b>	<b>Unit</b>	<b>Unit Price</b>	<b>Ext. Price</b>
1	AU	(b) (4)	(b) (4)

Item Number: 00230 Line Item (Priced/Information/Option): P  
Supplies/Services: GNA Fees - Base  
Qty Unit Unit Price Ext. Price  
1 AU (b) (4) (b) (4)

Item Number: 00240 Line Item (Priced/Information/Option): P  
Supplies/Services: CSI/Nexus-USV  
Qty Unit Unit Price Ext. Price  
1 AU (b) (4) (b) (4)

Item Number: 00250 Line Item (Priced/Information/Option): P  
Supplies/Services: CSI/Nexus - CSI  
Qty Unit Unit Price Ext. Price  
1 AU (b) (4) (b) (4)

Total Funded Contract Value: \$6,139,462.60

---

---

**ACCOUNTING AND APPROPRIATION INFORMATION**

---

Item: 001306100.2525USCSGLCS0923020500Z00009400AP01 IS4502525 Amount (b) (4)

Item: 001406100.2525USCSGLCS0923020500Z00009400AP01 IS4502525 Amount (b) (4)

Item: 001506100.2525USCSGLCS0923020500Z00009400AP01 IS4502525 Amount (b) (4)

Item: 001606100.2525USCSGLCS0923020500Z00009164HQ01 IR1902525 Amount (b) (4)

Item: 001706100.2525USCSGLCS0923020500Z00009400AP01 IS4502525 Amount (b) (4)

Item: 001806100.2525USCSGLCS0923020500Z00009164HQ01 IR1902525 Amount (b) (4)

Item: 001906100.2525USCSGLCS0923020500Z00009164HQ01 IR1902525 Amount (b) (4)

Item: 002006100.2525USCSGLCS0923020500Z00009400AP01 640802525 Amount (b) (4)

Item: 002106100.2525USCSGLCS0923020500Z00009400AP01 640802525 Amount (b) (4)

Item: 002206100.2525USCSGLCS0923020500Z00009164HQ01 IR1902525 Amount (b) (4)

Item: 002306100.2525USCSGLCS0923020500Z00009164HQ01 IR1902525 Amount (b) (4)

Item: 002406100.2525USCSGLCS0923020500Z00009400AP01 IS4502525 Amount (b) (4)

Item: 002506100.2525USCSGLCS0923020500Z00009400AP03 171502525 Amount (b) (4)



**STATEMENT OF WORK  
FOR THE  
BUREAU OF CUSTOMS & BORDER PROTECTION  
COMPUTER HARDWARE MAINTENANCE SERVICES  
SOLICITATION HSBP1006-R-0491**

**PR # 20036725**

**March 2009**

## TABLE OF CONTENTS

<u>C.1</u>	<u>Mission and Background</u>	3
<u>C.2</u>	<u>Scope of Work</u>	6
<u>C.3</u>	<u>Service Provider Tasks to be Performed</u>	8
<u>C.4</u>	<u>Operating Processes and Procedures</u>	17
<u>C.5</u>	<u>Deliverables and Reporting Requirements</u>	18
<u>C.6</u>	<u>Personnel Requirements</u>	23
<u>C.7</u>	<u>Performance Measures</u>	26
<u>C.8</u>	<u>Security</u>	26
<u>C.9</u>	<u>Service Provider's Quality Assurance Program</u>	30
<u>C.10</u>	<u>Government Furnished Equipment and Information</u>	31
<u>C.11</u>	<u>Service Provider Personnel</u>	31
<u>C.12</u>	<u>Period of Performance</u>	33
<u>C.13</u>	<u>Homeland Security Enterprise Architecture Requirements</u>	33
<u>C.14</u>	<u>Compliance with Section 508 of the Rehabilitation Act</u>	34
<u>C.15</u>	<u>Information Security</u>	36
<u>C.16</u>	<u>Infrastructure Transformation Program (ITP) Compliance</u>	41
<u>C.17</u>	<u>Interconnection Security Agreement</u>	41
<u>C.18</u>	<u>Contracting Officers Technical Representative (COTR)</u>	42
<u>C.19</u>	<u>EA Clause</u>	43
<u>Appendix A:</u>	<u>ACRONYMS</u>	44
<u>Appendix B:</u>	<u>COMPUTER HARDWARE GROUP CALL STATISTICS</u>	45
<u>Appendix C:</u>	<u>EQUIPMENT REPAIR, REPLACEMENT &amp; WARRANTY STATISTICS</u>	47
<u>Appendix D:</u>	<u>CBP COPMPUTER HARDWARE MAINTENANCE GROUP EQUIPMENT</u>	49
<u>Appendix E:</u>	<u>CBP COMPUTER HARDWARE GROUP SPARES LIST</u>	53
<u>Appendix F:</u>	<u>CBP EQUIPMENT THAT REQUIRES OEM CERTIFIED MAINTENANCE</u>	58
<u>Appendix G:</u>	<u>LABOR CATEGORY DESCRIPTIONS</u>	59
<u>Appendix H:</u>	<u>COMPUTER HARDWARE GROUP SAMPLE REPORTS</u>	61

**STATEMENT OF WORK  
INFORMATION TECHNOLOGY (IT)  
COMPUTR HARDWARE MAINTENANCE SERVICES**

**C.1 Mission and Background**

***C.1.1 The Bureau of Customs and Border Protection Mission within the Department of Homeland Security***

The Bureau of Customs and Border Protection's (CBP) mission within the Department of Homeland Security (DHS) is to lead the unified national effort to secure America; prevent and deter terrorist attacks; protect against and respond to threats and hazards to our Nation; ensure safe and secure borders, welcome lawful immigrants and visitors; and promote free flow of commerce.

In support of this mission, on an average day, CBP agents will:

- Process over 1.1 million passengers arriving into our nation's airports and seaports;
- Inspect over 57,000 trucks and containers, 580 vessels, 2,459 aircraft, and 323,622 vehicles coming into this country;
- Execute over 64 arrests;
- Seize 4,639 pounds of narcotics in 118 narcotics seizures;
- Seize an average of \$715,652 in currency in 11 seizures;
- Seize an average of \$23,083 in arms and ammunition and \$467,118 in merchandise;
- Deploy 1,200 dog teams to aid inspections;
- Make 5,479 pre-departure seizures of prohibited agricultural items;
- Apprehend 2,617 people crossing illegally into the United States;
- Rescue 3 people illegally crossing the border in dangerous conditions;
- Deploy 350,000 vehicles, 108 aircraft, 118 horses on equestrian patrol, and 480 all-terrain vehicles;
- Utilize 238 remote video surveillance systems, each system using 4-6 cameras to transmit images to a central location; and
- Maintain the integrity of 5,525 miles of border with Canada and 1,989 miles of border with Mexico.

A list of acronyms utilized in this Statement of Work is contained at **Appendix A**.

### **C.1.2 Background**

CBP's Office of Information and Technology (OIT), Enterprise Network and Technology Support division, that CBP employees are provided reliable, on-time, and easy access to OIT products and services. The CBP customer support model is comprised of a single point-of-contact 24x7 help desk. This 24X7 supports operational efforts in addition to deployment and maintenance of various IT related products, such as servers, PCs, radios, wireless, non-intrusive technology and several projects.

Office of Information and Technology: OIT is the information technology component of CBP. OIT is responsible for supporting business processes with the design; development, programming, testing, implementation, training and maintenance of CBP automated systems. OIT is responsible for management of all CBP computer facilities and systems including hardware, software, data, and voice telecommunications and related financial resources. OIT is responsible for the maintenance of CBP hardware and the identification and tracking of hardware maintenance incidents through a centralized group, the Information Technology Center. It is responsible for identifying and evaluating new technologies for application in support of CBP business processes. CBP is responsible for the development and implementation of the CBP Modernization Program, a long-term program to modernize the existing CBP systems and infrastructure. OIT provides centralized research, development, test, evaluation, acquisition, training and maintenance services in support of CBP process owners and core strategies. It ensures the coordination of applied technology programs with other domestic and international law enforcement.

Enterprise Network and Technology Support (ENTS) Division: The ENTS component within OIT is responsible for the implementation and support of the CBP information, including engineering and operation of all platforms, management of the CBP network and communications (data, video, and voice) functions, data base administration for all platforms and desktop support for all users of CBP automated systems. ENTS is responsible for acceptance testing of all applications, systems software, and releases into the production environment; ensuring the security of the infrastructure, establishing security policy, and providing security management services across the enterprise.

ENTS – Technology Training and Technology Support's Technology Support Center (TSC – Computer Hardware Group: ENTS is composed of various components in which support is provided. The Computer Hardware Group is one part of the Technology Support Center (TSC), which is the initial single point of contact for reporting system problems, for CBP information technology worldwide.

The objectives of the ENTS Computer Hardware Group are:

- To minimize CBP systems downtime.
- Treat our users with courtesy and professionalism.
- Resolve basic problems, not symptoms, through careful problem resolution processes and analysis of the issues.

- Be proactive, by seeking to prevent problems through user communication, training, resolution, and follow-up.
- Escalate problems and respond to our users within a designated timeframe with a status, resolution and/or outcome.
- Support the Model Port project.
- Track equipment as required.

Asset Management as utilized in this Statement of Work is defined as the management of a comprehensive list of end user computer equipment. This asset management function includes Level 1 – 3 help desk support, maintenance of various end user computer equipment, and entry and updating of asset management information into COTS asset management products. A list of end user computer assets to be maintained is included in Appendix D.

### ***C.1.3 Current Computer Hardware Group Workload Information***

**The following information is provided in order to provide background information on the historical call volume and repair maintenance volume performed by the Computer Hardware Group.**

In the past six months the Computer Hardware Group has taken approximately 24,000 total calls and has dispatched approximately 4,500 of those calls. Approximately 18,000 were related to the Computer Hardware Group. Out of those 18,000 40% of the were Level 1 calls (initial call handling, 45% of the 18,000 calls were Level 2 calls (normal diagnosis and resolution) and 15% of the 18,000 calls were Level 3 calls which were critical, urgent or a more complex IT related call. The Computer Hardware Group is currently staffed on a 24-hour per day, five days per week (Monday through Friday) basis. These 18,000 calls during this six-month time period can be further grouped into the following:

- 60% of the calls to the Computer Hardware Group were received during the day shift (7:00 a.m. – 3:00 p.m. Eastern Standard Time (EST)), 35% of the calls were received during the evening shift (3:00 p.m. – 11:00 p.m. EST) and 5% of the calls were received during night shift (11:00 p.m. – 7:00 a.m. EST). Current Computer Hardware Group staffing is six (6) contractor personnel during day shift, two (2) contractor personnel during evening shift, two (2) contractor personnel during night shift, and two (2) contractor personnel during noon shift (the noon shift overlaps the day and evening shifts and runs from 12:00 noon to 8:00 p.m. EST)
- Approximately 6,000 calls were for received for Level 1 support not related to Computer Hardware Group requirements. These calls were entered into the Problem Tracking System (PTS) by asset management personnel and then referred to other components of the Technology Support Center for resolution.

