

REQUEST FOR QUOTATION (THIS IS NOT AN ORDER)		THIS RFO <input type="checkbox"/> IS <input checked="" type="checkbox"/> IS NOT A SMALL BUSINESS SET ASIDE		PAGE 1 OF 76 PAGES	
1. REQUEST NO. HSSCCG-10-Q-00025		2. DATE ISSUED 10/15/2009		3. REQUISITION/PURCHASE REQUEST NO.	
5a. ISSUED BY USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403		6. DELIVERY BY (Date)		7. DELIVERY <input checked="" type="checkbox"/> FOB DESTINATION <input type="checkbox"/> OTHER (See Schedule)	
5b. FOR INFORMATION CALL: (No collect calls)		8. DESTINATION		9. NAME OF CONSIGNEE Office of Field Operations	
NAME Steven Putnam		TELEPHONE NUMBER AREA CODE 802 NUMBER 872-4111		b. STREET ADDRESS 20 Mass. Ave NW, 1st Floor Attn: Mark Jeanmaire	
8. TO:		a. NAME		b. COMPANY	
c. STREET ADDRESS		c. CITY Washington		d. STATE DC	
d. CITY		e. STATE		f. ZIP CODE 20529	
10. PLEASE FURNISH QUOTATIONS TO THE ISSUING OFFICE IN BLOCK 5a ON OR BEFORE CLOSE OF BUSINESS (Date) 10/29/2009 1600 ET		IMPORTANT: This is a request for information, and quotations furnished are not offers. If you are unable to quote, please so indicate on this form and return it to the address in Block 5a. This request does not commit the Government to pay any costs incurred in the preparation of this quotation or to contract for supplies or services. Supplies are of domestic origin unless otherwise indicated by quote. Any representations and/or certifications attached to this Request for Quotations must be completed by the quote.			
11. SCHEDULE (Include applicable Federal, State and local taxes)					
ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)
0001	<p>ALL PRICING PROVIDED SHALL BE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THE CONTRACTOR'S RESPECTIVE DHS FIRSTSOURCE CONTRACT.</p> <p>A FIRM-FIXED PRICED DELIVERY ORDER WILL BE ISSUED FROM THIS SOLICITATION.</p> <p>Biometric (Live-Scan) Capture Systems, Cabinet Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A.</p> <p>Continued ...</p>	400	EA		
12. DISCOUNT FOR PROMPT PAYMENT		a. 10 CALENDAR DAYS (%)	b. 20 CALENDAR DAYS (%)	c. 30 CALENDAR DAYS (%)	d. CALENDAR DAYS NUMBER PERCENTAGE
NOTE: Additional provisions and representations <input type="checkbox"/> are <input type="checkbox"/> are not attached					
13. NAME AND ADDRESS OF QUOTER		14. SIGNATURE OF PERSON AUTHORIZED TO SIGN QUOTATION		15. DATE OF QUOTATION	
a. NAME OF QUOTER		16. SIGNER		b. TELEPHONE	
b. STREET ADDRESS		a. NAME (Type or print)		AREA CODE	
c. COUNTY		c. TITLE (Type or print)		NUMBER	
d. CITY		e. STATE		f. ZIP CODE	

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition not usable

STANDARD FORM 18 (REV. 6-95)
Prescribed by GSA - FAR (48 CFR) 53.215-1(a)

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED

HSSCCG-10-Q-00025

PAGE

OF

2

76

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0002	Biometric (Live-Scan) Capture Systems, Desktop Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A.	100	EA		
0003	Biometric (Live-Scan) Capture Systems, Laptop (Mobile) Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A.	100	EA		
0004	Disposal of existing Biometric (Live-Scan) systems in conjunction with the installation of the new Live-Scan systems at all USCIS locations specified in Attachment A and in accordance with the Statement of Work.	602	EA		
1001	Option Period 1 - Biometric (Live-Scan) Capture Systems, Cabinet Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A. (Option Line Item)	40	EA		
1002	Option Period 1 - Biometric (Live-Scan) Capture Systems, Desktop Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A. (Option Line Item)	10	EA		
1003	Option Period 1 - Biometric (Live-Scan) Capture Systems, Laptop (Mobile) Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support systems as specified in the Statement of Work. All locations for delivery, install and training Continued ...	10	EA		

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED	PAGE	OF
	HSSCCG-10-Q-00025	3	76
NAME OF OFFEROR OR CONTRACTOR			

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	are in Attachment A. (Option Line Item)				
1004	Option Period 1 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Cabinet Type Biometric System, as detailed in the Statement of Work. (Option Line Item)	400	EA		
1005	Option Period 1 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Desktop Type Biometric System, as detailed in the Statement of Work. (Option Line Item)	100	EA		
1006	Option Period 1 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Laptop (Mobile) Type Biometric System, as detailed in the Statement of Work. (Option Line Item)	100	EA		
2001	Option Period 2 - Biometric (Live-Scan) Capture Systems, Cabinet Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. (Option Line Item)	40	EA		
2002	Option Period 2 - Biometric (Live-Scan) Capture Systems, Desktop Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. (Option Line Item)	10	EA		
2003	Option Period 2 - Biometric (Live-Scan) Capture Systems, Laptop (Mobile) Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support systems as specified in the Statement of Work. (Option Line Item)	10	EA		
2004	Option Period 2 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Cabinet Type Biometric System, as detailed in the Statement of Work. (Option Line Item)	400	EA		
2005	Option Period 2 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Desktop Type Biometric System, as detailed in Continued ...	100	EA		

CONTINUATION SHEET

 REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSSCCG-10-Q-00025

PAGE 4 OF 76

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
2006	the Statement of Work. (Option Line Item) Option Period 2 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Laptop (Mobile) Type Biometric System, as detailed in the Statement of Work. (Option Line Item)	100	EA		

STATEMENT OF WORK

UNITED STATES CITIZENSHIP & IMMIGRATION SERVICES (USCIS) Application Support Center (ASC) BIOMETRICS (LIVE-SCAN) REFRESH

September 30, 2009

1.0 Title of Project

USCIS ASC Biometric (Live-Scan) Refresh

2.0 Period of Performance

The period of performance for this delivery order consists of a one year base period and two consecutive one year options. The base period will cover the replacement of the 602 existing biometric capturing systems (to include disposal of old equipment and delivery and installation of the new equipment), also the first year Operations & Maintenance (O&M) support will be provided as part of the new equipment purchased. In option years one and two, continued O&M support will be provided. Also, in the option years, additional Live-Scan Systems may be purchased up to a maximum of 60 units per year.

3.0 Contacts

The Contracting Officer at time of award will appoint a Contracting Officer Technical Representative (COTR) and furnish appointment information to the contractor.

4.0 Background

The United States Citizenship and Immigration Services (USCIS) utilizes Live-Scan electronic fingerprint scanning systems to digitally capture and electronically submit applicant fingerprint images to the Federal Bureau of Investigation (FBI) and US-VISIT. The fingerprints are used to conduct criminal background checks prior to USCIS making a determination whether to grant immigration benefits to applicants. Live Scan systems are currently at approximately 134 USCIS Application Support Centers (ASCs) located throughout the United States and the U.S. territories of Saipan, Guam, the Virgin Islands, and Puerto Rico. In 2001, in response to increased applicant workload resulting from the Legal Immigration Family Equity (LIFE) Act, USCIS initiated collection of digital photographs and digital signatures at the ASCs to further streamline and reduce timeframes needed to process USCIS benefits applications. Live-Scan systems acquired under this delivery order are expected to be used predominately at domestic ASCs and other domestic USCIS sites to replace existing Live-Scan technology that has become worn and outdated. Deployment of Live Scan devices and applicable support to overseas sites may be required under this delivery order, and is considered to be within scope. The existing live scan systems are to be replaced by newer model Live-Scan systems (approximately 400 "cabinet" style machines, 100 "desktop" style machines, and 100 "mobile" style machines) in early 2010. As new systems are deployed at each site, the old systems must be de-installed and disposed. USCIS intends for the contractor to dispose of 602 live scan systems at the ASC sites. This solution will continue to support USCIS' biometrics capturing goals of:

- Improving efficiencies,
- Preventing fraud,
- Ensuring accurate biographic/demographic data,
- Validating the biometrics data, and
- Meeting FBI image quality standards.

5.0 Scope

A description of the application process and the USCIS operating environment and resources available to the Contractor is provided below. Based on the current environment, the Contractor shall provide a turn-key Live-Scan system that can be connected to the USCIS LAN/WAN and which includes all the turn-key Live-Scan components and configurations to meet the operational requirements of this SOW. Live-Scan systems and components must have "plug and play" capability to capture and transmit FD-258 type 14 and type 4 fingerprint impressions, biographic and demographic data, and digital signatures in standard TIFF image format, and Joint Photographic Experts Group (JPEG) photograph images. As Citizenship and Immigration Services' requirements evolve, the Live-Scan systems provided under this delivery order shall be capable of capturing and transmitting additional biometrics data (e.g., iris, pressed 2-print images, etc.) with minor component and configuration changes, if required by the Government. The Contractor shall also provide, as a minimum, Live-Scan system hardware and software installation and integration services, remote VPN software maintenance, remedial hardware maintenance, technical support (toll-free telephone hotline), training (on-site user/ on-site systems administrator), standard commercial warranty, shipping, and removal/disposal of old equipment. The Contractor shall furnish all necessary personnel, materials, and other supplies/services as may be required to perform the work set forth in this SOW.

5.1 Current Environment

USCIS collected biometrics data from 2.5 million immigration benefits applicants in Fiscal Year 2009, of which approximately 1 million required ten-print fingerprinting and the remainder required collection of single flat impression (press) fingerprints, photographs, and digital signatures. USCIS will continue to use Live-Scan systems for electronic submission of FD-258 fingerprint images to the FBI and US-VISIT for use in searching criminal history databases for records that may disqualify an applicant for benefits. USCIS currently operates 602 Live-Scan devices at 134 ASC sites. **Attachment A** lists current ASC sites. Site locations are subject to change by the Government and the contractor will be notified via modification of specific location changes. Some location changes may require placement of equipment at overseas locations. These overseas locations, when added, will require O&M support. When the government requires relocation of Live Scan systems provided under this delivery order, the government may require the contractor to accomplish the equipment relocation. Any changes to the Live-Scan locations will be conducted through a contract modification and negotiated separately.

Live-Scan systems installed at ASCs will be interfaced to Government-provided store-and-forward mail servers, which in turn interface with USCIS Service Centers. The USCIS Service

Centers are the connectivity points to the Criminal Justice Information System (CJIS) WAN for submitting fingerprints and other biometrics data to the FBI, US-VISIT's IDENT, as well as interfacing with other internal USCIS systems. The ASCs use static Internet Protocol (IP) addresses that require Live-Scan Contractor personnel to maintain and change IP addresses in the field in coordination with the USCIS Help Desk.

The process for capturing biometrics data for immigration benefits is as follows (see **Attachment C** for diagram): The applicant submits an application to USCIS to request an immigration benefit. Application requirements vary for each specific benefit, and therefore require different biometrics collection requirements. Depending on the application being processed, USCIS generates either a 1D bar coded or 2D bar coded scheduling notice informing the applicant where and when to go to get processed for benefits. A 2D barcode is usually generated when FD-258 ten-print processing is required, and a 1D barcode is usually generated when only single press prints, photographs, and signatures are required. When notified, the applicant will go to an ASC to have fingerprints, photographs, signatures, and potentially other data captured using Live-Scan technology.

The normal data capture at the ASCs involves the Live-Scan system operator collecting biographic and demographic data including USCIS-specific identification numbers, name, date of birth, social security number, and other data, either by scanning the scheduling notice 1D or 2D barcode to populate the Live-Scan device data fields, using pull-down menus, or by manually entering the data using the keyboard. Current immigration benefits application requirements call for one of the following scenarios: the application requires FD-258 fingerprints (ten-prints) only; the application requires photograph, single press print (optional), and signature (optional) only; or, the application requires ten-print, photograph, single press fingerprint (optional), and signature (optional).