- Approximately 18,000 calls were received by the Computer Hardware Group and are listed in **Appendix B** which contains detailed information on the number of service calls generated by the Computer Hardware Group for a recent six-month period. The 18,000 service calls can be further separated into the following:
  - 99% of the calls were from CBP locations in the area consisting of the 50 United States, Washington D.C. Aruba, Bermuda, the U.S. Virgin Islands, the Bahamas, Guam and Puerto Rico. Less than 1% of the service calls were from other CBP locations.
  - 1% of the service calls were critical maintenance requirements; 63% were standard maintenance requirements and 36% were user assistance calls;
  - The service calls resulted in over 6,000 equipment maintenance, Original Equipment Manufacturer (OEM) warranty maintenance or equipment replacement actions. **Appendix C** contains information on the number of out of warranty replacements, repair activities and warranty (OEM warranty) repairs during the six-month same time period.
  - 4,000 requests fulfilled by CHG by shipping equipment. The equipment shipped was either spare units or parts to either replace equipment that could not be economically repaired or repair parts that were purchased and either on-hand or purchased from third party to support equipment repair. 4,050 were for standard maintenance requirements (C.3.7.1) and 400 were for critical maintenance requirements (C.3.7.1).
  - A list of current CBP Computer Hardware Group equipment is located in **Appendix D** and may be modified by the COTR.
  - A list of existing equipment in the CBP Computer Hardware Group inventory utilized for replacement spares or repair parts is contained in **Appendix E** and may be modified by the COTR.
  - A list of CBP Computer Hardware Group equipment that must be maintained by an OEM certified maintainer is contained in **Appendix F**.

## C.2 Scope of Work

The Service Provider shall report to the CBP, Office of Information Technology, Enterprise Network and Technology Support, Enterprise Information Technology Program branch, Computer Hardware Group. The Service Provider shall provide services to staff the Computer Hardware Group.

The Service Provider shall:

- Provide project management for the Computer Hardware Group in support of its mission;
- Furnish experienced professionals that are qualified to support CBP equipment that can provide the best possible IT solutions for CBP customers and users reducing dispatches and shipping requirements.
- Provide solutions to assets and are shipped and manage, track equipment through the entire process.

- Provide assistance to help desk that will include providing help desk support for CBP equipment maintenance requirements, but shall also include answering CBP level 1 support calls not related to equipment maintenance and then referring these calls to the appropriate CBP CHG help desk component for further diagnosing and trouble-shooting;
- Provide worldwide IT equipment hardware maintenance and user / customer assistance for CBP.
- Provide oversight and management of dispatches ensure only critical and equipment still under OEM warranty are dispatched; those not under warranty and not critical will require the COTR or COTR government representatives.
- Identify, acquire, ship and manage an inventory of critical replacement or repair parts required to maintain CBP worldwide IT equipment/systems; and track monies allocated to replacement equipment for the year.
- Provide updated reports in accordance with ITIL services within DHS incident or service tracking tool.
- Provide Customer Relations support in this SOW.

CBP equipment is geographically dispersed throughout the United States and worldwide. The physical environments of these locations requiring maintenance support include office settings, warehouses, air and seaports, and land border inspection stations both in Territorial United States (the Territorial United States consists of the fifty states, Washington D.C. and U.S. Territories (Guam, U.S. Virgin Islands, Puerto Rico, American Samoa, Midway Islands, American Samoa and the Federated States of Micronesia)) as well as CBP non-US Territorial locations. CBP Non-US Territorial locations currently include, but are not limited to; Belgium, Bahamas, Bermuda, Brazil, Canada, China, England, France, Germany, Greece, Hong Kong, Italy, Korea, Malaysia, Japan, Netherlands, Singapore, South Africa, Sweden, Spain, Taiwan, Thailand, and the United Arab Emirates. (UAE).

Some locations present extreme weather and usage elements to the maintenance effort.

Section C.1.3 provides information on current Computer Hardware Group workload statistics. For the purpose of sizing the level of support required under this contract, the Government estimates the following:

- Computer Hardware Group workload (help desk call volume and number of maintenance requests) is estimated to increase by 5% per year over the life of this contract; and
- Weekend helpdesk call volume and number of maintenance requests is anticipated to be equivalent to the call volume currently experienced on the third shift (11:00 p.m. to 07:00 a.m. on weekdays), or 5% of total calls. Unforeseen events such as future OIT reorganizations may change this percentage.

### **C.3 Service Provider Tasks to be Performed**

The Service Provider shall have experience in the facilitation of large-scale, worldwide support efforts and the ability to effectively coordinate partnerships with other vender and/or subcontractors as necessary. The Service Provider shall provide the following types of maintenance services: Critical (C.3.1.1), Standard (C.3.1.2), and On-site Technical Support Services.

#### **C.3.1 IT Equipment Services**

For all equipment maintenance services provided under this contract, the Service Provider shall:

- A. The Service Provider shall provide maintenance (labor, parts, and transportation) manuals and schematics, and shall keep the equipment in operating condition, consistent with OEM requirements and recommendations. Maintenance service shall not include electrical work external to the equipment, and adding or removing accessories, attachments, or other devices. Much of CBP's IT equipment is purchased with a manufacturer's warranty. The Service Provider shall coordinate warranty repairs/replacements with the OEM or warranty service provider. As new equipment/systems comes into the CBP infrastructure the Service Provider shall research warranty information (through the vender) and update CBP automated Problem Tracking System (C.3.3.2). The Service Provider is not responsible for entering new equipment/system that enters into the CBP inventory into the CBP asset management module. Information on new equipment/systems shall be entered into the asset management module by the appropriate CBP Local Property Officer that receives the equipment.
- B. The Service Provider shall repair IT equipment damage resulting from usage, both normal and abnormal. Damage may be caused by: accidents, transportation between Government sites, neglect, misuse, failure of electrical power, air conditioning or humidity control, or causes other than ordinary use.
- C. In analyzing the cost benefit, the Service Provider shall conform to the following This applies to non-critical replacements not under warranty and critical equipment over \$2,500 dollars. COTR or COTR representatives' approval is still required before: (1) Replacement equipment purchase in more then 40% or more of its original value; (2) Replacement parts for inventory are purchased; (3) Equipment purchases are over its end of life cycle; (3) All PM work will be approved by COTR or COTR representative before dispatch is made or work begins. (4) When the Service Provider is authorized to replace defective equipment it must be equal in functionality. Notifications to the COTR and approvals from the COTR for purchases made must be reported in the weekly and Monthly Contract Status Report. The COTR is equipped with a Blackberry email device to enable the Service Provider to notify the COTR on a 24 X 7 X 365 basis when seeking approval.

The Service Provider shall thoroughly document all work performed in the associated call or problem ticket in the automated CBP Tracking System (C.3.3.2).

For on-site field visits, the Service Provider shall always coordinate the visit with a government representative at the site prior to arrival and contact the Computer Hardware Group technician located at the Technology Support Center to update the associated problem ticket before leaving the site. The Service Provider technician on the Technology Support Center shall provide the name and number of the government representative at the site. The Government representative at the site is documented in the CBP Tracking system. The Service Provider shall not close any problem ticket without obtaining confirmation from the customer that the service has been performed or the problem has been resolved, each call to the site shall be documented in the CBP Tracking System. An exception is made if 3 attempts to contact the customer (shall be documented in the DHS Tracking System) over a 4-day period do not produce a response from the customer, then the technician may closed the ticket.

- D. The Service Provider shall provide personnel experienced and qualified to perform the required services.
- E. The Service Provider shall be responsible for determining and implementing appropriate solutions to hardware, software and/or firmware problems. Expected actions to determine and resolve typical IT equipment problems are:
  - a. Telephone-based advice and guidance;
  - b. Information gathering;
  - c. Analysis;
  - d. Research, including attempted reproduction of malfunctions;
  - e. Provide Operational user assistance;
  - f. Providing a resolution or steps towards a resolution;
  - g. Provide Workaround;
  - h. Identification of errors;
  - i. Advice on features and capabilities;
  - j. Dispatching on-site service providers;
  - k. Shipping equipment and determining shipment tracking status; and
  - l. Parts provisioning.
  - m. Document all incoming calls and provide necessary information in DHS incident tracking tool.
- F. The Service Provider shall work in conjunction with CBP personnel and other Technical Operations Division Service Providers to fulfill all customer reported and system outage prevention tasks.
- G. The Service Provider shall comply with CBP's Information Systems Security Policy and Procedures Handbook, HB 1400-05B, February 2005. HB 1400-05B

is classified as for Official Use Only and is not attached to this RFP. The HB 1400-05B policies are critical to ensuring the safety of our nation. As an example, one of the policies that the Service Provider shall ensure compliance to is that all components capable of storing electronic data shall not be removed from CBP facilities without first being cleansed of data. Components in which data cannot be cleansed shall not be removed from Government property. The Service Provider shall notify the COTR about equipment that cannot be cleansed and the COTR will provide direction. A copy of HB 1400-05B will be provided to the Service Provider upon contract award.

- H. Service Provider maintenance personnel who are required to perform hardware support on CBP information systems within CBP-controlled facilities are required to have completed Full-Field Background Investigations. Service Provider maintenance personnel who are required to perform maintenance on CBP information systems within CBP-controlled facilities will be escorted by Government personnel at all times (unless they have been approved for unescorted access after having completed a Full-Field Background Investigation).

#### **C.3.1.1 Critical Infrastructure Maintenance Service**

The term "Critical" refers to equipment (**Appendix D**) that is integral to the performance of CBP mission activities, such as LAN equipment from Cisco switches, servers, APC units and is generally related to any multi user piece of equipment. Critical infrastructure equipment requires continuous availability and is expected to be operational 7 days a week, 24 hours per day, 365 days per year. Critical infrastructure maintenance shall be provided on a fixed-price, per call basis. Critical maintenance ensures that inoperative critical equipment is made operational within 24 hours of the initial problem call. The determination of criticality of specific equipment may vary from site to site or to specific equipment due to the mission responsibilities of each location. As stated in C.3.1.C the COTR or COTR representative must be notified on all critical dispatches and in responding to a critical maintenance call, the Service Provider shall expeditiously determine why equipment is malfunctioning and implement either immediate repair or replacement of it to return the equipment to full operation as relayed to the COTR. Repairs and replacements shall be completed within 24 hours from the time the initial problem call is received by the CBP Technology Support Center technician, regardless of equipment location, normal business hours, weekends, or holidays.

When performing critical maintenance, the following technical elements of maintenance shall apply:

- A. The Service Provider shall ensure equipment conforms to voltage levels,

component values, clearances, tolerances, and safety methods as set forth in the appropriate manufacturer's acceptance test procedures, specifications, handbooks, and drawings.

- B. Parts manufactured of plastic or insulating material shall be replaced when cracked, chipped, burned or if their insulating efficiency, reliability or functional capability is impaired.
- C. Worn, frayed, loose or deteriorated components such as cords, cables, boots, grommets, gaskets, and strain reliefs shall be replaced with new components.
- D. Pitted electrical contacts shall be replaced or repaired as necessary to provide a safe and serviceable item.
- E. Any assembly that has been opened shall be cleaned internally prior to re-assembly.
- F. The Service Provider shall conduct an inspection during re-assembly of repaired equipment to assure that:
  - Component parts and assemblies are securely mounted.
  - Wiring is properly routed, laced, and fastened.
  - Circuit boards are securely plugged in.
  - Electrical circuits are properly fused when applicable.
  - All tools and foreign objects have been removed, including loose parts.

### **C.3.1.2 Standard Maintenance**

As stated in C.3.1.C all standard maintenance calls not under warranty and over 40% of its original cost must be relayed to the COTR or COTR rep for approval. Standard maintenance service shall also be provided on a fixed-price, per call basis. Standard maintenance differs from the definition of critical maintenance in that the item to be repaired is not required to be continuously operating. Standard maintenance is required to be repaired/replaced within 5 business days (by 5 p.m. local time of the site on the fourth business day) from the receipt of a service request by the National Help Desk.

When performing standard maintenance, the following technical elements of maintenance shall apply:

- A. The Service Provider shall ensure equipment conforms to voltage levels, torque values, clearances, tolerances, and safety methods as set forth in the appropriate manufacturer's acceptance test procedures, specifications, handbooks, and drawings.

- B. Parts manufactured of plastic or insulating material shall be replaced when cracked, chipped, burned or if their insulating efficiency, reliability or functional capability is impaired.
- C. Worn, frayed, loose or deteriorated components such as cords, cables, boots, grommets, gaskets, and strain reliefs shall be replaced with new components.
- D. Pitted electrical contacts shall be replaced or repaired as necessary to provide a safe and serviceable item.
- E. Any assembly that has been opened shall be cleaned internally prior to re-assembly.
- F. The Service Provider shall conduct an inspection during re-assembly of repaired equipment to assure that:
  - Component parts and assemblies are securely mounted.
  - Wiring is properly routed, laced, and fastened.
  - Circuit boards are securely plugged in.
  - Electrical circuits are properly fused when applicable.
  - All tools and foreign objects have been removed, including loose parts.
  - Ensure all parts work as intended.

#### **C.3.1.3 Preventive Maintenance**

All preventive maintenance shall be approved by COTR or COTR rep before work is performed.

Requests for preventive maintenance in the past have been nominal; however, there is a known need for regular maintenance on the video imaging and production equipment located in the CBP, DHS, Headquarters (Ronald Reagan Building) in Washington, DC, and at the National Data Center in Springfield, VA, on an estimated once a month or once a quarter basis, depending on actual amount of imaging productions.

#### **C.3.1.4 OEM Certified Maintenance**

In some cases, only the OEM or OEM authorized technicians can repair certain IT equipment or components. In those cases, the Service Provider shall provide OEM certified repair technicians to perform the required maintenance. A list of CBP equipment requiring OEM maintenance is at **Appendix F**. In either case, these equipment repairs that require OEM certified technicians shall be billed on a fixed price, per incident basis, either at the critical infrastructure maintenance service rate or at the standard infrastructure maintenance rate. All equipment on Appendix F shall be verified by the Computer Hardware Group as needing repair before a dispatch is made. All documentation for this process will be entered into DHS's ticket tracking system.

### **C.3.1.5 On-Site TSC/Computer Hardware Group Help Desk**

A. The Service Provider shall provide Government-site technical support services for the Computer Hardware Group on a 24 hours per day, 7 days per week, 365-days per year basis, including holidays. The Service Provider shall provide on-site technical support service, which includes supporting approximately 900 weekly customer calls and management support for this contract at 12825 Worldgate Dr., Herndon VA.

B. Duties of the TSC on-site IT equipment technical staff include: providing telephone support, opening and documenting incident, trouble-shooting incident, providing work around, updating DHS tracking tool with resolution and when available provide assistance to the general user/customer. After approval provide and maintain dispatch records.

C. The Service Provider is responsible for answering incoming customer calls and user assistance calls. This shall also include the answering of some Level 1 calls not related to equipment maintenance requirements. The Service Provider shall create and update IT equipment call and problem tickets in accordance with the CBP Technology Support Center (TSC) procedure.

D. All Service Providers Computer Hardware Group/Help Desk personnel located at the Springfield, Virginia National Data Center, shall be United States citizens and are required to pass a complete background investigation before gaining access to any of CBP's networks or equipment.

### **C.3.2 *Parts Provisioning***

#### **C.3.2.2 Service Requirement Parts Provisioning**

As stated in C.3.1.C COTR approvals is required before ordering spare parts and the Service Provider then shall provide all parts approved and required to satisfy all CBP IT equipment maintenance requirements. This will include critical items such as GBIC, APC unit, SCSI hard drives and other related critical items.

The Service Provider shall acquire repair parts that are have a quality and functionality equal to or exceeding that which was installed in the equipment by the OEM. Only new parts or parts equal in performance and warranted by the manufacturer as equal to new shall be used in effecting repairs.

Any and all replaced parts defective or not, are the property of the Government. The Service Provider may use these replaced defective parts as core exchanges. (Core exchanges are when used parts that are traded in to a part provider in order to reduce

the cost of the new or reconditioned part). The Government will retain defective hard drives or other storage devices containing sensitive or classified material, drums and old toner which is required by the CBP Information Systems Security Policy and Procedures Handbook to be destroyed. When the Service Provider has replaced a defective hard drive or other storage device containing sensitive or classified material, the Service Provider will perform the following (1) If the Local Property Officer (LPO) at the remote site retains the defective device, then the Service Provider will annotate this fact in the CBP Problem Ticket as well as in the Monthly Contract Status Report. (2) If the Local Property Officer (LPO) does not take possession of the defective device, then the Service Provider will ship the defective device back to the duty location and await quarterly destruction. The CBP NDC Facilities Management Contractor will perform the quarterly destruction or when requested by the COTR. The COTR will witness the quarterly destruction of all defective devices capable of storing sensitive or classified information that are returned to duty location. Additionally, the Service Provider will annotate in the Monthly Contract Status Report all defective hard drives or other storage devices containing sensitive or classified material that were shipped back to duty location and destroyed in the quarterly destruction.

### **C.3.2.3 CBP Replacement Parts Inventory**

The Service Provider shall maintain, for the Government, at the Government's site, a supply of high failure and critical equipment parts, equipment, and or customer replaceable parts, i.e., PC components such as keyboards, monitors, hard drives, network switches, fingerprint readers, and project related spare parts equipment. The Service Provider shall acquire and maintain all parts, in quantities appropriate to usage trends and will be required to maintain and repair all equipment within timeframes identified under this contract. A list of current spares/replacement parts inventory is shown at **Appendix E**.

The Government shall provide a CBP warehouse area in the Springfield, Virginia area of approximately 2,500 square feet for the storage of the required spares and replacement parts. Additionally, another 300 square foot storage area for required spares and replacement parts is available at duty location and CBP warehouse.

### **C.3.3 Software Support**

Software support services shall be required where such software is vital to the effective operation of related equipment. For example, the Service Provider shall be required, when performing repairs involving personal computers, to reload operating system software onto the repaired system in order to ensure that the device works correctly. The Service Provider must have an expert command of CBP Microsoft XP image operating system software in order to differentiate between normal or abnormal system operations, to isolate which area of the system may be a cause of the symptom defect.

The Service Provider shall not be required to reload CBP software onto repaired devices.

### **C.3.3.1 Software Technical Support**

The Service Provider shall assist in software technical support for CBP. Software technical support shall include, but is not limited to:

- Assistance in the operation of software, software configuration files and forms.

The Service Provider shall record all software support activities with the DHS PTS. The primary software utilized by CBP is Microsoft operating systems and Microsoft Office Suite.

### **C.3.4 Optional CLIN efforts**

#### **C.3.4.1 Problem Tracking System (PTS)**

DHS's automated PTS is the application for tracking all incidents and service requests and CMS reports on all reported incoming and out going calls. The PTS system is a Commercial Off the Shelf (COTS) product and is currently Remedy. The Service Provider's technicians shall be responsible for populating the PTS in accordance with the maintenance procedure described in Section C.5.1.

The Service Provider shall provide one systems administrator in support for the Remedy system. This includes granting user access to the system, creating or modifying Remedy queues and ensuring that Remedy queue managers are kept up to date. This person will also be required to work with the BEMS and ensure TSC changes are initiated in Remedy.

#### **C.3.4.2 Customer Relations Support**

The Service Provider shall provide one Customer Relations Support for analyzing and defining the Technology Support Center performance measurement criteria, such as: statistics, TSC operational trends, customer service strategy and the development and implementation of customer satisfaction focused processes and procedures. This support shall include integration of new systems into the Technology Support Center. This Customer Relations Support Analyst shall also manage Call Management System ensure that all phone login are current and calls are monitored tracked and all issues are reported to COTR.

The Service Provider shall provide required statistical reports showing TSC operational trends, weekly statistics, etc. A copy of sample Customer Relations Support statistical reports is shown in **Appendix H**.

### **C.3.4.3      *Travel***

During the performance of this contract, the Service Provider may be requested by the Contracting Officer (CO) or the COTR to travel to attend conferences, symposiums, meetings, or for other reasons associated with the Service Provider's duties. Travel costs are not applicable to maintenance calls, as the fixed price for per incident maintenance includes all applicable travel costs required for maintenance efforts. The CO or the COTR will submit all travel requests in writing to the Service Provider. The Service Provider will be reimbursed for travel associated with maintenance support activities of more than 50 miles from the Service Provider's base facilities. Reimbursement of travel expenses shall be in accordance with the latest revision of the Government's Joint Federal Travel Regulations (JFTR). The Service Provider shall submit invoices for travel reimbursement within 30 calendar days of completing the travel. A copy of the requesting letter from the CO or COTR and all receipts associated with the related travel shall accompany the Service Provider's invoices for reimbursement. The Service Provider will not be reimbursed for travel that is not authorized by the CO or the COTR.

### **C.3.5          *Warranty***

#### **C.3.5.1      *Warranty of Labor and Parts.***

The Service Provider's warranty for labor and parts shall be in accordance with the applicable Warranty of Services, Inspection of Services and Warranty of Supplies of a Noncomplex Nature included in section A of this SOW.

#### **C.3.5.2      *UL Certification***

All equipment and parts shall be Underwriters Laboratories (UL) certified, as applicable

### **C.3.6          *Equipment Shipping***

#### **C.3.6.1      *Standard and Critical Maintenance Shipping***

The Service Provider is responsible for shipping all equipment and parts applicable to the performance of maintenance activities associated with the performance of this contract. The cost for all shipping shall be included in the per incident fixed price for maintenance. Shipping costs shall not be billed separately but billed according to each corresponding Remedy ticket. All shipping shall conform to all domestic and to all international shipping regulations, as applicable.

## **C.4 Operating Processes and Procedures**

This section provides a brief description of CBP IT support activities in response to a user-reported issue/problem.

### **C.4.1 Maintenance Procedure**

As the CBP Technology Support Center receives a service call, the Service Provider shall open a call ticket in the PTS, document the user's information, including location, equipment, and nature of the problem. The technician provides initial telephonic troubleshooting instructions and analyzes whether the issue can be quickly resolved on the phone or if the problem requires either a dispatch for on-site service or replacement equipment.