FD-258 fingerprints (ten-prints) taken at individual Live-Scan devices are forwarded in an Electronic Fingerprint Transmission Specification (EFTS) v7.0 compliant transaction to the local ASC store-and-forward mail server. EFTS is a National Institute of Standards and Technology (NIST) standard used by the law enforcement community (local, state, and federal) and civilian agencies to transmit demographic and image files using a common format. If required, a single press fingerprint image that meets FBI image quality standards is captured of the right index finger, or other finger if necessary. A digitally captured signature in standard TIFF image format is then recorded into the Live-Scan system followed by a facial photograph in standard JPEG image compression format. All the data and images captured can be reviewed and updated at the Live-Scan device before accepting and transmitting to the ASC mail server.

From the local store-and-forward mail server, the EFTS formatted applicant data files (biographic/demographic masthead data and EFTS formatted FD-258 ten-print images) are transmitted to the applicable USCIS Service Center. The Service Center server electronically sends all EFTS formatted applicant data files to the FBI. Applicant data files that include a photograph, press fingerprint, signature image, and associated biographic data are sent to the applicable USCIS service center.

The local ASC mail servers store the EFTS formatted applicant data file records for up to 30 days for reporting and resubmission. Each Live-Scan device currently deployed has minimum

capacity to store and retrieve at least 300 EFTS formatted applicant data files. (Note – This SOW requires a minimum storage and retrieval capacity of 500 each of FD-258 Ten-print files and Biometrics Capture files (total is 1,000). The primary objective of the storage of biometrics on the capture devices is to ensure continuity of operations and not to provide a fail safe for biometric data that gets lost in transmission in the store and forward process.

Neither the Live-scan device nor the local store-and-forward mail server communicates directly with the FBI.

ASC personnel are a mix of Government and contracted labor trained in the taking of quality fingerprints through Live-Scan and manual methods. ASC staffs are non-technical: the level of computer knowledge and abilities of the staff varies from location to location, but is generally very limited. The Live-Scan Contractor is advised that tasks including basic Live-Scan equipment set-up/configuration, basic computer file maintenance, account management, calibrating of systems, basic and preventive maintenance, installation of hardware components, etc. are not within the functional areas and technical abilities required of the ASC staff.

6.0 Live-Scan System Requirements

6.1 FBI Certification

All Live-Scan systems and components delivered by the Contractor shall be capable of transmitting FBI NIST/EFTS images to a local store-and-forward server. Live-Scan systems and components provided under this contract shall be FBI certified to comply with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) Image Quality Specifications (IQS) (See Appendix F) and the US-VISIT IDENT System.

6.2 Functional Requirements

The Live-Scan systems provided by the Contractor shall meet all the functional requirements in Section 6.2 and its sub-sections.

6.2.1 FD-258 Ten-Print Capture Requirements

The Live-Scan system:

- Shall process a minimum of six (6) ten-print applicants per hour (i.e., total time for a skilled fingerprint technician to process one FD-258 applicant shall be 10 minutes or less). The process begins when the Live-Scan system scans the 2D bar code with its scanner, entering FD-258 biographic and demographic masthead data, and ends with the submission of the record to the local store-and-forward mail server.
- Shall create an EFTS transaction containing 14 fingerprint images and biographic masthead data.

The applicant data files transmitted by the Live-Scan system to the local store-and-forward mail server shall include: (a) biographic and site operations text data,

and (b) Wavelet Scalar Quantization (WSQ) compressed fingerprint images (14 blocks) corresponding to fingerprint boxes on the applicant fingerprint card.

The applicant data shall include name, date of birth, sex, race, height, weight, eye and hair color, place of birth, residence, country of citizenship, and all other applicable biographic and demographic data as contained in the masthead of the FD-258 Fingerprint Card. Site operations data shall include fields such as an ASC site identifier; machine code, operator code, and Live-Scan make and model. Text data fields shall conform to EFTS v7.0. Information that populates the EFTS standard will be provided to the vendor after award of the delivery order.

Currently, the fingerprint image records shall include the ten rolled fingerprints, two flat impressions of four fingers (left and right hands) and two flat thumb prints. The image sizes shall be consistent with the fingerprint boxes on the standard FD-258 fingerprint card. The transmitted fingerprint images shall be in compliance with ANSI/NIST Standards identified in the attached FBI Appendix F. The compression algorithms used in the Live-Scan system for compressing the fingerprint images must comply with FBI approved WSQ gray scale compression standards.

- Shall support EFTS v7.0 specifications for maximum sizes of fingerprint images (provided in Table C-2).

Fingerprint	Width Pixels (inches)	Height Pixels (inches)
Rolled impressions Fingers 1 – 10	800 (1.6)	750 (1.5)
Plain Thumb impression	500 (1.0)	1000 (2.0)
4 Finger Plain impression	1600 (3.2)	1000 (2.0)

Table C-2 Maximum Sizes for Fingerprint Images

- Shall support transmission of an EFTS v7.0 file format fingerprint image to the local store-and-forward mail server. **Attachment B** lists typical USCIS server configurations. All the data files shall be transferred to a specified directory on the mail server. All the data files transmitted by the Live-Scan systems shall comply with all applicable FBI, ANSI/NIST and NIST/EFTS standards for the data interchange.
- Shall create and support transmission of an EBTS 8.001 XML file.
- Shall meet the basic format requirements for Logical Record types as defined by the EBTS message set forth in the ANSI standards which are also applicable to transmissions to the FBI.
- Shall create an alpha/numeric identification number in a specified FD-258 field in the event that the applicant does not have either an A-number or a social security

number. The alpha/numeric identification number will consist of a unique applicant identifier appended with a 12-digit date and time stamp in the format CCYYMMDDHHMM. The unique applicant identifier may be a "Z number", which is a 10-digit number generated randomly by the Live-Scan device, an "F number", which is a manually entered number with F in the first position followed by nine numeric numbers, or another unique number specified by USCIS.

- Shall store and transmit a unique site code on each submission in a FD-258 field specified by USCIS.
- Shall read both 1D and 2D bar codes.
- Shall capture type 14 and type 4 fingerprints.
- Shall be capable of capturing quality (FBI-acceptable) fingerprint images for a complete spectrum of skin pigmentation.
- Shall be capable of performing data entry of demographic information using pull down menus/tables.
- Shall be capable of performing instant preview and editing capabilities.
- Shall capture information used for quality control (QC) checks (user ID of the QC checker).
- Shall capture management information to include processing time (date and time stamp for start time and stop time for each applicant record) by machine and by operator, and for each applicant, number of reprints or rejects by machine and by operator. This management data shall, at a minimum, be saved to an ASCII text file and sent to the store-and-forward mail server or other devices.
- Shall have the capacity to store a minimum of 500 ten-print fingerprint records in each machine and 500 biometric records.
- Shall have the capability to purge records from the Live-Scan system upon demand by the user.
- Shall have the capability at the Live-Scan device to query the records stored in the Live-Scan device on an applicant's name, A-number, social security number, or date fingerprinted, and retrieve records and fingerprints (that have not been purged).
- Shall be capable of displaying retrieved records and fingerprints at the Live-Scan device.
- Shall have the capability to edit, modify, and resubmit retrieved records that replace the modified record.

6.2.2 Requirements for Other Biometrics Capture

This subsection specifies requirements for non-tenprint Biometric Capture Only (Single Pressed Print, Photograph, and Signature)

The Live-Scan system:

- Shall process a minimum of six (6) non-tenprint applicants per hour (i.e., total time for a skilled technician to process one applicant shall be 10 minutes or less.) The process begins when the Live-Scan system scans the 2D bar code with its scanner, entering biographic and demographic data, captures a single press fingerprint image, a digital signature, and a digital facial photograph, and ends with the submission of the record to the local store-and-forward mail server.
- Shall allow specified biographic data fields to be entered through the use of 1D and 2D bar code scanners/light pens.
- Shall capture an applicant's signature using a digital signature pad.
- Shall allow the single press-print image and/or digital signature capture to be optional.
- Shall require the digital photograph capture of a single facial photo per record for applicants whose press print, photo and signature are captured.
- The digital camera shall be controlled using the fingerprinting station's keyboard and will utilize face detection software that locates an applicant's face and automatically centers it in the photo. The photo shall be automatically sized to 300 pixels x 300 pixels and saved in the jpeg format.
- Shall create a file containing one facial photograph, biographic data, and an optionally captured digital signature and/or single press fingerprint image.
- The applicant data files transmitted by the Live-Scan system to the local store-and-forward mail server shall include: (a) demographic and site operations data (b) Wavelet Scalar Quantization (WSQ) compressed fingerprint images (one block), (c) FAX4 compressed signature image, and (d) JPEG compressed facial photographic image.
- The applicant data shall include name, alien registration number, social security number and other applicable biographic and demographic data as directed by the ASC Program. Site operations data shall include fields such as an ASC site code, machine code, operator id, and Live-Scan make and model. Text data fields shall conform to EFTS v7.0. Information that populates the EFTS standard will be provided to contractor by the Government after award of the delivery order.
- Shall produce a single press fingerprint .wsq image with maximum dimensions 500 pixels (1.0 inch) wide by 500 pixels (1.0 inch) high.

- Shall support transmission to the local store-and-forward mail server of fingerprint images that meet FBI image quality standards. All the data files transmitted by the Live-Scan systems shall comply with all applicable FBI, ANSI/NIST and NIST/EFTS standards for the data interchange.
- The Live-Scan System shall create an alpha/numeric identification number called a Transaction Control Number (TCN) on each submission in a field specified by the Government. The TCN shall consist of a receipt number (3 alpha characters, 10 numerics) followed by a zero, and followed by a date CCYYMMDD.
- Shall store and transmit a unique site code on each submission in a field specified by the ASC Program.
- The Live-Scan System shall be capable of performing data entry of demographic information using pull down menus. Data entry shall be done using touch screen displays to speed up the processing of the masthead data.
- Shall be capable of performing instant preview and editing capabilities.
- Shall capture management information to include processing time (date and time stamp for each applicant record) by machine and by operator. This management data shall, at a minimum be sent to the store-and-forward mail server.
- Each applicant record shall include demographic data; one JPEG compressed photograph image; one optionally captured fingerprint; and one optionally captured signature.

6.2.3. Technical Requirements for the Live-Scan System

The Live-Scan system provided by the Contractor shall:

- Comply with all applicable FBI, ANSI/NIST, NIST/EFTS Standards outlined in the FBI Appendix F for the data interchange and list such standards in its documentation.
- Be capable of transmitting records using the latest FBI record format – Electronic Biometric Transmission Specification (EBTS) 8.1 and EBTS 8.001 XML.
- Provide the run time licenses for its local applications (e.g., database).
- Include a standard 1yr warranty or better.
- Incorporate standard system security features (e.g., operator log-on, passwords).

- Use Commercial Off The Shelf (COTS) software to allow for the customization of data entry and menu screens. The COTS software should run on a variety of hardware platforms to ensure all devices have the same look and feel to the operators.
- Use Computer equipment (Workstations, laptops, etc.) that meets USCIS Office of Information Technology (OIT) specifications to ensure a consistent platform across USCIS. The workstations and laptops shall be the same or equivalent (brand name or equal) to:

The current OIT-Approved Workstation configuration is: a DELL Optiplex 760 Small Form Factor with an Intel Core 2 Duo E7300 2.66 GHz Processor, 4 GB Memory (2 X 2GB Modules), 160 GB Hard Drive, 8x DVD +/-RW Slimline Drive, 256 MB ATI Radeon HD 3450 Dual DVI/VGI Graphics Card with TV-out, Slimline Floppy Disk Drive, and a 10/100/1000 MB Network Interface Card.

The current OIT-Approved Laptop configuration is: a DELL Precision M6400 with an Intel Core 2 Duo T9550 2.66 GHz Processor, 4 GB Memory (2 X 2GB Modules), 160 GB Hard Drive, 8x DVD +/-RW Drive, 17 inch WUXGA LCD Wide Screen, 9 Cell/85 WHr Primary Battery, 100/1000 MB Network Interface Card, Bluetooth Wireless and 802.11 a/b/g/n Mini-Card, Internal Backlit Keyboard, Internal/External Floppy Disk drive.

- Use an Uninterrupted Power Supply (UPS) that meets USCIS Office of Information Technology (OIT) specifications to ensure a consistent platform across USCIS (applicable to "cabinet" and "desktop" systems). The UPS shall be the same or equivalent (brand name or equal) to:

The current OIT-Approved UPS is: a Smart Pro LCD UPS with a Network Monitoring USB Port, 4 UPS Battery Support Outlets, and Additional 4, Surge Suppression-Only Outlets.

- Be designed to function in an office environment of 60 to 90 degrees Fahrenheit and 20 to 80 percent relative humidity, non-condensing, and shall not require any special air conditioning.
- Meet or provide equivalent facilitation for applicable Section 508 Electronic and Information Technology Accessibility standards for the disabled (see Section 16.0, Electronic and Information Technology Accessibility).
- Be upgradeable such that it is capable of capturing a variety of biometric data including type 14, type 4 fingerprint images, iris, photos, and signature using plug and play devices.

- Be capable of adjusting the height of the scanner decks, and shall have angled keyboards to make the fingerprint equipment ergonomic; for ease of use by the fingerprint technicians (pertains to "cabinet" systems).
- Allow fingerprint capture by use of a foot pedal. The Live-Scan Operator shall be able to capture an applicant's fingerprint images by pressing a foot pedal so that he/she has full use of his/her hands to assist in rolling an applicant's fingers for print capture (applicable to "Mobile", "Desktop" and "Cabinet" systems). This requirement may be omitted if the Live-Scan System allows the Live-Scan Operator full use of his/her hands to assist in rolling an applicant's fingers for print capture.

6.2.4. Hardware Configurations

The Live-Scan Systems are comprised of 3 different hardware configurations in the quantities specified in the delivery order schedule:

1. Cabinet System:

- A standalone system that has the computer, uninterrupted power supply, fingerprint scanner, foot pedal, touchscreen monitor, 1D & 2D barcode reader, digital camera, and digital signature pad supported by a "cabinet" structure.
- A stand may be substituted for a cabinet as long as it meets all of the requirements of the cabinet.
- The "cabinet" or stand shall no larger than 30" deep X 24" wide.
- The "cabinet" or stand shall be robust enough to support all of the above mentioned equipment and withstand full-time operational use for a 5yr lifecycle.
- The "cabinet" or stand shall have locking wheels.
- The fingerprint scanner is easily adjustable for height so that scanner can be raised or lowered to fit the height of the fingerprint technicians and to allow for handicapped access.
- The foot pedal rests on the floor and allows the Live-Scan Operator to capture an applicant's fingerprint images by pressing a foot pedal so that he/she has full use of his/her hands to assist in rolling an applicant's fingers for print capture (applicable to "Mobile", "Desktop" and "Cabinet" systems). This requirement may be omitted if the Live-Scan System allows the Live-Scan Operator full use of his/her hands to assist in rolling an applicant's fingers for print capture.
- The camera is affixed to the cabinet to prevent it from being knocked over.
- The keyboard is angled to help prevent injuries to the operators.
- The CPU and UPS shall be located in a locking enclosure to prevent tampering.
- Computer cables are hidden or are secured to avoid entanglement with the operator or applicant.
- Cable connections are secured to prevent damage if the cabinet is moved.
- Components will be plug and play compatible.

2. Desktop System:

- Composition is the same as the cabinet system, excluding the cabinet itself.
- Hardware is capable of being used on existing tables and or system furniture.
- Camera has to be secured to prevent it from being knocked over or knocked out of position.
- Table top version has all the same functionality as the cabinet version except for height-adjustable scanner deck and angled keyboard.
- Components will be plug and play compatible for ease of setup and removal.

3. Mobile System:

- Composition is the same as the cabinet system with the addition of a ruggedized case and the exclusion of the cabinet, UPS, computer (laptop as substitute), touchscreen monitor, height-adjustable scanner deck, and angled keyboard.
- Camera will be secured to a tripod for easy set up.
- Portable system will be capable of being packed into a single contractor-provided ruggedized case for transport. System must be capable of meeting all airline travel requirements.
- External battery power is provided to allow equipment to be operated in remote locations without electricity.
- All devices will be plug and play compatible for ease of setup and removal.
- A portable backdrop will be included for the purposes of capturing photographs

All components, such as the uninterrupted power supply, fingerprint scanner, foot pedal, touchscreen monitor, 1D & 2D barcode reader, digital camera, and digital signature pad, that may require device drivers shall be consistent across all Live-Scan Systems, without deviation in make and model. This ensures a consistent Live-Scan System across USCIS, which is critical for USCIS operating system image configuration.

6.2.5. Software Configurations

The Contractor shall perform all required Live-Scan software configurations/modifications required to interface with USCIS systems and meet USCIS data profile requirements. The Contractor shall submit the modified software for USCIS approval prior to placement on live-scan systems. Immediately following contract award, USCIS will provide the Contractor with the specifications for data fields and types, screen layouts, and the local store-and-forward mail server connection information. The Contractor will then be responsible for customizing its COTS Live-Scan application software and submitting it to USCIS (Attention: Hugh Jordan) for testing and approval. Testing will occur at USCIS HQ (111 Massachusetts Ave, NW, Washington DC, 20001) in the 2nd floor ASC lab.

As part of the software customization, the Contractor shall be required to maintain USCIS software tables that include demographic information used in processing USCIS Live-Scan transactions. Tables are accessed by the Live-Scan operator through the use of pull-down menus on the Live-Scan device. USCIS will provide USCIS-specific tables (e.g., Originating Agency Indicator (ORI) Code, Reason Fingerprinted, Place of Birth, and Country of Citizenship) to the

Contractor after award for incorporation into the Contractor's Live-Scan software. USCIS will validate all tables during the software approval process.

In addition to the USCIS software configurations, the software requires customization for the processing of UKvisas applicants. See **Attachment E** for the customization requirements for UKvisas.

The Live-Scan application must operate on a USCIS-provided Windows XP operating system with the Federal Desktop Core Configuration (FDCC). The National Institute of Standards and Technology (NIST) FDCC guidelines and specifications are available at the following link: http://csrc.nist.gov/itsec/download_WinXP.html

The USCIS operating system "image" will be provided to the contractor upon award of the delivery order. As part of the USCIS image, the software (to include the operating system), corresponding licenses, and maintenance will be provided by the government via Enterprise License Agreements.

The Live-Scan System shall support a Lightweight Directory Access Protocol (LDAP) connector such that the scanner application software utilizes the Microsoft Active Directory for user accounts and login.

7.0 Delivery

The Contractor shall provide the COTR with one central point of contact for all activities related to initial setup and deployment.

The Contractor must provide two (2) of each type of Live-Scan System ("cabinet", "desktop", and "mobile") to USCIS Headquarters (Attention: Hugh Jordan, Office of Field Operations, 111 Massachusetts Avenue, Washington, DC 20001) within five (5) business days following contract award. A business day is defined as Monday – Friday, 8AM to 5PM. The systems shall include all peripherals and the COTS software (if the "cabinet" and "desktop" configurations include identical computers and peripherals, then only one (1) "cabinet" system and one (1) "desktop" system shall need to be provided). These systems will be used for the purpose of systems configuration/compatibility testing and solidifying the USCIS operating system "image" to be used by the Live-Scan Systems.

No later than 28 calendar days after the delivery order award date, all software configurations and testing must be completed and final acceptance by the government must be received. The Contractor will be required to work on-site with USCIS staff at USCIS Headquarters to solidify the customization of the Live-Scan Application and the operating system images (one for each computing platform). Any time saved on the 28 calendar days will also be added to the 100 calendar day deployment schedule (up to 14 calendar days). After final acceptance of the software customization by the government, an additional 14 calendar days will be required to complete the USCIS image. Once complete, the government will provide the Contractor a copy of the USCIS Image. Once the image is provided to the contractor, the deployment period begins.

All 400 "cabinet" and 100 "desktop" Live-Scan Systems Live-Scan Systems shall be operational at all USCIS locations identified in **Attachment A** no later than 100 calendar days from the start of the deployment period. The contractor shall dispose of all old equipment; deliver and install new Live-Scan equipment, perform operational testing, and provide required training at every USCIS location, listed in **Attachment A**, in order for the systems to be considered operational.

"Mobile" Live-Scan Systems will not require installation and training. The 100 mobile systems shall be delivered to the USCIS Sites as specified in **Attachment A**, except for the laptop/computing devices themselves, which shall be shipped to USCIS Headquarters (111 Massachusetts Ave, Washington D.C. 20001) no later than 100 days from the beginning of the deployment period, where the government will install the USCIS operating system image, application software, and deliver them to the USCIS locations. The government will be responsible for the installation of the 100 "mobile" systems.

The deployment schedule is included as **Attachment D**. The contractor is to provide a written deployment plan immediately following contract award addressing the deployment schedule to include the disposal of old equipment, installation of new equipment, and training of users by USCIS Site. (**Attachment A** identifies the quantity and types of Live-Scan Systems to be installed at each USCIS location)

Operations and Maintenance (O&M) Support provided with the purchased equipment shall commence when all Live-Scan Systems are operational. Any installed systems, prior to all systems being operational, shall be supported by the contractor and any service shall be considered part of the installation. Inside delivery will be required for all shipments and curbside delivery (drop-shipping is not allowed and/or acceptable).

7.1 Shipping

The Live-Scan Systems shall be shipped to arrive at the installation site no sooner than 72hrs prior to installation. Live-Scan Systems shall be shipped as complete systems as opposed to shipping separate components. Live-Scan assembly shall be completed prior to shipment. The operating system and necessary software shall be installed and configured prior to shipment. Shipment dates shall be coordinated with the COTR. Shipping shall be considered FOB Destination and acceptance of the Live-Scan Equipment will occur upon receipt of a G504 Form. Shipping, packaging, and packing materials shall use recycled/recyclable materials to the maximum extent practicable. The Contractor is responsible for removing all shipping, packaging, and packing materials during installation and disposal.

7.2 Milestone Chart

MILESTONE CHART

Milestone	Description	Due Date
-----------	-------------	----------

1	Deliver 2 of each Live-Scan System model to USCIS HQ (111 Massachusetts Ave, Washington DC 20001)	5 business days after award
2	Submit Final Systems Deployment Plan and Final Program Management Plan	5 business days after award
3	Appoint a senior official to act as the Corporate Security Officer Provide the COTR with one central point of contact for all activities related to initial setup and deployment	5 business days after award
4	Successful completion of Test Phases 1-3. Complete Live-Scan Software Customization	28 calendar days after contract award
5	Prospective Contractor employees shall submit completed background investigation forms to OSI through the COTR	No less than 30 days before the starting date of the contract or 30 days prior to entry on duty of any employees (approx 5 days after award)
6	Submit IT Security Plan for approval	Within 30 calendar days after contract award
7	Favorable entry on duty (EOD) determination received Contractor employees shall submit LAN account and GFE request forms	After favorable entry on duty (EOD) determination (approx 35 calendar days after award)
8	Submit MAC Address List	Prior to systems deployment (approx 36 calendar days after award)
9	USCIS Operating System Image completed and distributed to Contractor	42 calendar days after contract award
10	LAN Accounts and GFE received Begin deployment of Live-Scan Systems	43 calendar days after contract award
11	Complete Computer Security Awareness Training (CSAT)	60-days from the date of entry on duty (EOD)
12	All Live-Scan Systems Fully Operational (mobile unit cases and peripherals deployed and laptops sent to USCIS HQ)	143 calendar days after award
13	End of Deployment Phase & Operations and Maintenance Support begins	144 calendar days after award

8.0 Test and Acceptance

The test and acceptance evaluation shall occur in four (4) phases (and will be performed on the 4-6 systems provided immediately following contract award):

Phase 1 - Acceptance of the customization required of the COTS biometrics software application. The test will ensure all necessary data capture fields and corresponding data entry screens have been added in order to process UKvisas and Code 1-3 applicants. Login and password integration (using an LDAP connector to access the Microsoft Active Directory) will also be tested. Phase 1 requires acceptance no later than 28 calendar days after award date. Testing shall be performed at the USCIS ASC Lab (111 Massachusetts Avenue, 2nd floor, Washington D.C. 20001)

Phase 2 - This tests the communication connection between the Live-Scan system and the local store-and-forward mail server. The test must demonstrate that the fingerprint file generated by the Live-Scan is in the format specified by all relevant standards, compliant with ANSI/NIST and FBI specifications, and stored in the proper directory on the local store-and-forward mail server. Processing an USCIS application will test the file format for acceptability. Phase 2 requires acceptance no later than 28 calendar days after award date. Additionally, at time of installation at each USCIS location, this must be reconfirmed in order for each system to be considered operational. Testing shall be performed at the USCIS ASC Lab (111 Massachusetts Avenue, 2nd floor, Washington D.C. 20001).