For problems that cannot be resolved on the initial call, the Service Provider shall initiate remedial service immediately from the creation of the problem ticket. Service requests for non-critical service that are received less than 45 minutes from the end of the normal business day (6:30 p.m. EST) may be deferred for dispatch to the next business day. Critical service is to be initiated immediately upon determination of a critical problem.

The Service Provider is responsible for dispatching service technicians to the field sites and shall coordinate the schedule of on-site service with the site representative prior to the technician being dispatched. The Service Provider will have access of site representatives through the automated tracking system (PTS). The Service Provider shall ensure that the technicians arrive on-site with the necessary parts/equipment to complete the repair. The Service Provider shall close problem tickets upon user acknowledgement that the problem has been resolved.

The Service Provider shall meet the following time frames for entering data into the PTS for call tickets and problem tickets:

- i. All call ticket information shall be entered/updated into the PTS system immediately.
- ii. If the call results in a problem ticket being generated, the problem ticket will be created within one hour of the initial call to the Service Provider at the help desk.
- iii. All updates to problem tickets will be entered within one hour of the information being received by the Service Provider at the help desk.

#### **C.4.1.1 Equipment Inventory Usage**

As a request for equipment support service is received, the Service Provider and Government representative will determine the cost effective method or providing either a service request or replacement item from the depot inventory. The Service Provider

maintains (Section C.3.2.3). Where the cost of replacement is less than the cost of repair for the item, the Service Provider is authorized to replace the defective equipment with one of equal functionality. When the cost of replacement is more expensive than the cost of repair, and repair of the defective equipment is not feasible, the Service Provider shall obtain permission from the COTR prior to replacing the defective equipment with a spare. As appropriate, the Service Provider will update changes to the inventory as quantities change.

#### **C.4.1.2 Notification of Problem Resolution Status**

The Service Provider's field service technicians are required to call the CBP Technology Support Center IT technical staff at 1-800-927-8729 before leaving sites where service was performed. The field service technician must provide a verbal report including:

- The CBP trouble ticket number
- Date and time of service completion
- A description of the repair actions taken or other resolution (including parts installed) used to make repairs
- Any associated preventive maintenance activities occurring while on-site

The field service technician shall make a bonafide attempt to have Government site representatives provide a verbal confirmation that the work has been satisfactorily completed. This step saves the Service Provider from having to track down the site representative to provide the verbal confirmation later.

### **C.5 Deliverables and Reporting Requirements**

#### **C.5.1 *Service/Equipment Historical Information***

The Service Provider shall develop equipment historical information reports. These reports shall be generated from information entered by the Service Provider into the PTS Tracking System. These reports shall allow for CBP analysis of problems, symptoms, and causes, and the determination of whether the equipment should be replaced instead of being repaired, or what other level of service needs to be provided. The Service Provider shall use the (PTS) to produce reports to determine equipment maintenance trends.

#### **C.5.2 *Invoicing.***

The Service Provider shall present monthly invoices to the COTR. Invoices shall provide information on fixed-price services and cost-reimbursement services. Invoices shall summarize all expenditures for the month by problem ticket on a contract CLIN basis. Invoices shall also show the cumulative total for expenditures to date for the contract period (either base period or applicable option period) by contract CLIN.

Information provided in the invoices will contain the following:

A. Fixed-Price Maintenance Repair CLINS Costs:

The invoice for the fixed price CLINS (critical and standard maintenance) shall provide the following information for each individual maintenance action performed:

- Date of the maintenance service;
- CBP trouble ticket number **(the CBP trouble ticket number must be closed out in order for the Service Provider to submit this cost in the invoice);**
- Location of the maintenance service;
- Nomenclature, serial number and CBP asset tracking bar code number of the repaired item;
- Description of the maintenance service performed;
- Type of maintenance (critical or standard);
- Description of preventive maintenance performed (if applicable);
- Fixed price maintenance labor cost;
- Materials cost (if applicable);
- Materials General and Administrative Costs (G&A cost) (if applicable);
- Annotation as to whether the Service Provider at the site provided materials or if the materials were drawn from the spares/replacement parts inventory located in Springfield, Virginia.
- Annotation as to whether the defective unit was replaced by a spares drawn from inventory located in Springfield, Virginia;
- Total cost of the maintenance service (fixed price labor per incident cost & materials cost);
- Total number of standard maintenance calls for the billing period;
- Total number of critical maintenance calls for the billing period; and
- Total number of preventive maintenance calls for the billing period.

The invoice will summarize totals by CLINS for the invoice period. The invoice will also summarize cumulative cost totals to date by CLINS.

B. Cost-Reimbursement Spare/Replacement CLINS (Springfield, Virginia Warehouse) costs:

The invoice for spare/replacement parts purchased by the Service Provider for storage at the both duty location and Springfield, Virginia warehouse shall provide the following information:

- Parts purchased during the invoice period (part number, quantities, price and description of parts purchased);
- Cost discounts per part purchased from core exchange turn in of defective parts (should show discount for individual core exchange parts as applied to the new part cost);
- G&A on the parts purchased during the invoice period;

- Total price (parts price and G&A);

D. On-Site Technical Support Costs:

The invoice for the On-Site Technical Support Services (Government site at Springfield, Virginia) shall contain the following:

- Date of the Invoice;
- Dates of service that the invoice covers;
- Fixed Price Labor Category costs for the invoice period, broken down into individual labor categories costs, hours worked and total labor category costs; and
- Total costs for the billing period for the fixed price labor costs.

E. Travel Costs:

The invoice for travel costs shall contain the following:

- Dates of the travel;
- Purpose of the travel;
- A copy of the CO/COTR letter authorizing travel;
- Service Provider personnel who traveled;
- Travel itinerary (from departure to return);
- Travel costs;
- G&A Costs (if applicable); and
- Total travel costs.

Additionally, in order to encourage the timely submission of bills, costs for any amount billed more than 90 calendar days after completion of the maintenance service request shall NOT be paid.

**C.5.3 Monthly Contract Status Report.**

The Service Provider shall provide a bi-weekly contract status report. This report shall detail the following:

- A cover letter with the Service Provider's name and address, the contract number, the date of the report and the period covered by the report;
- Name and telephone number of the preparer of the report;
- Significant changes to the Service Provider's organization or method of operation;
- Reporting period;
- Summary of significant events occurring during the reporting period;
- Problem areas affecting technical, schedule, or cost elements of the contract, including background, impact and recommendations for resolution;

- Results related to previously identified problem areas with conclusions and resolutions;
- Trip reports and significant results;
- Planned accomplishments for the next reporting period;
- For each contract CLIN, the Service Provider shall provide information detailing the expenditures for the reporting period, cumulative expenditures and balances remaining, hours utilized by labor category for the month and cumulative hours utilized by labor category for the period of performance of the contract;
- Details on maintenance performed during the reporting period. This section of the monthly contractor report shall detail all standard and critical maintenance completed during the reporting period. It shall also contain information on all preventive maintenance performed during the reporting period. It shall contain summary information showing total maintenance calls by maintenance category (standard and critical). The report shall also contain details on each individual maintenance action as follows:
  - CBP trouble ticket number;
  - Serial number and CBP asset tag (barcode) number of equipment worked on;
  - Location of the equipment worked on;
  - Date and time of notification of the required maintenance service;
  - Type of maintenance (critical or standard);
  - If equipment requires OEM certified repair personnel, indicate that an OEM certified repair person worked on this maintenance service call;
  - Description of the maintenance service performed;
  - Description of spare part utilized to effect repairs (if applicable);
  - Description of any preventive maintenance performed;
  - Location of the required maintenance;
  - Date and time that the maintenance was completed and the unit returned to service;
- Summary of spares/replacement inventory changes;
- Summary of all equipment that was replaced with spares (replacement authorization by the COTR not required);
- Summary of all equipment that was replaced with spares (replacement authorization by the COTR was required);
- Summary of all equipment and equipment components that was cleansed and returned to the Government. The summary will show by individual equipment, equipment that was either (1) turned over to a Local Property Book Officer at the site or (2) shipped back to the Springfield, Virginia storage site for quarterly destruction;
- Summary of all equipment and equipment components that could not be cleansed and notification on this fact was given to the COTR. Also information on the disposition of the equipment;
- Summary of all equipment that was destroyed quarterly by the Service Provider, as well as the location, date and time of the destruction and the Government personnel (e.g. the COTR) that witnessed the destruction;
- Summary of all preventive maintenance performed by the Service Provider.

#### **C.5.4 Reporting.**

The Service Provider shall submit reports, in the format requested by the government. These reports can cover, but are not limited to such areas as:

- Trip reports;
- Meeting agenda reports;
- Meeting minutes
- Hardware dispatch trends
- Call Management Information
- Hardware Tech Statistics

#### **C.5.5 Report Formats.**

All reports shall be delivered in hardcopy and softcopy format. Softcopies shall be delivered utilizing Microsoft Suite file format. The Service Provider shall submit all reports electronically via CBP electronic mail system in a format specified by the COTR. In the event the system is unavailable or not accessible due to a system malfunction, the Service Provider shall submit all reports in a typewritten format to be followed simultaneously with an electronically transmitted copy as soon as the system becomes operational. All Service Provider reports shall conform to standard report formats contained in the OIT Process Asset Library (PAL).

#### **C.5.6 Delivery Schedule.**

<b>DELIVERABLE</b>	<b>SPECIAL INSTRUCTIONS</b>	<b>DELIVERY DATE</b>
Service Equipment Historical Information	See C.5.1	When Requested.
Monthly Invoice	See C.5.2	Invoice for the month is due by the 15 <sup>th</sup> calendar day of the following month
Monthly Contract Status Report	See C.5.3	Bi-weekly Contract Status Report for the month is due by the 15 <sup>th</sup> calendar day of the following month
Reporting	See C.5.4	As required.
Service Providers QA Plan	See C.9	Draft of the Service Provider's QA Plan is required 15 calendar days after contract award. Final version is due 30 calendar days after contract award.

Customer Relations Support Statistical Reports	See C.3.4 and Appendix H. Appendix H contains samples of the current statistical reports.	Weekly or as required.
--	---	------------------------

**C.6 Personnel Requirements**

**C.6.1 Estimated Personnel Requirements.**

For the purposes of indicating the level of work only, the Government's estimate for the work to be performed in the Computer Hardware Group Help Desk Support is provided below. This estimate is the Government's interpretation of the requirement and is given for illustration purposes only and is not intended to be binding on either party or to be the only possible solution to the requirement. The Service Provider shall provide their own mix and number of personnel required to perform the Help Desk support work based upon Government provided background information in section C.1.2 as well as below.