Phase 3 - This test provides for acceptance of the encrypted file format and external media (such as a DVD-ROM) format by the Government. The file format originates from the Live-Scan systems and is forwarded to the local store-and-forward mail server, which forwards a daily batch to the Government's applicable store-and-forward transaction manager. Data is written to the external media (such as a DVD-ROM) using the same EFTS 7.0 format as the file format. Phase 3 requires acceptance no later than 28 calendar days after award date. Additionally, at time of installation at each USCIS location, this must be reconfirmed in order for each system to be considered operational.

Phase 4 - This tests the communication connection between the Live-Scan system and the ESB. The test must demonstrate that the fingerprint file generated by the Live-Scan is in the format specified by all relevant standards, compliant with ANSI/NIST and FBI EFTS specifications. Processing a USCIS application will test the file format for acceptability. This phase shall be conducted after deployment, and at the discretion of the Government.

9.0 Disposal

For all systems requiring disposal, the Contractor shall:

a. De-install existing Live-Scan systems in coordination with the installation of the new Live-Scan systems per the deployment schedule. Live scan systems at each specific location are to be disposed of in accordance with this SOW.

b. Remove the hard drive component from the CPU of each Live-Scan system and give the hard drive components to the onsite Desktop Support Manager (DSM). If the onsite DSM is

absent, the ASC Manager or Site Supervisor shall suffice. The Contractor is responsible for providing written proof that the DSM, ASC Manager, or Site Supervisor certified in writing that the hard drive components for each specific machine have been removed and placed in custody of a government representative.

c. Dismantle and haul away each complete Live-Scan system and attached components for disposal as scrap.

d. Complete and Sign Form G-504, Report of Property Shipped/Received. The ASC Manager or Site Supervisor will also sign and take possession of the Form G-504 to acknowledge transfer of scrap property to the Contractor representative.

e. Ensure the following information included on and/or attached to the G-504 for each scrap system is correct:

- (1) Live-Scan System Property Control Number (PCN)
- (2) Component PCNs, if applicable
- (3) Live-Scan System Serial Number
- (4) Live-Scan Model Number

f. Remove all DHS PCN Labels from the Live-Scan Equipment and attach them to the back of the G-504. There are typically 3 labels on each Live-Scan system: 1 on the cabinet or computer, 1 on the barcode reader, and 1 on the digital camera.

g. Make all arrangements for transportation and disposal of scrap property, including inside pick-up, truck lift gate, shipping, and payment of disposal facility handling and disposal fees.

h. Ensure that all applicable Environmental Protection Agency (EPA) and state environmental regulations are met in disposing of the scrap property. Components of the scrap equipment contain hazardous materials. Prior to disposal, the Contractor shall obtain written certification and/or other proof from the waste disposal facility that the disposal facility is fully certified for hazardous waste disposal.

i. Following disposal, verify in writing to the ASC Program Contracting Officer Technical Representative (COTR) that the equipment has been disposed of as scrap material through proper waste disposal procedures and facilities in accordance with all applicable government regulations. The Contractor shall provide the information listed in paragraph e, above, to describe the disposed scrap in the scrap disposal verification letter(s).

9.1. Performance of Services: The Contractor shall coordinate the de-installation and removal of scrap Live-Scan systems with the HQ, USCIS ASC Branch and local USCIS ASC/District staff.

9.2. Reselling Prohibition: The Contractor shall not resell any equipment that contains a memory component. Such components shall be disposed of in accordance with MD4300.1.

10.0 Installation

The contractor shall be responsible for all aspects of installation. Installation includes the following activities:

- Install and/or integrate Live-Scan hardware
- Install and/or integrate Live-Scan software, to include the USCIS image (provided by USCIS)
- Install and/or integrate component pieces as required to meet the requirements of this SOW
- Install DHS Property Control Number (PCN) Labels on Live-Scan Systems
- Complete a Form G-504 for the installation at each USCIS site.

The Government is responsible for installation site modifications, if required, to prepare the facility to receive the equipment, to include cabling, wiring, construction, and mail server installation.

The Contractor shall integrate all the hardware and load all necessary software and conduct a complete configuration test sufficient to ensure that the Live-Scan system is fully functional in each USCIS ASC site. The configuration for each ASC Live-Scan system shall be identical. The Contractor shall be responsible for setup and integration of devices. The Contractor shall certify each system as completely operational following installation and integration, in accordance with all terms and conditions of this delivery order.

Installation of the operating system on the fixed-disk drives in its own subdirectory; USCIS will provide the contractor with the USCIS operating system image. The contractor will be responsible for installing the image on each Live-Scan System. The USCIS image (containing the operating system and necessary software) shall be installed and configured prior to installation at a USCIS site.

The Contractor shall, in all cases, be responsible for certification, and delivery of hardware and software not later than the delivery date specified in this delivery order, in accordance with the Schedule. The Contractor shall adequately package Live-Scan systems to prevent shipping damage, make all arrangements for transportation, shipping, insurance, and commercial Bills of Lading, and unpack and install systems at the receiving USCIS fingerprinting locations. Shipping costs shall be included in the price of the Live-Scan systems.

After contract award and prior to deployment, USCIS shall provide the Contractor with approximately 1,800 PCN Labels. While in the care of the Contractor, the Contractor shall be responsible for the PCN labels. The Contractor shall install the PCN labels on the Live-Scan Systems as follows:

Each model ("cabinet", "desktop", and "mobile") shall have a total of 3 PCN Labels:

- 1) One on the cabinet (if applicable) else on the computer
- 2) One on the Barcode Reader

3) One on the Digital Camera

Upon successful Live-Scan System installation at a USCIS site, the Contractor shall complete and Sign Form G-504, Report of Property Shipped/Received. The ASC Manager or Site Supervisor will also sign and take possession of the completed Form G-504 to acknowledge transfer of new property to the Government.

The Contractor shall ensure the following information included on the G-504 for each new system is correct:

- (1) Live-Scan System Property Control Number (PCN)
- (2) Component PCNs, if applicable
- (3) Live-Scan System Serial Number
- (4) Live-Scan Model Number

11.0 On-Site Training

At the time of installation, the Contractor shall conduct on-site training of all USCIS designated Live-Scan operators. The anticipated total number of individuals requiring initial training is approximately 1,000. Training shall be conducted at each ASC site (**Attachment A**). On-site training includes User training and Site Supervisor training. User Manuals and User Systems Administrators Manuals shall be provided at delivery and reviewed/used to facilitate training.

User Training includes the following:

- Operational instruction to identified Live-Scan operators.
- Review and familiarization with User Manual documentation (e.g., manual, video).
- Instruction on the systems' plug and play capabilities.
- Instruction on the setup and disassembly of portable systems.
- Basic instruction on general maintenance such as calibration and system restart.

Site Supervisor Training includes User Training plus the following activities:

- Basic troubleshooting/depot component replacement.
- Train the trainer instruction.
- Review and familiarization with User Manual documentation (e.g., manual, video).
- Instruction on software setup, if applicable.

12.0 Operations and Maintenance (O&M) Support

12.1 Technical Support Services (Hotline)

The Contractor shall provide a system of technical support for all Live-Scan systems delivered by the Contractor. The Contractor shall provide 24/7 hotline support via a single toll-free number in order to support the following hours of operation:

Sunday	Closed
Monday	7 am – 5 pm (local time at each USCIS site as listed in Attachment A)
Tuesday	7 am – 5 pm (local time at each USCIS site as listed in Attachment A)
Wednesday	7 am – 5 pm (local time at each USCIS site as listed in Attachment A)
Thursday	7 am – 5 pm (local time at each USCIS site as listed in Attachment A)
Friday	7 am – 5 pm (local time at each USCIS site as listed in Attachment A)
Saturday	Closed

The USCIS Service Desk will use the hotline to report technical problems for all ASC sites. The Contractor shall provide a telephonic response within one (1) hour, at which time a resolution or plan for resolution will be provided.

The Contractor shall provide the most effective method of providing responsive technical troubleshooting and resolution support, to include VPN remote access support. USCIS will provide VPN connections via the use of USCIS-issued laptops and SecureID tokens.

12.2 Remedial and Preventive Maintenance Services

The Contractor shall be responsible for hardware and software maintenance support for Live-Scan systems provided under this delivery order. The Contractor shall provide all maintenance coverage necessary to meet the requirements of this SOW. The Contractor shall coordinate warranty information and warranty services with the manufacturer of the hardware or software. At a minimum, the Contractor shall provide remedial maintenance coverage. Subject to security policies, regulations and procedures, the Government will permit on-site access to the equipment that is to be maintained.

12.2.1 General Maintenance Requirements

The Contractor shall provide all necessary personnel, materials, parts, tools, diagnostic and test equipment, technical manuals/publications and other services as may be required for the hardware maintenance support.

- Maintenance support shall include technical troubleshooting, problem resolution and component repair or replacement in order to maintain and keep the equipment covered under the order in full operating condition.
- The Contractor shall provide data concerning all maintenance activities. A service incident report (SIR) shall be available to the Government for any maintenance rendered by the Contractor under this delivery order (See Section 13.2.1.4. Responsibilities of the Contractor).

12.2.1.1 Periods of Maintenance

The Principal Period of Maintenance (PPM) and Official Operation Hours for equipment covered under this delivery order is 7 a.m. through 5 p.m., local time for each location as identified in **Attachment A**, Monday through Friday (five (5) days per week), excluding Federal Holidays.

12.2.1.2 Software Maintenance

The Contractor shall remotely load all revised software configurations and table updates down to the individual Live-Scan system from a central location utilizing the USCIS issued laptops and SecureID tokens. Remote access to the individual Live Scan systems can only be accomplished through the SecureID VPN token connections. VPN connections via SecureID tokens is the only means of performing certain types of maintenance to include software and hardware maintenance or system troubleshooting.

12.2.1.3 Hardware Maintenance

1. Preventive Maintenance

Preventive Maintenance is defined as regularly scheduled activities to maintain hardware in full operating condition. The frequency of preventive maintenance shall be at the discretion of the Contractor). The preventative maintenance shall be performed during remedial maintenance calls and/or during a mutually acceptable time during the specified PPM, unless otherwise agreed to by the Contractor and the Government. The Contractor shall provide the Government with a Preventative Maintenance schedule for Government review and approval.

2. Remedial Maintenance

Remedial maintenance is defined as identifying the source of an equipment or software malfunction and either repairing or replacing the malfunctioned component or subsystem. The Contractor shall provide the parts and equipment required for the diagnosis and repair of malfunctioning components of the Live-Scan system at the most cost effective manner available which will also minimize the downtime of the system. Remedial maintenance shall include transportation, labor and parts required for return of a malfunctioning system or equipment to full operating condition.

Repaired and/or replaced parts and labor shall be warranted for the standard 1 year warranty period from the date all systems are operational. If additional calls are required during the warranty period, for the warranted repair, they shall be made at no additional cost to the Government. The contractor shall submit a copy of the Live-Scan warranty in writing to the COTR upon award of the delivery order.

The Contractor's responsibilities for remedial maintenance shall include:

- The administration and management of all warranties associated with the Live-Scan systems.

- Tracking the status and invoking the use of all applicable warranties of the Live-Scan systems.
- Telephonic responses to the originator within 1 hour of trouble call
- When on-site support is not required, the support must be completed within one (1) business day or three (3) business days if the shipping of parts is required.
- When on-site support is required, the support must be completed within three (3) business days for ASCs located within the Contiguous United States.
- When on-site support is required, the support must be completed within four (4) business days for ASCs located in Puerto Rico, U.S. Virgin Islands, and five (5) business days for ASCs located in Hawaii, Guam, Saipan, and Alaska.

Remedial maintenance shall be performed after notification that the system is inoperative (down). The Contractor shall provide USCIS with a designated point of contact and make arrangements to enable its maintenance representative to receive such notification and provide continuous telephone coverage within the PPM to permit USCIS to make such contact (See Section 13.1, Technical Support Services (Hotline)). Within one (1) hour of notification, the Contractor shall provide a telephonic response that assesses the situation, identifies the problem, and proposes the resolution and the time to fix the problem. Resident on-site maintenance at the USCIS sites is not required.

Downtime is that time in which the Contractor maintained equipment is inoperable due to a hardware malfunction. If the failure of one device causes other devices to be inoperable, these other devices may, at the Government's option, be considered down also. A determination of downtime will be made solely by the Government. Downtime for each failure shall start at the time the Government notifies the Contractor of a failure and shall run until the failed equipment is returned to full operating condition.

Types of Coverage Required

The Contractor shall provide all maintenance coverage necessary to meet the requirements of this SOW, to include system performance requirements in SOW Section 14.0. At a minimum, the Contractor must provide remedial hardware maintenance services that meet all maintenance requirements of this SOW.

12.2.1.4 Responsibilities of the Contractor

1. Parts Quality

The Contractor shall use only new standard parts or refurbished parts, certified as equal in performance to new parts by the Original Equipment Manufacturer, in performed repairs. Parts that have been replaced shall become the property of the Contractor. The Contractor shall maintain a replacement parts policy consistent with supporting the performance requirements as stated in this SOW.

2. Protection of Information During Equipment Maintenance

The Contractor shall prevent loss of hard drive information during all maintenance activities by taking steps to protect and, at the Government's option, restore as necessary, any information residing in the equipment being maintained. The Contractor is responsible for the erasing or wiping of information from all hard drives removed or replaced by the Contractor. Hard drives must be wiped under the supervision of the Government Computer Systems Security Officer (CSSO). The Contractor shall be responsible for notifying the Contracting Officers Technical Representative (COTR) or designated representative if a hard drive containing information has been removed from an USCIS facility without erasing the data contained on the hard drive.

3. Remote System Access for Maintenance

A VPN connection via SecureID tokens is the only means of remote system access to perform required hardware maintenance or system troubleshooting.

4. Service Incident Reports (SIRs)

The Contractor shall maintain an electronic database of all SIRs to respond to Government inquiries regarding specific problems and issues. The SIR shall contain at a minimum, the following information:

- (1) Name of person requesting service
- (2) Location, including site code, office, city and state/country
- (3) Phone number of the person requesting service
- (4) Type of equipment
- (5) Serial number and USCIS property control number (PCN) of component being serviced
- (6) Date and time of request for service
- (7) Date and time of arrival of maintenance personnel (if applicable)
- (8) Date and time replacement part shipped (if applicable)
- (9) Description of problem
- (10) Parts replaced (including serial number and PCN if applicable)
- (11) Date and time problem was resolved
- (12) Reason problem not resolved within required timeframe (if applicable)
- (13) Any required follow-up actions
- (14) USCIS ticket number and vendor ticket number
- (15) Name of individual at affected site certifying the repair was completed

13.0 System Performance

The Contractor shall ensure that the Live-Scan systems meet the following availability and reliability requirements:

Live-Scan Systems:

- 95% availability per machine

Availability is defined as a system that is technically operational and supporting the mission of fingerprinting applicants for immigration benefits. The Live-Scan System is "unavailable" if it is unable to support the mission of capturing and transmitting complete applicant biometric data. Availability per machine is calculated as follows: number of business days/year that the machine was available divided by the number of total business days/per year x 100%. A machine is considered unavailable for one day when the machine is unavailable for over 50% of the day's total operational hours.

(Example: $255 / (365 \times (5/7)) \times 100\% = 247/260 \times 100\% = 95\%$)

At the Government's request, the Contractor shall replace systems that do not meet the stated requirements, above, at no cost to the Government.

13.1 Performance Deductions

The USCIS has determined that the Live-Scan equipment provided under this delivery order will perform functions that require assessment of payment deductions if the Contractor fails to correct technical malfunctions within the Government's timeframes specified below.

When on-site support is required, the Contractor shall provide all remedial action necessary to correct technical failures in Live-Scan equipment at USCIS sites within the 48 contiguous United States within three (3) business days of the trouble call, within four (4) business days for ASCs located in Puerto Rico, U.S. Virgin Islands, and five (5) business days for ASCs located in Hawaii, Guam, Saipan, and Alaska. The Contractor shall incur a \$100 invoice deduction per machine per day for each machine that remains down beyond these required timeframes.

When on-site support is not required, the Contractor shall provide all remedial action necessary to correct system issues/failures in Live-Scan equipment within one (1) business day of the trouble call. The Contractor shall incur a \$100 invoice deduction per machine per day for each machine that remains down beyond these required timeframes.

Availability shall be assessed by the COTR on a semi-annual basis. For each Live-Scan System found to be available less than 95% of the total operational time, an invoice deduction (taken in the following month) in the amount of \$100 per machine per day over the 95% threshold shall occur.

The Contractor shall not incur deductions when Acts of God (e.g. weather), Government actions (e.g., denial of facilities access), or other events outside of Contractor control prevent the Contractor from providing remedial action within the required timeframes.

14.0 Written Deliverables/Reports

a) The Contractor shall provide a written Systems Deployment Plan in electronic format to the COTR via email no later than five (5) business days following contract award. The Systems Deployment Plan shall incorporate the deployment schedule (**Attachment D**) and address the disposal of old equipment, installation of new equipment, and training of users by USCIS Site. (**Attachment A** identifies the quantity and types of Live-Scan Systems to be installed at each USCIS location). The Systems Deployment Plan shall be in electronic format and shall not be longer than 30 pages in length.

b) The Contractor shall provide a Program Management Plan in electronic format to the COTR via email no later than five (5) business days following contract award. The Program Management Plan shall address at a minimum, a risk management plan, a communication plan, key personnel (to include résumés), and subcontractor teaming arrangements. The Program Management Plan shall not be longer than 30 pages in length.

c) The Contractor shall provide a monthly utilization report in MS Excel format to the COTR via email no later than ten (10) business days following the end of the month. This report shall detail the number of calls received, time to respond to messages, time of arrival if an on-site maintenance call, technician's name, time to resolve, length of time a machine is "unavailable", type of problem, solution, corresponding USCIS ticket number, corresponding machine's serial number, location of problem, and point of contact.

d) Prior to the commencement of deployment, the contractor shall deliver (to the COTR) via email an updated **Attachment A**, which includes the Media Access Control (MAC) addresses of each Live-Scan System to be installed at each location. The MAC addresses must be provided so that port security settings may be set by USCIS to allow for the installation of the new machines.

e) The Contractor shall provide a preventative maintenance schedule to the COTR in MS Excel format via email no later than ten (10) business days prior to performing preventative maintenance. The schedule shall identify the date of preventative maintenance for each Live-Scan System.

f) The Contractor shall provide a preventative maintenance report to the COTR in MS Excel format via email no later than ten (10) business days following the end of a preventative maintenance cycle. The report shall identify each Live-Scan System by serial number and the corresponding dates when preventative maintenance was performed.

g) The Contractor shall provide a quarterly inventory report to the COTR in MS Excel format via email no later than ten (10) business days following the end of the quarter. During the deployment of the new Live-Scan Systems, the contractor shall provide the report on a weekly-basis. The report shall consist of a list of all system locations, serial numbers, DHS Property Control Numbers (PCN), as well as IP addresses and other network information necessary to maintain the systems on the USCIS Network.

h) In Lieu of submitting individual Service Incident Reports (SIR), the Contractor shall provide a monthly Service Incident Report (SIR) that aggregates the SIRs from the month into

one report. The report shall be delivered to the COTR in MS Excel format via email no later than ten (10) business days following the end of the month.

i) The Contractor shall provide a monthly USCIS Systems Information Report to the COTR in MS Excel format via email no later than ten (10) business days following the end of the month. The report shall contain at a minimum, the following information:

1. ASC Location
2. Type (Stand Alone or Co-Located)
3. ASC Site Code (i.e. X-code)
4. Live-Scan Model
5. Live-Scan System Name
6. IP Address
7. Live-Scan System Serial Number
8. Software Version
9. Software Modified Date
10. Live-Scan System Code
11. Mail Server IP Address
12. Gateway IP Address
13. Subnet Mask
14. Network IP
15. ORI Code

j) The Contractor shall provide a monthly Service Desk Report to the COTR in MS Excel format via email no later than ten (10) business days following the end of the month. The report shall contain at a minimum, the following information:

1. Remedy Ticket Number
2. Service Desk Ticket Number
3. Date Ticket Opened
4. Date Ticket Closed
5. Number of Business Days Ticket was Open
6. System Down (Yes or No)
7. ASC Site Code (i.e. X-code)
8. ASC Site Name
9. Problem Type
10. Summary (i.e. description of problem)
11. Status (Open or Closed)

k) The Contractor shall reconcile the USCIS Remedy Monthly Report, provided to the Contractor by USCIS, with the monthly Service Desk Report on a monthly-basis and submit to the COTR via email within ten (10) business days following the receipt of the USCIS Remedy Report. The USCIS Remedy Monthly Report contains the following data:

1. Remedy Ticket Number
2. ASC Site Code (i.e. X-Code)

3. ASC Location
4. Date Ticket was Opened
5. Issue/Problem
6. Ticket Assignment (miss assigned or not)
7. Status (Open or Closed)

14.1 Written Deliverables Schedule

WRITTEN DELIVERABLES SCHEDULE

Deliverable	Due Date	Format
Systems Deployment Plan	5 business days after award	Electronic
Program Management Plan	5 business days after award	Electronic
Monthly Utilization Report	10 business days following the end of the month	MS Excel
MAC Address List	Prior to Deployment	MS Excel
Preventative Maintenance Schedule	10 business days prior to performing preventative maintenance	MS Excel
Preventative Maintenance Report	10 business days following the end of the month	MS Excel
Quarterly Inventory Report	10 business days following the end of the quarter (weekly-basis during deployment)	MS Excel
Service Incident Report	10 business days following the end of the month	MS Excel
Systems Information Report	10 business days following the end of the month	MS Excel
Monthly Service Desk Report	10 business days following the end of the month	MS Excel
Reconciled USCIS Remedy Monthly Report	10 business days following receipt of Remedy Report	MS Excel

15.0 Government Furnished Equipment (GFE)

Upon contract award and after the issuance of proper EOD clearances, the government shall provide a maximum of five (5) USCIS Laptops and five (5) SecureID VPN Tokens to the Contractor. A laptop and a VPN token each must be assigned to a single individual. The laptops and VPN tokens may only be distributed upon successful completion of the security clearance paperwork (see section 18.0 Security Requirements) resulting in a favorable Entry On Duty (EOD) determination. Additionally, the Contractor shall submit the following forms for each individual prior to attainment/use of the GFE:

- Information Technology Service Request (ITSR) Form

- USCIS HQ LAN Account Request Form
- A New Laptop User Registration Form
- USCIS VPN Request Form
- G504 Property Receiving and Acceptance Form

16.0 Electronic and Information Technology Accessibility

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 EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable 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, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then “1194.21 Software” standards also apply to fulfill functional performance criteria.

36 CFR 1194.23 – Telecommunications Products, 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, 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 is through the use of a Web or Software application interface having 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.

36 CFR 1194.26 – Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) 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 DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

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 meets 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 of 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.

17.0 Facility Access Control

The Contractor shall observe all internal building security regulations that apply to any and all buildings concerned with this contract. The Contractor shall only enter the facility or building with continuous escort service. When entering and departing the facility or building each Contractor must sign in and out as required at the site.

Equipment and Materials Dismantling, Handling, and/or Hauling: The Contractor shall coordinate the route of moving equipment and materials within the facility before dismantling, handling and/or hauling same with the COTR or authorized Government representative. The Contractor shall notify the COTR or authorized Government representative to reach a mutually acceptable time and date corrective action will be completed for work required in response to an emergency or urgent service call within the response time specified herein. The Government reserves the right to inspect the equipment before, during and after any work performed.