**Appendix G** contains labor category descriptions for the labor categories shown below. These labor category descriptions are provided also only to illustrate work to be performed and illustrated staff schedules:

	Labor Category	Number of Staff	HRS
Technical Support	Program Manager	1	1,920
	HW Technician	12	23,040
	Inventory Mgt. Specialist	1	1,920
	Customer Relations Manager	1	1,920
	Weekend Hardware Technician	1	1,921
	Systems Analyst	1	968

LABOR CATEGORY	Number of Day Shift (07:00 a.m. to 3:30 p.m. Monday to Friday) Personnel	Number of Evening Shift (3:00 p.m. to 11:30 p.m. Monday to Friday) Personnel	Number of Midnight Shift (11:00 p.m. to 07:30 a.m. Monday to Friday) Personnel	Number of Weekend Shift (07:00 a.m. Saturday – 07:30 a.m. Monday)
Program Manager	1			
Inventory Management Specialist	1			

Customer Relation Manager	1			
Hardware Technician – See Note 2.	3	3	3	3 denotes additional schedule below
System Analyst	1			
TOTALS:	7	3	3	3

Taking into considerations of available funding the schedule below denotes the additional staff schedule for the remaining three techs:

1-6am to 1430  
1-1400 to 2100  
1-2100-630am

Blank areas in the above chart denote no staffing requirements for the labor category for the designated shift/time period.

The Service Provider shall provide only trained and technically experienced personnel to perform service under this contract. The individuals shall possess the level of expertise required for the proper performance of the contract.

Additionally, Service Provider personnel shall have at least the following minimum work experience:

Program Manager: 5 years experience as a Program Manager or Supervisor in a program providing support similar to that of the CBP Computer Hardware Group. Also meets qualifications shown in Appendix G.

Inventory Management Specialist, Customer Relation Manager, Hardware Technician and System Analyst: 3 years experience in a program providing support similar to that of the CBP Computer Hardware Group. Also meets qualifications shown in Appendix G.

Hardware Repair Technicians: 2 years experience in the repair of the appropriate equipment that they will repair under this contract, or equipment that is similar to that shown in Appendix D.

**C.6.2 On-Site Supervisor and Backup**

The Service Provider shall provide an on-site supervisor or Program Manager (PM), responsible for the daily supervision, status of contract funds and operations of this contract. The PM/on-site supervisor shall also serve as a Senior Level Technical Support Analyst. The individual shall interface with the COTR/ACOTR and shall also provide technical support to the COTR on issues related to services outlined within the contract. This support may consist of attending meetings to provide a maintenance

point of view, drafting position papers, planning guides, developing cost/budgetary estimates or other support cost documentation to provide analysis of potential impacts to IT equipment maintenance. This effort will require the supervisor/PM to keep abreast of CBP priorities why to better plan for associated Computer Hardware Group hardware/software support requirements.

**C.6.3 Key Personnel**

The following labor categories or equivalent positions are identified as key personnel:

Labor Category
Program Manager – Key Personnel

(a) The Service Provider agrees to assign those persons whose resumes were submitted with its proposal and who are necessary to fulfill the requirements of the contract as "Key Personnel". No substitutions of Key Personnel may be made except in accordance with the conditions set below. Service Provider personnel who are designated as Key Personnel must be available telephonically to the Government to contact 24 hours per day, 365 days per year, through local or toll-free telephone numbers.

(b) During the first 90 days of contract performance period, no key personnel substitutions will be permitted unless these substitutions are unavoidable because of the incumbent's sudden illness, death or termination of employment. In any of these events, the Service Provider shall promptly notify the CO and the COTR by providing the information described in paragraph (d) below. After the initial 90 day period, the Service Provider must submit to the CO and the COTR all proposed substitutions, in writing, at least 15 days in advance (120 days if security clearance must be obtained) of any proposed substitution and provide the information required by paragraph (d) below.

(c) Any request for substitution must include a detailed explanation of the circumstances necessitating the proposed substitution, a resume for the proposed substitute, and any other information requested by the CO or the COTR. Any proposed substitute must have qualifications equal to or superior to the qualifications of the incumbent. The CO or his/her authorized representative will evaluate such requests and promptly notify the Service Provider in writing of his/her approval or disapproval thereof.

**C.6.4 Technical Support Service Staff - Labor Category Descriptions**

Personnel assigned to perform on this order shall possess a diverse set of skills. **Appendix G** contains representative labor category descriptions for the Computer Hardware Group requirement. Personnel performing on this contract shall be able to

perform the duties for equivalent labor category positions described in **Appendix G**. CBP reserves the right to determine whether an individual's background and experience are sufficient to ensure adequate performance of this order. All Service Provider personnel shown in **Appendix G** will be performing duties at a Government site.

## **C.7 Performance Measures**

The following performance measures shall apply to this contract:

### **C.7.1 *Maintenance Repair Time***

The Government shall track the Service Provider's performance in meeting the stated repair completion times as tracked in the PTS. For Critical and Standard Maintenance problems not completed within the time specified, the Service Provider shall not bill the Government the fixed-price labor cost of that service call. The Government shall not pay for any fixed-price labor costs associated with service calls that do not meet the required repair and return to service thresholds. Critical Maintenance problems shall be completed within 24 hours from the time the problem ticket is opened. Standard incident/service problems shall be completed within 5 business days from the time the problem ticket is opened.

Measurement data for determining the above maintenance repair times will be obtained from repair completion times contained in the PTS.

## **C.8 Security**

### ***Security Requirements***

The Contractor shall comply with CBP administrative, physical and technical security controls to ensure that the Government's security requirements are met. During the course of this Order, the Contractor shall not use, disclose, or reproduce data, which bears a restrictive legend, other than as required in the performance of this Order.

### ***Personnel Security Background Data***

All Service Provider Computer Hardware Group personnel stationed at the National Data Center in Springfield, Virginia and employed by the Service Provider or responsible to the Service Provider for the performance of work at the National Data Center shall either currently possess or be able to favorably pass a full field five (5) year background investigation required by CBP policies and procedures for employment prior to beginning work with CBP. This policy applies to any new personnel hired as replacement(s) during the term of this contract. Service Provider maintenance

personnel who are required to perform maintenance on CBP information systems within CBP-controlled facilities (Ports of Entry) **are not required** to have completed a Full-Field Background Investigation. Service Provider maintenance personnel who are required to perform maintenance on CBP information systems within CBP-controlled facilities will be escorted by Government personnel at all times (unless the Service Provider personnel have been approved for unescorted access after completing a Full-Field Background Investigation).

The Contractor shall submit within ten (10) working days after award:

- a list containing the full name, social security number, and date of birth of those people who will require background investigation by CBP and,
- submit such information and documentation as may be required by the Government to have a background investigation performed

The information must be correct and reviewed by the designated CBP Security Official for completeness. Normally, information requested for a background investigation consists of SF-85P, "Questionnaire for Public Trust Positions" or SF-86, "Questionnaire for Sensitive Positions (For National Security)" TDF 67-32.5, "U.S. USCS Authorization for Release of Information", FD-258, "Fingerprint Chart" and a Financial Statement. Failure of any contract personnel (**except maintenance personnel – see above**) to successfully pass a background investigation shall be cause for the candidate's dismissal from the project and replacement by a similar and equally qualified candidate as determined and approved by the Contracting Officer/COTR. This policy also applies to any personnel hired as replacements during the term of the contract order.

Upon award and when applicable, the CBP assigned COTR of record shall be responsible for processing the "Department of Defense, Contract Security Classification Specification (DD254)" on behalf of the Contractor. The DD254 will authorize the Contractor to conduct additional background investigations for assigned contract personnel required to access SCI facilities and/or classified National Security information and applies to any and all personnel hired as replacements during the term of the contract order.

All background investigation forms must be accepted by CBP with verbal approval from a representative from CBP Office of Management Inspection and Integrity Assurance, Security Program Division (MIIA-SPD), before contract personnel can begin work under this order. MIIA-SPD estimates these procedures will take approximately ten (10) days from the time they receive the packet. Currently, completion of background investigations is taking approximately six (6) months from initial acceptance of the package.

The Contractor shall notify the COTR and CBP Office of Information & Technology (OIT) Workforce Management Group, BI Coordinator of any personnel changes in access requirements for its personnel no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to another contract. The Contract/Project Manager is responsible for the completion

and timely submission to the COTR of the CF-242 for all departing contract personnel. The Contractor shall provide OIT/WMG/BI Coordinator the following information on behalf of their contract personnel to telephone number 703-921-6237 or fax the below information to 703-921-6780:

FULL NAME  
SOCIAL SECURITY NUMBER  
EFFECTIVE DATE  
REASON FOR CHANGE

In accordance with CBP Directive No. 51715-006, "Separation Procedures for Contractor Employees (CF-242)" the Contractor is responsible for ensuring that contract employees separating from the agency complete the relevant portions of the CF-242. This requirement covers all Contract employees who depart while the contract is still active (including resignation, termination, etc.) or upon final completion of contracts. Failure of a contract to properly comply with these requirements shall be documented and considered when completing Contractor Performance Reports.

### ***C.8.1 Security Procedures***

A. Controls: The Service Provider shall comply with the CBP administrative, physical, and technical security controls to ensure that the Government's security requirements are met. During the course of this contract, the Service Provider shall not use, disclose, or reproduce data, which bears a restrictive legend, other than as required in the performance of this contract.

B. Identification Badges: All Service Provider employees shall be required to wear CBP identification badges when working in Government facilities.

C. Security Background Data: The Service Provider employee shall not begin working under the contract until the entire Background Investigation (BI) is completed with approval from CBP, Security Programs Division (**except for Service Provider maintenance personnel – see above**). Exceptions to this requirement will be handled on a case-by-case basis, and access to facilities, systems, data, etc., will be limited until the individual is cleared.

Service Provider employee personnel hired to work within the United States or its territories and possessions that require access to CBP facilities, information systems, security items, and products, and/or sensitive, but unclassified information shall either be U.S. citizens or have lawful permanent resident status.

The following security screening requirements apply to both U.S. citizens and lawful permanent residents who are hired as Service Provider personnel:

All personnel employed by the Service Provider or responsible to the Service Provider for the performance of work hereunder shall currently possess and be able to favorably pass a BI (**except for Service Provider maintenance personnel – see above**).

The Service Provider shall submit within 10 working days after award of this contract a list containing the full name, social security number, and date of birth of these people who claim to have successfully passed a background investigation by the CBP, or submit such information and documentation as may be required by the Government to have a BI performed for all personnel. The information must be correct and be reviewed by a CBP official for completeness. Normally, this shall consist of SF-85P, "Questionnaire for Public Trust Positions;" FD-258, "Fingerprint Chart;" and a Financial Statement.

Failure of any Service Provider personnel to pass a BI means that the Service Provider has failed to satisfy the contract's requirement to provide cleared personnel. The BI is detailed and costly for the government to perform. When a Service Provider employee fails to pass a BI, it costs the government twice as much to complete the investigation. Therefore, if the Service Provider has a continuous problem with providing personnel capable of passing a BI, this will be grounds for termination of the contract.

The Contracting Officer must approve all personnel replacements.

Estimated completion of the investigation is approximately 120 days from the date the completed forms are received in the Security Programs Division.

#### Notification of Personnel Changes

The Service Provider shall notify the COTR and CO via phone, FAX, or electronic transmission, no later than 1 workday after any personnel changes occur. Written confirmation is required for phone notification. This includes, but is not limited to, name changes, resignations, terminations, and reassignments (i.e., to another contract.)

The Service Provider shall notify the OIT ISSB of any change in access requirements for its employees no later than 1 day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other contractors.

The Service Provider shall provide the following information to OIT ISSB at TEL: (703) 921-6116 and FAX (703) 921-6570: full name, social security number, effective date, and reason for change.

C. Separation Procedures: In accordance with Customs Directive No. 51715-006, "Separation Procedures for Contractor Employees," the Service Provider is responsible for ensuring that all separating employees complete relevant portions of the Contractor Employee Separation Clearance, Customs Form 242. This requirement covers all Service Provider employees who depart while a contract is still active (including resignations, terminations, etc.) or upon final contract completion. Failure of a Service

Provider to properly comply with these requirements shall be documented and considered when completing Service Provider Performance Reports.

**D. General Security Responsibilities During Performance:** The Service Provider shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various CBP regulations pertaining thereto, good business practices, and the specifications, directives, and manuals for conducting work to generate the products as required by this contract. Personnel will be responsible for the physical security of their area and GFE issued to them under the provisions of the contract.

All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Service Provider shall conform to all security policies contained in the U.S. Customs and Border Protection Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05B.

**E. Non-Disclosure Agreements:** When determined to be appropriate, Service Provider employees may be required to execute a non-disclosure agreement as a condition to access of sensitive, but unclassified information.

### **C.9 Service Provider's Quality Assurance Program**

The Service Provider shall establish and maintain a Quality Assurance (QA) program. The Service Provider shall document the processes and procedures of their QA program in the Service Provider's QA Plan. The Government shall review and approve the Service Provider's QA plan.

The QA program shall provide independent corporate and on-site management surveillance and inspection of the Service Provider maintenance support operations to assure that the requirements of the contract are satisfactorily being performed. At a minimum, the QA plan shall include the following:

- Information on the staffing plan and subcontractor utilization and management (if applicable);
- Information on the Service Providers inspection program for covering all of the services stated in this SOW. It should specify the areas to be inspected on either a scheduled or unscheduled basis and the Service Provider personnel performing the inspections;
- Methods of identifying deficiencies in the quality of services performed before the level of Service Provider performance becomes unacceptable and the corrective actions needed to be taken; procedures for notifying the COTR when deficiencies are encountered; and descriptions of proposed sampling techniques;
- Methods of documenting and enforcing quality control operations of both the Service Providers' and subcontractors' (if any) work, including inspection and

testing;

- The format for the Service Provider's Quality Control Reports;
- The location of all Quality Assurance inspections, inspection results and any corrective action required and/or performed by the Service Provider.

## **C.10 Government Furnished Equipment and Information**

### ***C.10.1 Government Furnished Equipment***

The Government shall furnish all Government-site, Computer Hardware Group Service Provider personnel located in the Herndon, Virginia area with required computer equipment, telephones, office equipment and office space required to perform these requirements. All work shall occur on Government provided equipment.

The Government shall furnish toll-free (800 telephone numbers) for CBP customers to place maintenance request calls to the Computer Hardware Group.

The Government shall furnish spare/replacement parts warehouse space located in the Springfield area for the storage of required parts. One warehouse facility is the CBP storage facility located in the Springfield area and the other location is on-site, at the Data Center. The warehouse space located in the data center is there to facilitate immediate and quicker response to a user's need. The typical square footage to house this equipment in the warehouse area is approximately 2500 feet and the other in Herndon Va is approximately 300 feet.

The Government shall make available at the time of contract award, all spare/replacement parts currently stored in the Springfield area warehouse. The Government has already purchased the existing spare/replacement parts from the incumbent Computer Hardware Group contractor. The Service Provider shall utilize these existing spare/replacement parts in their maintenance effort, but shall not charge the Government any additional charges for the spare/replacement parts in stock at the time of the contract award.

### ***C.10.2 Government Furnished Information.***

The Government shall furnish all Standard Operating Procedures for CBP Help Desk operations, appropriate Customs Directives, etc necessary to the Service Provider. This will include the CBP Technical Reference Model (TRM), the CBP Information Systems Security Policy and Procedures Handbook (HB 1400-05B) and the CBP Technology Support Center procedures.

## **C.11 Service Provider Personnel**

### **C.11.1 Service Provider Employee Conduct.**

The Service Provider shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance and integrity and shall be responsible for their employee's performance or the quality of their services.

### **C.11.2 Holidays and Administrative Leave.**

U.S. Customs and Border Protection (CBP) personnel observe the following days as holidays: The Service Provider is require to maintain performance criteria noted in this SOW.

New Year's Day,  
Martin Luther King's Birthday,  
Presidents' Day,  
Memorial Day,  
Independence Day,

Labor Day  
Columbus Day  
Veterans Day  
Thanksgiving Day  
Christmas Day

Any other day designated by Federal statute, by Executive Order or by the President's proclamation.

When any such day falls on a Saturday the preceding Friday is observed. When any such day falls on a Sunday, the following Monday is observed. Observance of such days by Government personnel shall not be cause for an extension to the delivery schedule or period of performance or adjustment to the price, except as set forth in the contract.

Except for designated around-the-clock or emergency operations, Service Provider personnel will be able to perform on site under this contract with CBP on holidays set forth above. The Service Provider will only apply a direct charge of a limited staff to the contract for holidays noted above. In the event Service Provider personnel work during a holiday other than those above, no form of holiday or other premium compensation will be reimbursed as either a direct or indirect cost. This does include reimbursement for authorized overtime work.

In the event CBP grants administrative leave to its Government employees, at the site, on-site Service Provider personnel shall also be dismissed if the site is being closed, however, the Service Provider shall continue to provide sufficient personnel to perform around-the-clock requirements of critical efforts already in progress or scheduled and shall be guided by the instructions issued by the Contracting Officer or her/his duly appointed representative. In each instance when the site is closed to Service Provider personnel as a result of inclement weather, potentially hazardous conditions, explosions, or other special circumstances; the Service Provider shall direct its staff as necessary to take actions such as reporting to its own site(s) or taking appropriate leave consistent with its policies. The cost of salaries and wages to the Service Provider for

the period of any such site closure are a reimbursable item of direct cost under the contract for employees whose regular time is normally a direct charge if they continue to perform contract work; otherwise, costs incurred because of site closure are reimbursable as direct costs in accordance with the Service Provider's established accounting policy.

### **C.11.3 Additional Service Provider Personnel Requirements.**

The Service Provider shall ensure that its employees will identify themselves as employees of their respective company while working on CBP contracts. For example, Service Provider personnel shall introduce themselves and sign attendance logs as employees of their respective companies, not as CBP employees.

The Service Provider shall ensure that their personnel use the following format signature on all official e-mails generated by CBP computers:

[Name]  
[Position or Professional Title]  
[Company Name]  
Supporting the XXX Division/Office...  
Bureau of Customs and Border Protection  
[Phone]  
[FAX]  
[Other contract information as desired]

### **C.12 Period of Performance**

Period: March 1, 2009 through February 28, 2010

### **C.13 Homeland Security Enterprise Architecture Requirements**

Information Security Clause:

All services provided under this task order must be compliant with DHS Information Security Policy, identified in MD4300.1, *Information Technology Systems Security Program and 4300A Sensitive Systems Handbook*.

All developed solutions shall be compliant with the HLS EA.

All IT hardware or software shall comply with the HLS EA.

All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO)

for review and insertion into the DHS Data Reference Model.

In compliance with OMB mandates, all network hardware provided under the scope of this Statement of Work and associated Task Orders shall be IPv6 compatible without modification, upgrade, or replacement.

#### **C.14 Compliance with Section 508 of the Rehabilitation Act**

Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998, requires that when Federal agencies develop, procure, maintain, or use Electronic and Information Technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to and use of information and services that is comparable to the access and use available to non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following standards have been identified:

- 36 CFR 1194.21 – Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.
- 36 CFR 1194.22 – Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as Flash or Asynchronous Javascript and XML (AJAX) then “1194.21 Software” standards apply to fulfill functional performance criteria.
- 36 CFR 1194.23 – Telecommunications Products. This applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. that are procured or developed or used by the Federal Government.
- 36 CFR 1194.24 – Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software

standards (1194.21) when the presentation has user controls available.

- 36 CFR 1194.25 – Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this work statement. Specifically but not limited to items using biometrics as described in this work order shall apply with this requirement as well as any other technical standard involving the use of software or Web based interfaces.
- 36 CFR 1194.26 – Desktop and Portable Computers, applies to all desktop and portable computers that are procured or developed under this work statement.
- 36 CFR 1194.31 – Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.
- 36 CFR 1194.41 – Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required “1194.31 Functional Performance Criteria”, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Exceptions for this work statement have been determined by the Department of Homeland Security. Only the exceptions described herein shall be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS Management Directive (MD) 4010.2. DHS has identified the following exceptions that may be applied:

- 36 CFR 1194.2(b) – (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards.

When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the

agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires approval from the DHS Office on Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

- 36 CFR 1194.3(b) – Incidental to Contract, all EIT that is exclusively owned and used by the Contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those Contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.
- 36 CFR 1194.3(f) – Back Office, applies to any EIT item that will be located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment. This exception does not include remote user interfaces that are accessible outside the enclosed “space”.

## **C.15 Information Security**

### **3052.204-70 Security Requirements For Unclassified Information Technology Resources (JUN 2006)**

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, 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 DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security 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.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as

approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

3052.204-71 Contractor employee access.

As prescribed in (HSAR) 48 CFR 3004.470-3(b),

**CONTRACTOR EMPLOYEE ACCESS  
(JUN 2006)**

(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of S SI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities,

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) The individual must be a legal permanent resident of the U. S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

(2) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

(3) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

### **Security Certification/Accreditation**

CBP shall provide personnel with the appropriate clearance levels to support the security certification/accreditation processes under this Agreement in accordance with Attachment D of the DHS Sensitive Systems Handbook Publication 4300A. During all SDLC phases of CBP systems, CBP personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools.

### **Security Review and Reporting**

(a) The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.

(b) The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the Office of Inspector General, CBP ISSM, and other government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/CBP data or the function of computer systems operated on behalf of DHS/CBP, and to preserve evidence of computer crime.

"All services provided under this task order must be compliant with DHS Information Security Policy, identified in MD4300.1, *Information Technology Systems Security Program* and *4300A Sensitive Systems Handbook*."

### **C.16 Infrastructure Transformation Program (ITP) Compliance**

#### **HELP DESK AND OPERATIONS SUPPORT**

The contractor shall provide third tier reporting for trouble calls received from the Help Desk, the DHS Task Manager, or the users. The Contractor shall respond to the initiators of trouble calls as by receiving telephonic notifications of problems, resolving them, or directing them to the proper technical personnel for resolution. Problems that cannot be resolved immediately or with the requirements of the performance standards are to be brought to the attention of the DHS Task Manager. The Contractor shall document notification and resolution of problems in Remedy.

#### **INTERFACING**

As requested by the COTR, assistance in consolidating all systems with the DHS Consolidated Data Center. Resources to be consolidated with the DHS Consolidated Data Center for each system to be determined by the COTR.