Temporary Outages: The Contractor shall coordinate all temporary outages of any equipment with the COTR/authorized representative not less than 72 hours in advance of such outages.

18.0 Security Requirements

Prior to the commencement of work, the Contractor shall ensure that all personnel involved in the operations and maintenance service, and related work thereof, meet the security requirements identified in this SOW.

SECURITY REQUIREMENTS

GENERAL

U.S. Citizenship & Immigration Services (USCIS) has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to sensitive but unclassified information, and that the Contractor will adhere to the following.

SUITABILITY DETERMINATION

USCIS shall have and exercise full control over granting, denying, withholding or terminating access to government facilities and/or access of Contractor employees to sensitive but unclassified information, based upon the results of a background investigation. USCIS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by USCIS, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a USCIS facility without a favorable EOD decision or suitability determination by the Office of Security and Integrity (OSI).

BACKGROUND INVESTIGATIONS

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information, shall undergo a position sensitivity analysis based on the duties, outlined in the Position Designation Determination (PDD) for Contractor Personnel, each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI. Prospective Contractor employees shall submit the following completed forms to OSI through the COTR no less than 10 days after award of delivery order or 30 days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1. Standard Form 85P, "Questionnaire for Public Trust Positions"
2. DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement"
3. FD Form 258, "Fingerprint Card" (2 copies)
4. Form DHS-11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
5. Position Designation Determination for Contract Personnel Form
6. Foreign National Relatives or Associates Statement

Required forms will be provided by USCIS at the time of award of the contract. Only complete packages will be accepted by OSI. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive but unclassified information has resided in the US for three of the past five years, OSI may not be able to complete a satisfactory background investigation. In such cases, USCIS retains the right to deem an applicant as ineligible due to insufficient background information.

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to or development of any DHS IT system. USCIS will consider only U.S. Citizens for employment on this contract. USCIS will not approve LPRs for employment on this contract in any position that requires the LPR to access or assist in the development, operation, management or maintenance of DHS IT systems. By signing this contract, the contractor agrees to this restriction. In those instances where other non-IT requirements contained in the contract can be met by using LPRs, those requirements shall be clearly described.

EMPLOYMENT ELIGIBILITY

The Contractor must agree that each employee working on this contract will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall

be responsible to USCIS for acts and omissions of his own employees and for any Subcontractor(s) and their employees to include financial responsibility for all damage or injury to persons or property resulting from the acts or omissions of the contractor's employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or with this contract. The Contractor will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the COTR will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

USCIS reserves the right and prerogative to deny and/ or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom USCIS determines to present a risk of compromising sensitive but unclassified information to which he or she would have access under this contract.

The Contractor will report any adverse information coming to their attention concerning contract employees under the contract to USCIS OSI. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employees' name and social security number, along with the adverse information being reported.

OSI must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and building passes, or those of terminated employees to the COTR. If an identification card or building pass is not available to be returned, a report must be submitted to the COTR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card.

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OSI through the COTR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COTR and OSI shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COTR determine that the Contractor is not complying with the security requirements of this delivery order, the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

COMPUTER AND TELECOMMUNICATIONS SECURITY REQUIREMENTS

Security Program Background

The DHS has established a department wide IT security program based on the following Executive Orders (EO), public laws, and national policy:

- Public Law 107-296, Homeland Security Act of 2002.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Executive Order 12829, *National Industrial Security Program*, January 6, 1993.
- Executive Order 12958, *Classified National Security Information*, as amended.
- Executive Order 12968, *Access to Classified Information*, August 2, 1995.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001.
- National Industrial Security Program Operating Manual (NISPOM), February 2001.
- DHS Sensitive Systems Policy Publication 4300A v2.1, July 26, 2004
- DHS National Security Systems Policy Publication 4300B v2.1, July 26, 2004
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*.
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems (U)*, July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.
- Title 36 Code of Federal Regulations 1236, *Management of Vital Records*, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

GENERAL

Due to the sensitive nature of USCIS information, the contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security Program to address the

integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The contractor's security program shall adhere to the requirements set forth in the DHS Management Directive 4300 IT Systems Security Pub Volume I Part A and DHS Management Directive 4300 IT Systems Security Pub Volume I Part B. This shall include conformance with the DHS Sensitive Systems Handbook, DHS Management Directive 11042 Safeguarding Sensitive but Unclassified (For Official Use Only) Information and other DHS or USCIS guidelines and directives regarding information security requirements. The contractor shall establish a working relationship with the USCIS IT Security Office, headed by the Information Systems Security Program Manager (ISSM).

IT SYSTEMS SECURITY

In accordance with DHS Management Directive 4300.1 "Information Technology Systems Security", USCIS Contractors shall ensure that all employees with access to USCIS IT Systems are in compliance with the requirement of this Management Directive. Specifically, all contractor employees with access to USCIS IT Systems meet the requirement for successfully completing the annual "Computer Security Awareness Training (CSAT)." All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter.

CSAT can be accessed at the following: <http://otcd.uscis.dhs.gov/EDvantage.Default.asp> or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

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

SECURITY REVIEW

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 organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. 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 data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

The USCIS SDLC Manual documents all system activities required for the development, operation, and disposition of IT security systems. Required systems analysis, deliverables, and security activities are identified in the SDLC manual by lifecycle phase. The contractor shall assist the appropriate USCIS ISSO with development and completion of all SDLC activities and deliverables contained in the SDLC. The SDLC is supplemented with information from DHS

and USCIS Policies and procedures as well as the National Institute of Standards Special Procedures related to computer security and FISMA compliance. These activities include development of the following documents:

- *Sensitive System Security Plan (SSSP)*: This is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures. The SSSP shall be based upon the completion of the DHS FIPS 199 workbook to categorize the system of application and completion of the RMS Questionnaire. The SSSP shall be completed as part of the System or Release Definition Process in the SDLC and shall not be waived or tailored.
- *Privacy Impact Assessment (PIA) and System of Records Notification (SORN)*. For each new development activity, each incremental system update, or system recertification, a PIA and SORN shall be evaluated. If the system (or modification) triggers a PIA the contractor shall support the development of PIA and SORN as required. The Privacy Act of 1974 requires the PIA and shall be part of the SDLC process performed at either System or Release Definition.
- *Contingency Plan (CP)*: This plan describes the steps to be taken to ensure that an automated system or facility can be recovered from service disruptions in the event of emergencies and/or disasters. The Contractor shall support annual contingency plan testing and shall provide a Contingency Plan Test Results Report.
- *Security Test and Evaluation (ST&E)*: This document evaluates each security control and countermeasure to verify operation in the manner intended. Test parameters are established based on results of the RA. An ST&E shall be conducted for each Major Application and each General Support System as part of the certification process. The Contractor shall support this process.
- *Risk Assessment (RA)*: This document identifies threats and vulnerabilities, assesses the impacts of the threats, evaluates in-place countermeasures, and identifies additional countermeasures necessary to ensure an acceptable level of security. The RA shall be completed after completing the NIST 800-53 evaluation, Contingency Plan Testing, and the ST&E. Identified weakness shall be documented in a Plan of Action and Milestone (POA&M) in the USCIS Trusted Agent FISMA (TAF) tool. Each POA&M entry shall identify the cost of mitigating the weakness and the schedule for mitigating the weakness, as well as a POC for the mitigation efforts.
- *Certification and Accreditation (C&A)*: This program establishes the extent to which a particular design and implementation of an automated system and the facilities housing that system meet a specified set of security requirements, based on the RA of security features and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation). As appropriate the Contractor shall be granted access to the USCIS TAF and Risk Management System (RMS) tools to support C&A and its annual assessment requirements. Annual assessment activities shall include completion of the NIST 800-26 Self Assessment in TAF, annual review of user accounts, and annual review of the FIPS categorization. C&A status shall be reviewed for each incremental system update and a new full C&A process completed when a major system revision is anticipated.

**SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION
TECHNOLOGY RESOURCES**

(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 5.5, September 30, 2007) 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.

CONTRACTOR EMPLOYEE ACCESS

(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 SSI," 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, and 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, sensitive information, or resources.

(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 ASSURANCES

DHS Management Directives 4300 requires compliance with standards set forth by NIST, for evaluating computer systems used for processing SBU information. The Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards and applicable legislation and regulatory requirements. Systems shall offer the following visible security features:

- *User Identification and Authentication (I&A)* – I&A is the process of telling a system the identity of a subject (for example, a user) (*I*) and providing that the subject is who it claims to be (*A*). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All USCIS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the USCIS standard system in use at the time of a systems development.
- *Discretionary Access Control (DAC)* – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- *Object Reuse* – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- *Audit* – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the USCIS IT

Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.

- *Banner Pages* – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

DATA SECURITY

SBU systems shall be protected from unauthorized access, modification, and denial of service. The Contractor shall ensure that all aspects of data security requirements (i.e., confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the DHS Sensitive Systems Handbook and USCIS policies and procedures. These requirements include:

- *Integrity* – The computer systems used for processing SBU shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated by either the sender or the receiver of the information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.
- *Confidentiality* – Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis and vulnerability assessment shall be performed to determine if threats to the SBU exist. If it exists, data encryption shall be used to mitigate such threats.
- *Availability* – Controls shall be included to ensure that the system is continuously working and all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.
- *Data Labeling* – The contractor shall ensure that documents and media are labeled consistent with the DHS *Sensitive Systems Handbook*.

19.0 Homeland Security Enterprise Architecture (HLS EA) Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as it relates to this Statement of Work. Specifically, the Contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware or software shall be compliant with the HLS EA Technology Reference Model (TRM) Standards and Products Profile.
- 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.

The Contractor shall provide, the full range of business and technical management services that assist in the development and implementation, of IT products and services that are compliant with the USCIS Enterprise Architecture, as well as the DHS Enterprise Architecture policies, procedures, guidelines, and directives (e.g., EA reference models, Investment Review Process).

All IT products and services provided by the Contractor shall be subject to EA governance oversight performed by USCIS Office of Information Technology (OIT).

The contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirement:

- In compliance with OMB mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

20.0 List of Attachments

Attachment A – List of Existing Live-Scan Systems for Disposal and New Equipment for Installation, by USCIS Location

Attachment B – ASC Store and Forward Configurations

Attachment C – Biometrics Capture Flow Chart

Attachment D – Live-Scan Deployment Schedule

Attachment E – UKvisas Software Requirements

Attachment F – FBI Appendix F

Additional Delivery Order Terms and Conditions

52.252-2 Clauses Incorporated by Reference. (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address (es): <http://www.acquisition.gov/far>

(End of clause)

52.217-9 Option to Extend the Term of the Contract (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 3 years.

(End of clause)

52.251-1 Government Supply Sources (APR 1984)

The Contracting Officer may issue the Contractor an authorization to use Government supply sources in the performance of this contract. Title to all property acquired by the Contractor under such an authorization shall vest in the Government unless otherwise specified in the contract. Such property shall not be considered to be "Government-furnished property," as distinguished from "Government property." The provisions of the clause entitled "Government Property," except its paragraphs (a) and (b), shall apply to all property acquired under such authorization.

(End of clause)

Homeland Security Acquisition Regulation (HSAR) clauses and provisions incorporated by reference.

FAR clause 52.252-2, this contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of HSAR clauses may be accessed electronically at this internet address:

http://www.dhs.gov/xlibrary/assets/opnbiz/cpo_hsar_finalrule.pdf

3052.242-71 Dissemination of Contract Information (DEC 2003)

3052.242-72 Contracting officer's technical representative (DEC 2003)

Homeland Security Acquisition Regulation Clauses & Provisions in Full Text

3052.204-71, 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 SSI," 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, and 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, sensitive information, or resources.

(End of clause)

Performance Reporting

For active contracts valued in excess of simplified acquisition threshold, the Federal Acquisition Regulation (FAR) 42.1502 requires federal agencies to prepare Contractor performance evaluations. Performance evaluations are completed and forwarded to the Contractor for review within thirty (30) calendar days from the time the work under the contract is completed for each contract year. Interim evaluations by the Contracting Officer may be completed as necessary. The Contractor has thirty (30) days to reply with comments, rebutting statements, or additional information that will be made part of the official record.