### **C.17 Interconnection Security Agreement**

Interconnections between DHS and non-DHS IT systems shall be established through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnect service agreements. Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the official designated by the DAA to have signatory authority.

## C.18 Contracting Officers Technical Representative (COTR)

COTR

(b) (6)

US Customs and Border Protection  
7501 Boston Blvd  
Springfield, Virginia 20598

(b) (6)

## C.19 EA Clause

The Offeror shall ensure that the design conforms to the DHS and CBP enterprise architecture (EA), the DHS and CBP technical reference models (TRM), and all DHS and CBP policies and guidelines as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA) such as the CBP Information Technology Enterprise Principles and the DHS Service Oriented Architecture - Technical Framework.

The Offeror shall conform to the federal enterprise architecture (FEA) model and the DHS and CBP versions of the FEA model as described in their respective EAs. Models will be submitted using Business Process Modeling Notation (BPMN 1.1, BPMN 2.0 when available) and the CBP Architectural Modeling Standards for all models. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

Where possible, the Offeror shall use DHS/CBP approved products, standards, services, and profiles as reflected by the hardware software, application, and infrastructure components of the DHS/CBP TRM/standards profile. If new hardware, software and infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal technology insertion process which includes a trade study with no less than four alternatives, one of which shall reflect the status quo and one shall reflect multi-agency collaboration. The DHS/CBP TRM/standards profile will be updated as technology insertions are accomplished.

All developed solutions shall be compliant with the HLS (Homeland Security) EA (Enterprise Architecture).

All IT hardware or software shall comply with the HLS EA.

Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

All data assets, information exchanges and data standards, whether adopted or

developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model. Submittal shall be through the CBP Data Engineering Branch and CBP EA.

In compliance with OMB mandates, all network hardware provided under the scope of this Statement of Work and associated Task Orders shall be IPv6 compatible without modification, upgrade, or replacement.

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public. All deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt.

## **Appendix A: ACRONYMS**

BI: Background Investigation  
CBP: Bureau of Customs and Border Protection  
COTR: Contracting Officer's Technical Representative  
COTS: Commercial Off-the-Shelf  
DHS: Department of Homeland Security  
ENTS: Enterprise Network and Technology Support  
EST: Eastern Standard Time  
GFE: Government Furnished Equipment  
GFI: Government Furnished Information  
IT: Information Technology  
TSC: Technology Support Center  
LPO: Local Property Officer  
OEM: Original Equipment Manufacturer  
OIT: Office of Information and Technology  
PAL: Process Asset Library  
PM: Preventive Maintenance  
PM: Program Manager  
PTS: Problem-Tracking System  
QA: Quality Assurance  
TRM: CBP's Technical Reference Model  
UL: Underwriters Laboratories

## Appendix B: COMPUTER HARDWARE GROUP CALL STATISTICS

Below is a six (6) month snap shot of service calls placed with the CBP Technology Support Center from the CBP user community. The call volume may change due to equipment age or upgrade in equipment. The calls below are designed to give some insight to the regional areas that service calls were generated from within CBP. These calls cover a variety of equipment failures from simple monitor problems to Server / Switch problems.

Area (States, Territories, Aruba, Bermuda & Bahamas) Service Call Generated
--

1. Washington, Idaho, Montana, North Dakota, Northern Minnesota, Oregon, California, Nevada, Utah, Wyoming, Colorado, Alaska, Hawaii, Guam.	1,566
2. South Dakota, Southern Minnesota, Michigan, Wisconsin, Iowa, Nebraska, Kansas, Illinois, Indiana, Ohio, Missouri, Arkansas, Louisiana, Mississippi, Alabama, Tennessee, Kentucky.	1,264
3. New York, Pennsylvania, West Virginia, Virginia, Maryland, Delaware, Washington, DC., Puerto Rico, U.S. Virgin Islands.	1,978
4. Eastern New York, New Jersey, New Hampshire, Vermont, Connecticut, Massachusetts, Maine.	1,524
5. North Carolina, South Carolina, Georgia, Florida, Aruba, Bermuda and Bahamas.	2,804
6. Eastern and Southern Texas	1,502
7. Western Texas, Oklahoma, New Mexico.	2,180
8. Arizona	1,830
9. Southern California, Southern Nevada	1,006
<b>Total Service Calls Generated:</b>	<b>15,654</b>

### Outside Territorial United States

France	54
Canada	55
Dublin	24
England	04
Belgium	02
Beijing	06

Total Service Calls Generated: 145

As stated, these totals are subject to change due to equipment age and technology upgrades.

## **Appendix C: EQUIPMENT REPAIR, REPLACEMENT & WARRANTY STATISTICS**

***Major Equipment replacement and warranty report for a recent six-month time period***

### ***Vendor Out of Warranty Replacements***

#### **American Power Conversion (APC)**

Units ranging from 500 to 2200.

#### **Cisco Switches**

Switches ranging from 2900 to 4000

#### **Hewlett Packard Printers**

Ranging from Ink Jet to Laser Jet. Dispatching on LAN printers and prior approval for stand alone printers.

#### **Tektronix**

5 Phaser 740	Replaced with Phaser 840
6 Phaser 860	Replaced with Phaser 6200N

#### **Genicom Printers**

25 – Genicom 3910S	Replaced with Genicom 3860S
20 – Genicom 3910IS	Replaced with Genicom 3860S
10 – Genicom 4840	Replaced with Genicom 5100

#### **Dell P.C.s**

GX 270 / 280 / 620 / 745 / 755

### ***REPAIR Activities***

#### **Rochford Thompson Passport Readers**

361 – Passport Readers

Identix Fingerprint Reader

3 – Readers

CrossMatch Fingerprint Readers

66 – Single print Reader

LaserCard Document Scanner

30 – Scanners

**Warranty Repairs:**

Dell

2300 – Systems boards (Dell model 240/270)

2300 – 40gig Hard drives (Dell model 240/270)

## Appendix D: CBP COMPUTER HARDWARE GROUP EQUIPMENT

Customs and Border Protection, (CBP) currently has approximately 2600 sites in the Territorial United States and 200 sites outside of the Territorial United States with about 65,000 personnel. The equipment information displayed contains the majority, but not all manufacturers Makes and Models, of CBP equipment located within the CBP organization.

Customs and Border Protection currently has 1800 sites that currently hold critical equipment. Critical equipment is defined as "any piece of equipment that supports multiple users and is essential to the CBP mission. That equipment is identified as, but not limited to: Servers, Switches, Controllers, and Gateways. Critical equipment is located throughout CBP, both in the Territorial United States and outside of the Territorial United States, and will require Critical maintenance requirements, per the SOW.

Noted below is a partial equipment list that CBP has currently in its' user community. This list is subject to change through upgrade or technology refresh. Unless approved by COTR, any item falling outside of the scope of this list (i.e. Fax machines, Blackberries, etc.) shall not be covered by this Statement of Work. Additionally, consumable items such as toner cartridges, maintenance kits, etc. are also not covered.

(b) (7) (E)

(b) (7) (E)

(b) (7) (E)

(b) (7) (E)

(b) (7)(E)

(b) (7)(E)

## Appendix E: CBP COMPUTER HARDWARE GROUP SPARES LIST

Noted below is a list of spare equipment used to support CBP's users and customer community. This equipment is housed at two locations. One is the CBP storage facility located in the Springfield area and the other location is on-site, at the Technology Support Center (TSC), Herndon, Va. The equipment located in the TSC is there to facilitate immediate and a faster response to a customer or user's need. This equipment is generally used for Urgent or critical situations. Once these spare units have been diminished, only COTR or COTR representative can authorize new purchase equipment order for spare equipment. The typical square footage to house this equipment in the warehouse area is approximately 2,000 feet. A separate location approximately 20X20 will be available for critical equipment access and shipments. This spares list is not all-inclusive of the spares utilized by CBP. Additionally, this list is subject to change due to technology additions and support requirement for the CBP mission.

Computer Hardware Group Spares List
-------------------------------------

(b) (7) (E)

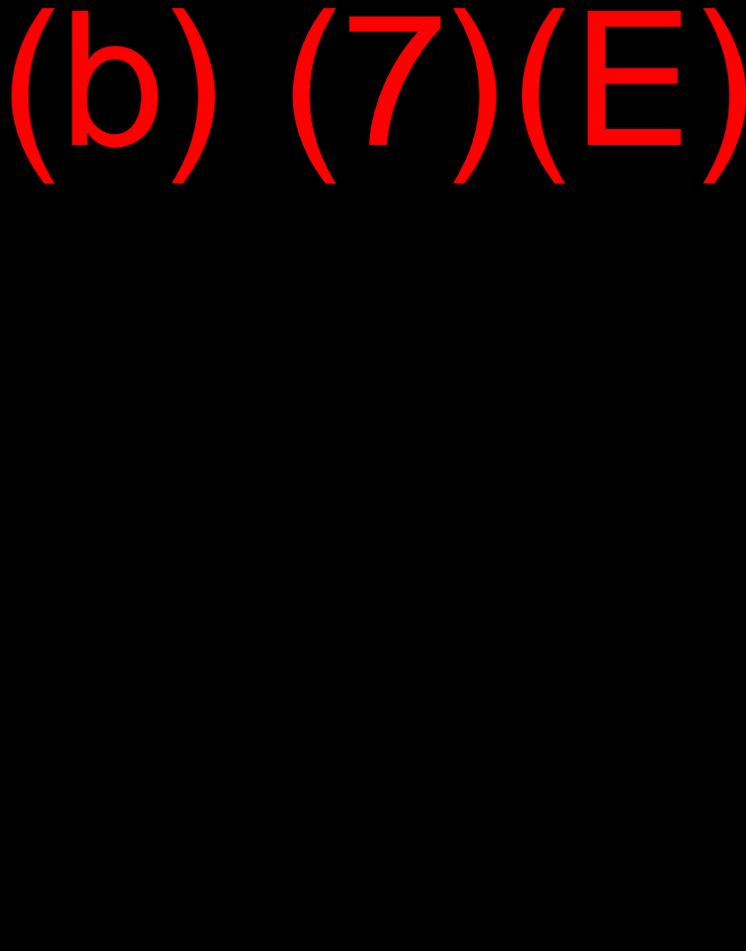


(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)



## Appendix F: CBP EQUIPMENT THAT MIGHT REQUIRES OEM CERTIFIED MAINTENANCE

CBP has established a list of equipment that is deemed to require Original Equipment Manufacturer (OEM) certified maintenance technicians. These vendors are listed as, but not limited to the following:

Vendor	Equipment
Anteon Corporation	Lasercard Readers
Communications Engineering Inc.	Television Studio Equipment @ HQ
Datacard Group	Magna AIT & Magna PS Printers
IBM	RISC Servers w/ external Drives
IBM	T520 – T522 Printers
Intermec	Model 155 Handheld Scanners
OSI	Laser Readers
Rochford Thompson	Passport Readers
Total Video Solutions Inc.	TV Equipment located at NDC & Herndon
TransCore	Radio Frequency Equipment & Antennas - UAP 2100
TransCore	Radio Frequency Equipment & Antennas - AA3110 Transcore Antennas
Xerox Corporation	Techtronic Printers (Models 340s – 8200 series)

*\*CBP reserves the rights to add to this OEM list as technology enhancements are made to support the CBP mission.*

## **LABOR CATEGORY DESCRIPTIONS**

Personnel assigned to perform on this order shall possess a diverse set of skills. The following are examples of the labor categories that may be associated in support of this effort. Personnel performing on this contract shall be able to perform the duties for equivalent labor category positions described herein. CBP reserves the right to determine whether an individual's background and experience are sufficient to ensure adequate performance of this order. All Service Provider personnel will be performing duties at a Government site.