Invoicing Requirements

The Statement of Work contains the invoicing requirement instructions. The invoice shall be sent via e-mail to the USCIS COTR and the USCIS Contracting Officer. The payment office address is as follows:

Dallas Finance Center
PO Box 561547
Dallas, TX 75356-1547

Advertisements, Publicizing Awards & News Releases

All Press releases or announcements about agency programs, projects, and contract awards need to be cleared by the Program Office and the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity news release or

commercial advertising without first obtaining explicit written consent to do so from the Program Office and the Contracting officer.

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

Organizational Conflict of Interest

(a) The Contractor warrants that, to the best of the Contractor's knowledge and belief, there are no relevant facts or circumstances which could give rise to an organizational conflict of interest, as defined in FAR Subpart 9.5, or that the Contractor has disclosed all such relevant information.

(b) Prior to commencement of any work, the Contractor agrees to notify the CO immediately that to the best of its knowledge and belief, no actual or potential conflict of interest exists or to identify to the CO any actual or potential conflict of interest the firm may have. In emergency situations, however, work may begin but notification shall be made within five (5) working days.

(c) The Contractor agrees that if an actual or potential organizational conflict of interest is identified during performance, the Contractor shall immediately make a full disclosure in writing to the CO. This disclosure shall include a description of actions which the Contractor has taken or proposes to take, after consultation with the CO, to avoid, mitigate, or neutralize the actual or potential conflict of interest. The Contractor shall continue performance until notified by the CO of any contrary action to be taken.

(d) Remedies – USCIS may terminate this contract for convenience, in whole or in part, if it deems such termination necessary to avoid organizational conflict of interest. If the Contractor was aware of a potential organizational conflict of interest prior to award or discovered an actual or potential conflict after award and did not disclose it or misrepresented relevant information to the CO, the Government may terminate the contract for default, debar the Contractor from Government contracting, or pursue such other remedies as may be permitted by law or this contract.

Contractor Employee Suitability Determinations

In accordance with the Security Requirements contained the Statement of Work, employees requiring USCIS Information System access for installation of images or system configuration require Suitability Determinations. The Security Requirement section of the SOW details the requirements of the Suitability Determinations. **To expedite processing of appropriate suitability documentation, contractor is required to submit documentation within 10 calendar days of award.**

52.211-6 Brand Name or Equal (AUG 1999)

(a) If an item in this solicitation is identified as "brand name or equal," the purchase description reflects the characteristics and level of quality that will satisfy the Government's needs. The salient physical, functional, or performance characteristics that "equal" products must meet are specified in the solicitation.

(b) To be considered for award, offers of "equal" products, including "equal" products of the brand name manufacturer, must—

(1) Meet the salient physical, functional, or performance characteristic specified in this solicitation;

(2) Clearly identify the item by—

(i) Brand name, if any; and

(ii) Make or model number;

(3) Include descriptive literature such as illustrations, drawings, or a clear reference to previously furnished descriptive data or information available to the Contracting Officer; and

(4) Clearly describe any modifications the offeror plans to make in a product to make it conform to the solicitation requirements. Mark any descriptive material to clearly show the modifications.

(c) The Contracting Officer will evaluate "equal" products on the basis of information furnished by the offeror or identified in the offer and reasonably available to the Contracting Officer. The Contracting Officer is not responsible for locating or obtaining any information not identified in the offer.

(d) Unless the offeror clearly indicates in its offer that the product being offered is an "equal" product, the offeror shall provide the brand name product referenced in the solicitation.

(End of provision)

3052.209-70 Prohibition on Contracts with Corporate Expatriates (JUN 2006)

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting 'more than 50 percent' for 'at least 80 percent' each place it appears.

Foreign Incorporated Entity means any entity which is, or but for subsection (b) of Section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

Inverted Domestic Corporation. A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) *Certain Stock Disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) stock of such entity which is sold in a public offering related to the acquisition described in subsection (b)(1) of Section 835 of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) *Plan Deemed In Certain Cases.* If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) *Certain Transfers Disregarded.* The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) *Special Rule For Related Partnerships.* For purposes of applying Section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

- (i) warrants;
- (ii) options;
- (iii) contracts to acquire stock;
- (iv) convertible debt instruments; and
- (v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.

(f) *Disclosure.* The Vendor under this quotation represents that [Check one]:

___ it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.104-70 through 3009.104-73;

___ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.104-70 through 3009.104-73, but it has submitted a request for waiver pursuant to 3009.104-74, which has not been denied; or

___ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.104-70 through 3009.104-73, but it plans to submit a request for waiver pursuant to 3009.104-74.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of provision)

Instructions for Offerors

1. The Department of Homeland Security, U.S. Citizenship & Immigration Services (USCIS) is considering issuing a Delivery Order against one of the current DHS FirstSource contracts. The purpose of this delivery order is to obtain Biometric (Live-Scan) Equipment to refresh approximately 134 USCIS locations.

2. All offers shall be received at the office below by the date and time specified in Block 10 of the SF-18 (RFQ). All offers shall include the signed SF-18, acknowledgement of Amendments, if applicable, filled out and signed Offeror's response to provision 3052.209-70. All submissions shall have the name and address of the Offeror along with the Solicitation Number.

Submit one original electronic version (must be Section 508 compliant) of the offerors submission, to:

steven.putnam@dhs.gov and Kristie.Nestle@dhs.gov

All offeror's submission must be received at email addresses above by the date and time specified in Block 10 of the SF-18 to be considered on time.

NO FAXED QUOTATIONS WILL BE ACCEPTED.

4. Prospective Offeror's Questions:

Questions concerning the solicitation shall be submitted via e-mail to Steven Putnam , steven.putnam@dhs.gov and Kristie Nestle, kristie.nestle@dhs.gov, or by fax to (802) 951-6455, ATTN: Steven Putnam and must be received no later than **4:00 pm (EST) 20 October 2009** to allow a reply to be provided in a timely manner before quotation response are due. In order to ensure traceability for questions, Offerors shall cite the section, paragraph, and page numbers.

NO TELEPHONIC INQUIRES WILL BE ACCEPTED.

5. General Quotation Preparation Instructions:

Quotation submissions will be a combination of electronic written narrative and oral demonstration/presentation.

Quotation Limitations: The contents of the volumes shall be within the required page limits specified in the table below. Page limitations shall be treated as maximums. **IF PAGE LIMITATIONS ARE EXCEEDED, THE QUOTATION WILL BE REJECTED.**

The contents of the volumes shall be within the required page limits specified in the table below. Page limitations shall be treated as maximums.

- Proposals must be submitted using Microsoft Office 2000 including Word (.DOC), Excel (.XLS), and PowerPoint (PPT or PPS). Disable all macros on all files.
- Submissions must be legible, single-spaced, computer-printed copy (**on one side only**).
- Except for the reproduced sections of the solicitation document, the text font will be

- Times New Roman and text size no less than 10-point proportional.
- Page size shall be 8.5 by 11.0 inches.
 - Foldouts are not allowed.
 - Elaborate brochures or documentation, binding, detailed artwork, or other embellishments are not allowed.
 - Tracking, kerning, and leading values shall not be changed from the default values of the word processing or page layout software.
 - Use at least 1-inch margins from the page edge to the main text on the top and bottom and ¾ inch side margins.
 - Tables, charts, graphs, appendices, and attachments may be used wherever practical. These pages will be included as part of the page limitation. They should be used to illustrate items such as organization structures, systems and layout, implementation schedules, or plans. These displays shall be uncomplicated, legible and shall not exceed 8.5 by 11.0 inches.

QUOTATION SUBMISSION ORGANIZATION AND PAGE LIMITS

TITLE	PAGE LIMIT
Volume I – Part 1, Technical Response (Written) <ul style="list-style-type: none"> - Project Management/Approach - Deployment Plan - Operations & Maintenance Plan - Vendor Compliance Checklist (Appendix A) - Part 2, Part Performance Information 	Volume I shall not exceed 30 pages in length; Vendor Compliance Checklist is not included in Volume 1 Page Count Past Performance 10 Pages Max.
Volume II – Price Quotation <ul style="list-style-type: none"> - Business Information - Pricing Basis - Assumptions and Constraints (if any) 	No Page Limit

Quotation Submission Organization

The submission shall be organized in two separate volumes. One volume will contain the technical response and past performance. In addition, the contractor will be required to present and demonstrate its proposed solution for evaluation to determine if its solution acceptably meets the requirements of the Statement of Work and the contents of the RFQ. The second volume will contain the Price Proposal.

(1) Volume I - Technical Response (Part 1)

a. The contractor will be required to provide a written narrative detailing its proposed solution to accomplish the requirements of the Statement of Work. The technical response must address the following to determine acceptability of the contractor's proposed solution:

1. Project Management/Approach. The contractor will be required to demonstrate its ability to accomplish the requirements of the SOW to determine acceptability of its proposed project management/approach and level of empowerment provided to Program Manager for accomplishing the requirements of the Statement of Work. The contractor shall submit a draft Program Management Plan to include a risk management plan and communication plan. The plan should also address at a minimum, key personnel (to include résumés), and subcontractor teaming arrangements.

2. Deployment Plan. The contractor will be required to provide a Deployment Plan that describes its solution to accomplish the deployment schedule contained in the Statement of Work, to determine if its plan acceptably meets the requirements of the Statement of Work. Specifically, the deployment plan shall address the Contractor's methodology and ability to meet the deployment schedule, dispose of old equipment, install new equipment, and train Live-Scan system operators.

3. Operations and Maintenance Support Plan. The contractor will be required to demonstrate its ability to accomplish the requirements in section 12.0 of the SOW (Operations and Maintenance Support) and to determine acceptability of its proposed approach. The Contractor shall submit an O&M Plan to include the methodology used to support the 600 Live-Scan Systems in 134 Application Support Centers (ASC); specifically addressing: the method of getting new parts/components to the site, removal of defective parts/components, level of hotline and phone support, number of support personnel, locations of support personnel, getting personnel to the ASC sites when on-site support is required, response times, technical support services, preventative maintenance, remedial maintenance, periods of maintenance, software and hardware maintenance, parts quality, protection of information during equipment maintenance, and remote system access for maintenance.

4. Vendor Compliance Checklist - Appendix A. Contractor must complete the Vendor Compliance Checklist, Appendix A and submit with RFQ Response. RFQ Responses received without the completed Vendor Compliance Checklist - Appendix A will be rejected.

b. Oral Demonstration/Presentation. The contractor will be required to present and demonstrate its proposed solution for evaluation to determine if its solution acceptably meets the requirements of the Statement of Work and the contents of the

RFQ. The government will establish the demonstration date and time via a random draw of all contractors' quotations found to be compliant with the Request for Quotation.

- Location of Oral Demonstration/Presentation. The Oral Demonstration/Presentation will be held at HQ USCIS, 111 Massachusetts Ave, NW, Washington, DC. Detailed directions and instructions will be provided to each offeror with the oral presentation schedule.
- Oral Demonstration/Presentation Limitations. Offerors shall make their oral demonstration/presentation in person to the Technical Evaluation Committee. Submissions of video tapes or other forms of media containing the presentation for evaluation are not authorized and such technical proposals shall be rejected.
- Each offeror will have a maximum of one hour (60) minutes to setup for demonstration/presentation and a maximum of one hour (60) minutes of demonstration/presentation time in which to make its presentation to the TEC. The presentation will then recess for up to one hour. Following the recess, the Government may request clarification of any points addressed which are unclear and may ask for elaboration by the Offeror of any point which has not been adequately supported. Any such interchange between the Offeror and the Government will be for clarification only, and will not constitute discussions within the meaning of FAR 15.306.
- The Government shall make an audio/video recording of the oral demonstration/presentation, to include any requests for clarification. Such recordings will be used by the TEC during evaluation of the technical proposal. The recording shall start with the TEC's direction to begin. It will stop when the Offeror ends its' presentation or after one hour, which ever is less. It will restart when the Government starts the clarification portion and end when the Government is finished requesting clarification or after one hour, which ever is less. A copy of the recording will be provided to the Offeror.
- At the close of the demonstration/presentation, the offeror shall provide the TEC with a listing of the names, firms, and position titles of all presenters. The Government will not accept for evaluation any additional documentation, which may or may not have been referred to in the demonstration/presentation.
- Schedule for Presentation. Presentations will be scheduled with offerors as soon as possible after the closing date for the receipt of quotations. The presentations will be scheduled as tightly as possible.