### **Program Manager**

The Program Manager serves as the Service Provider's on-site technical manager. The Program Manager shall attend weekly and monthly meetings with the COTR (CO) to evaluate performance, and act as technical support representative in support of CBP IT equipment maintenance. The Program Manager keeps abreast of CBP project priorities to appropriately plan for hardware/software maintenance support, enhancements and/or personnel development requirements. The Program Manager may also be required to represent the CBP Technology Support Center hardware maintenance interests at meetings.

### **Inventory Management Specialist**

The Inventory Management Specialist is responsible for tracking and updating the status of IT equipment and spare/repair parts. This person provides overall inventory management of Government-owned IT equipment in the possession of the Technology Support Center. Duties include receipt of new equipment, transfer of equipment between separate organizations, and inventory disposal, in accordance with CBP property management processes and procedures. Additionally, this person researches prices and suppliers for parts and equipment and interfaces with these suppliers during inventory restocking activities. The inventory specialist shall maintain an up-to-date inventory of spare parts/equipment and shall complete a 100 percent physical inventory of Computer Hardware Group property at a frequency identified by the Government (this requirement has typically been yearly).

### **Customer Relation Manager**

The Customer Relation Manager recommends customer support strategy to the Technology Support Center government leads. This person develops, maintains, measures, and markets/communicates effective, customer-focused activities throughout the ENTS. Additional activities performed by this person are:

- Assessing, designing, and measuring the effectiveness of Customer Relationship Management (CRM) solutions
- Identifying opportunities for routine CRM processes
- Developing advanced service delivery capabilities
- Providing Customer Service oversight of all projects affecting TSC, CBP's customers and users.

- Interfacing with senior management in the development and delivery of the customer focused service strategy.
- Developing the TSC customer communications strategy.

### **Hardware Technician**

The Hardware Technician answers incoming user calls and telephonically or manually performs diagnostics, repairs, installation, maintenance, upgrades, configurations, and other technical support on a range of computer hardware and peripheral devices to resolve user reported IT equipment problems/issues. This role also installs PC software and configures PC systems as necessary to support effective use of the installed software. Additionally, the hardware technician maintains status updates to call/problem records in the PTS of PC repairs, installations, and hardware/software configurations in accordance with CBP processes and procedures. As necessary, the hardware technician packages parts/equipment for shipping, coordinates with shipping vendors, and tracks shipping/delivery status of shipments.

### **Systems Analyst**

The Systems Analyst is responsible for all PTS application support functions in the TSC. This Systems Analyst oversees and/or performs the process of PTS application administration, grants user access and initiates database field changes, in accordance with CBP Systems Development Life Cycle (available at contract award) processes and procedures. The Systems Analyst evaluates the PTS for process and interface improvements, creates and presents training documentation, acts as problem manager to ensure timely closure of problem tickets, is responsible for system maintenance, and accountable for planning system and version upgrades. The Systems Analyst also defines the scope and assesses the risks of configuration changes to the PTS product.

## **Appendix G: Customer Relation Manager SAMPLE REPORTS**

**Report 1 – TSC Dashboard Sample Report for each group and individual in that group: Example is of LAN Support**

Agent Name	ACD Calls Answered	Avg ACD Talk Time	Avg ACW Time	Extn In Calls	Avg Extn In Time	Extn Out Calls	Avg Extn Out Time	Total ACD Talk Time	Total Agent Ring Time	Total AUX Time	% of Time in Aux	Avail Time	Staffed Time	Ring No Ans
Totals	746	266.9129	67.53351	31	228.7419	489	85.95092	204884	4285	493722	27.1	1038249	1822787	2
(b) (6)	4	215.5	60	0	0	0	0	862	29	8054	27.7	19863	29048	C
(b) (6)	6	235.1667	54	0	0	1	4	1411	24	3298	10.4	25936	31839	C
(b) (6)	11	217.2727	60	0	0	7	55.57143	2478	79	3838	13.1	21837	29254	C
(b) (6)	17	242.4706	56.76471	0	0	9	49.33333	4122	124	10900	35.6	14393	30644	C
(b) (6)	3	138.6667	60	6	216	19	126.2105	416	17	21516	69.7	8526	30881	C
(b) (6)	7	175.4286	60	0	0	0	0	1044	40	2746	8.9	26019	30857	C
(b) (6)	9	209.7778	60.22222	0	0	0	0	1888	53	4601	12.1	30909	37993	C
(b) (6)	13	439.3077	51.53846	0	0	15	97.4	5711	72	10976	35.6	12782	30861	C
(b) (6)	17	387.9412	55.05882	0	0	4	287	6595	111	8205	26.7	14830	30726	C
(b) (6)	12	239.5	751.3333	0	0	7	36	2874	91	12359	36.8	9249	33618	C
(b) (6)	16	369.9375	59.75	0	0	16	100.375	5919	71	6955	23	16281	30297	C

## Report 2 – TSC Weekly Activity Sample Report

**TSC Activity for the week of:**

Management Observations and Comments	
<b>Service Center Call Ticket Activity:</b> All Tickets Created: (Method of Contact = Phone) 3988 All Tickets Created: (Method of Contact = All Other) 455	Note: Contact Resolution percentage activity includes TSC phone activity.
<b>All Handling Activity:</b> All Calls Answered: 4262 All Call Abandoned Percentage: 9% All of Phone calls answered by User Assistance: 20%	
<b>Contact Handling Adherence:</b> All Tickets created as a % of Calls Answered: 94% Impact Field Usage: See Note for Updated Definition. 8%	
<b>Contact Resolution:</b> All of Quick Closed Tickets (QC): All First Call Resolution: (QC as a % of Calls Answered): 49%	
<b>Same Day Resolution:</b> All of Phone Requests Resolved Same Day: 66%	
<b>Note: UPDATED measure:</b> Percentage of Call Tickets with "INFORMATIONAL" in Impact field in Service Center.	

Group		Opening Assignment Activity of	Call Tickets Created	# of Quick Closed tickets	Quick Closed %	Problem tickets: <u>Open status as of:</u>
						<b>Assignment Group</b>
ACE HELP DESK	264	ACE HELP DESK	212	130	61%	SERVICECENTER SUPPORT
TSC	106	TSC ACS	1	0	0%	SITUATION ROOM
Asset Management	194	ITC ASSET MANAGEMENT	689	164	24%	TECHNOLOGY SUPPORT CENTER
Communications *	803	TECHNOLOGY SUPPORT CENTER	171	61	36%	TSC ACS ASSISTANCE
INTERNAL ACE	108	INTERNAL ACE	127	39	31%	ITC ASSET MANAGEMENT
EMOPS	818	TSC EMOPS	1012	603	60%	ITC ASSET SHIPPING
LAN Support	712	TSC LAN	1563	999	64%	ITC ASSET VIATECH
APPLICATIONS SECURITY *	1121	ITC OPERATING SYSTEMS GROUP	0	0	0%	TSC DHS EMAIL
TSC	264	ITC APPLICATIONS SECURITY *	400	391	98%	

er Assistance	873	NCC COMMUNICATIONS *	126	29	23%
VISIT	186	TSC TECS	213	98	46%
ter Hour Calls	737				
		<b>Total*:</b>	<b>3988</b>	<b>2094</b>	<b>53%</b>
<b>tal* :</b>	<b>4262</b>				

TSC EMOPS
TSC EMOPS Level 2
TSC EMOPS Level 3
TSC FAST ASSISTANCE
TSC INSPECTIONS HARDWARE
TSC INSPECTIONS SOFTWARE
TSC LAN
TSC LAN NDC
ITC OPERATING SYSTEMS GROUP
ITC LICENSE PLATE READER
ITC MAINFRAME PASSWORD *
NCC COMMUNICATIONS *
NCC SPRINT SUPPORT *
TSC REMOTE
TSC TECS ASSISTANCE
TSC SECURE DIALUP PROBLEMS
TSC SECURE DIALUP REQUESTS
ECP ACE
ECP HELP DESK (INTERNAL ACE)
<b>TSC Total*:</b>

**Notes:**

NCC Communications, NCC Sprint Support and ITC Mainframe Password Open Problem tickets are shown but are not included in the TSC Open Problem Ticket Total.

ITC Applications Security and NCC Communications activity is shown but is not included in the overall TSC performance measures.

### Report 3 – TSC SUMMARY SAMPLE REPORT

Entire TSC	Total Calls Offered	Total Calls Answered	Total Calls Abandon	Total Transfer Calls	Voicemail Calls	Call Tickets Closed	Same Day Resolution
Week of	6512	4756	685	571	500	3084	<b>3084 (65%)</b>
Week of	6207	4765	587	603	252	3001	<b>3001 (63%)</b>
Week of	5936	4674	630	525	107	3007	<b>3007 (64%)</b>
Week of	5419	4262	466	616	75	2807	<b>2807 (66%)</b>

Group Name	Total Calls Offered	Total Calls Answered	% of Calls Answered	Total Calls Abandon	Total Transfer Calls	Voicemail Calls	Avg. Speed of Answer	Avg. Talk Time	Info. Purposes # of calls abandoned under 10 seconds
Week of									
ACS	135	106	79%	8	19	2	:32	2:22	2
Asset Management	204	194	95%	3	7	0	:32	6:22	1
EMOPS	1046	818	78%	174	37	17	1:57	3:13	30
LAN Support	769	712	93%	51	0	6	:59	5:24	9
TECS	656	264	40%	139	215	38	6:12	3:44	4
User Assistance	1238	873	71%	30	335	0	:18	3:09	20
US VISIT	201	186	93%	12	3	0	:34	3:35	3
After Hour Calls	765	737	96%	27	0	1	:23	2:48	13
ACE	276	264	96%	11	0	1	:14	3:20	3
INTERNAL ACE	129	108	84%	11	0	10	:11	2:31	6
<b>Total:</b>	<b>5419</b>	<b>4262</b>	<b>79%</b>	<b>466</b>	<b>616</b>	<b>75</b>			<b>91</b>

**Other area(s):**

Systems Security	1843	1121	61%	144	353	225	1:30	2:08	23
Communications	875	803	92%	61	0	11	:29	3:46	24

Comments:

\*

\* Approximately 100 contacts during the week of were associated with the rollout and use of the Learning Management System (LMS).

\*

\*

\* For information purposes, a column has been added reflecting the number of abandoned calls that occurred under 10 seconds.

Other Groups)	Total Calls Offered
SAP	200
ICE	1349