The order in which offerors will make their demonstration/presentation to the TEC will be determined by a lottery conducted by the contracting officer after receipt of the quotations. Once notified of their scheduled demonstration/presentation date and time, offerors shall present their presentations in person on the scheduled date and time. Requests for offerors to reschedule their demonstration/presentation will not be entertained and no rescheduling of demonstration/presentation will be done unless determined necessary by the Government at the contracting officer's sole discretion, to resolve unanticipated problems or delays encountered in the demonstration/presentation process.

- Pricing Information. No price information shall be included in the oral demonstration/presentation.
- Offeror's Presentation Team. The Offeror's presentation team is limited to a maximum of five individuals. Only members of the offeror's or subcontractor's in-house staff shall participate in the presentation. The only exception is that any individuals who are proposed to perform or the contract, such as the Project Manager, but who are not currently employed by the offeror or subcontractor, may participate in the presentation. For any portion of the work to be subcontracted, members of the subcontractor's staff will make that portion of the presentation.

Part 2 - Past Performance Information: The Offerors will provide past performance data with the proposal. The Offeror shall provide a list of customer contact information for not less than three (3) but not more than five (5) projects performed within the last three (3) years. The Vendor shall present the following information:

- Customer Name and Address
- Contract Number/Contract Title
- Delivery Schedule/Period of Performance
- Contract Value
- Description of Work Performed and How it Impacts on the Offeror's Ability to Meet the Requirement of the Solicitation
- Customer point of contact (name, telephone number and e-mail address)
 - Business Manager
 - Technical Manager

This list and the information it contains shall not exceed ten (10) pages.

(2) Volume II – Price Quotation

- a. The Price Quotation shall be submitted in an original electronic version (must be Section 508 compliant) by the date and time specified in the RFQ.
- b. The Offeror shall prepare a Price Quotation that contains all information necessary to allow for a comprehensive evaluation. The Price Quotation shall be structured as follows and contain the following information:

1. **Part 1 - Cover Letter shall include:**

- Solicitation Number
- Name and address of Offeror
- Name and Point of Contact telephone number, fax number and email address (primary POC for this quotation)
- DHS FirstSource Contract Number
- Date of submission
- Name, title, and signature of the Contractor's authorized representative (signature authority)
- Offeror's Data Universal Numbering System (DUNS) and Taxpayer Identification Number (TIN)

2. **Part 2 – Pricing Information:**

- Provide fixed unit pricing for all CLINs contained in Block 11 of the SF-18, Schedule of Services and Supplies. **The fixed unit price shall be inclusive of all associated costs (labor; travel, installation and training, etc.) required to perform the requirements of the Statement of Work.**
- Provide pricing data and assumptions utilized to derive the fixed unit price. The pricing data and assumptions should contain the labor categories, number of labor hours and the labor rates for each labor category proposed and details outlining other direct costs necessary during the performance of tasks contained in the Performance Work Statement.

Quotation Evaluation

The Government will make a **single** firm-fixed priced delivery order award resulting from this solicitation to the responsible offeror whose offer conforms to the solicitation and proposes the lowest evaluated total price for all line items, including options, combined.

The price will be evaluated on the basis of total estimated price of the line items combined. The Offeror's price quote shall be in accordance with their DHS FirstSource IDIQ contract, which has previously been determined fair and reasonable.

Basis for Award

This procurement is for commercial of the shelf (COTS) products and will be awarded to the offeror submitting the lowest price technically acceptable quote for all CLIN's listed. Technical compliance/acceptability is determined by the evaluation criteria stated above, oral demonstration/presentation and an acceptable record of past performance. USCIS requests Offerors to offer their best discounted pricing from established DHS FirstSource contract prices.

Brand Name or equal

This procurement contains brand name or equal products. See the FAR provision 52.211-6, Brand Name or Equal for the instructions to contractors if other than the brand named products are to be included in your quotation submission. Be reminded, if the instructions of FAR 51.211-6 are not complied with, your quotation will be rejected.

Appendix A**Vendor Compliance Checklist**

COMPLETED FORM MUST BE SUBMITTED WITH RFQ RESPONSE

	Requirement	Yes	No
	FD-258 Ten-Print Capture Requirements		
1	All Live-Scan systems and components delivered by the Contractor shall be capable of transmitting FBI NIST/EFTS images to a local store-and-forward server.		
2	Live-Scan systems and components provided under this contract shall be FBI certified to comply with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) Image Quality Specifications (IQS) (See Appendix F) and the US-VISIT IDENT System.		
3	Shall process a minimum of six (6) ten-print applicants per hour (i.e., total time for a skilled fingerprint technician to process one FD-258 applicant shall be 10 minutes or less). The process begins when the Live-Scan system scans the 2D bar code with its scanner, entering FD-258 biographic and demographic masthead data, and ends with the submission of the record to the local store-and-forward mail server.		
4	Shall create an EFTS transaction containing 14 fingerprint images and biographic masthead data		
5	The applicant data files transmitted by the Live-Scan system to the local store-and-forward mail server shall include: (a) biographic and site operations text data, and (b) Wavelet Scalar Quantization (WSQ) compressed fingerprint images (14 blocks) corresponding to fingerprint boxes on the applicant fingerprint card.		
6	The image sizes shall be consistent with the fingerprint boxes on the standard FD-258 fingerprint card.		
7	The transmitted fingerprint images shall be in compliance with ANSI/NIST Standards identified in the attached FBI Appendix F.		
8	The compression algorithms used in the Live-Scan system for compressing the fingerprint images must comply with FBI approved WSQ gray scale compression standards.		
9	Each compressed fingerprint image shall be stored in a separate file.		
10	Shall support EFTS v7.0 specifications for maximum sizes of fingerprint images (provided in Table C-2)		
11	Shall support transmission of an EFTS v7.0 file format fingerprint image to the local store-and-forward mail server. Attachment B lists typical USCIS server configurations. All the data files shall be transferred to a specified directory on the mail server. All the data files transmitted by the Live-Scan systems shall comply with all applicable FBI, ANSI/NIST and NIST/EFTS standards for the data interchange.		
12	Shall have the capability to support transmission of an EBTS 8.001 XML file format to the USCIS Enterprise Bus.		
13	Shall meet the basic format requirements for Logical Record types as defined by the EBTS message set forth in the ANSI standards which are also applicable to transmissions to the FBI.		

14	Shall create an alpha/numeric identification number in a specified FD-258 field in the event that the applicant does not have either an A-number or a social security number. The alpha/numeric identification number will consist of a unique applicant identifier appended with a 12-digit date and time stamp in the format CCYYMMDDHHMM. The unique applicant identifier may be a "Z number", which is a 10-digit number generated randomly by the Live-Scan device, an "F number", which is a manually entered number with F in the first position followed by nine numeric numbers, or another unique number specified by USCIS.		
15	Shall store and transmit a unique site code on each submission in a FD-258 field specified by USCIS.		
16	Shall read both 1D and 2D bar codes.		
17	Shall capture information used for quality control (QC) checks (user ID of the QC checker).		
18	Shall have the capacity to store a minimum of 500 ten-print fingerprint records in each machine and 500 biometric records.		
	Requirements for Other Biometrics Capture		
19	Shall process a minimum of six (6) non-tenprint applicants per hour (i.e., total time for a skilled technician to process one applicant shall be 10 minutes or less.) The process begins when the Live-Scan system scans the 2D bar code with its scanner, entering biographic and demographic data, captures a single press fingerprint image, a digital signature, and a digital facial photograph, and ends with the submission of the record to the local store-and-forward mail server.		
20	Shall allow specified biographic data fields to be entered through the use of 1D and 2D bar code scanners/light pens.		
21	Shall allow the single press-print image and/or digital signature capture to be optional.		
22	Shall require the digital photograph capture of a single facial photo per record for applicants whose press print, photo and signature are captured.		
23	Facial photographic images shall be transmitted using compression algorithms that conform to the standards approved and comply with the latest ANSI/NIST Standards identified in the FBI Appendix F.		
24	The applicant data files transmitted by the Live-Scan system to the local store-and-forward mail server shall include: (a) demographic and site operations data (b) Wavelet Scalar Quantization (WSQ) compressed fingerprint images (one block), (c) FAX4 compressed signature image, and (d) JPEG compressed facial photographic image.		
25	The applicant data shall include name, alien registration number, social security number and other applicable biographic and demographic data as directed by the ASC Program. Site operations data shall include fields such as an ASC site code; machine code, operator id, and Live-Scan make and model. Text data fields shall conform to EFTS v7.0.		
26	Shall support transmission to the local store-and-forward mail server of fingerprint images that meet FBI image quality standards. All the data files transmitted by the Live-Scan systems shall comply with all applicable FBI, ANSI/NIST and NIST/EFTS standards for the data interchange.		

27	The Live-Scan System shall create an alpha/numeric identification number called a Transaction Control Number (TCN) on each submission in a field specified by the Government. The TCN shall consist of a receipt number (3 alpha characters, 10 numerics) followed by a zero, and followed by a date CCYYMMDD.		
28	Shall store and transmit a unique site code on each submission in a field specified by the ASC Program		
29	Shall capture management information to include processing time (date and time stamp for each applicant record) by machine and by operator. This management data shall, at a minimum be sent to the store-and-forward mail server.		
30	Each applicant record shall include demographic data; one JPEG compressed photograph image; one optionally captured fingerprint; and one optionally captured signature.		
Technical Requirements for the Live-Scan System			
31	Comply with all applicable FBI, ANSI/NIST, NIST/EFTS Standards outlined in the FBI Appendix F for the data interchange and list such standards in its documentation.		
32	Be capable of transmitting records using the latest FBI record format – Electronic Biometric Transmission Specification (EBTS) 8.1 and EBTS 8.001 XML.		
33	Provide the run time licenses for its local applications (e.g., database).		
34	Be designed to function in an office environment of 60 to 90 degrees Fahrenheit and 20 to 80 percent relative humidity, non-condensing, and shall not require any special air conditioning.		
35	Meet or provide equivalent facilitation for applicable Section 508 Electronic and Information Technology Accessibility standards for the disabled (see Section 16.0, Electronic and Information Technology Accessibility).		
36	Be upgradeable such that it is capable of capturing a variety of biometric data including type 14, type 4 fingerprint images, iris, photos, and signature using plug and play devices.		
Software Configurations			
37	The Contractor shall perform all required Live-Scan software configurations/modifications required to interface with USCIS systems and meet USCIS data profile requirements		
38	The Live-Scan application must operate on a USCIS-provided Windows XP operating system with the Federal Desktop Core Configuration (FDCC).		
39	The Live-Scan System shall support a Lightweight Directory Access Protocol (LDAP) connector such that the scanner application software utilizes the Microsoft Active Directory for user accounts and login.		
40	In addition to the USCIS software configurations, the software requires customization for the processing of UKvisas applicants		

41	The contractor must provide two (2) of each type of Live-Scan System ("cabinet", "desktop", and "mobile") to USCIS Headquarters (Attention: Hugh Jordan, Office of Field Operations, 111 Massachusetts Avenue, Washington, DC 20001) within five (5) business days following contract award. The systems shall include all peripherals and the COTS software (if the "cabinet" and "desktop" configurations include identical computers and peripherals, then only one (1) "cabinet" system and one (1) "desktop" system shall need to be provided). These systems will be used for the purpose of systems configuration/compatibility testing and solidifying the USCIS operating system "image" to be used by the Live-Scan Systems.		
	Deployment		
42	No later than 4 weeks from delivery order award date, all software configuration and testing must be completed and final acceptance by the government must be received. The contractor will be required to work on-site with USCIS staff at USCIS Headquarters to solidify the customization of the Live-Scan Application and the operating system image.		
43	No later than 100 calendar days from final acceptance by the government of all software configurations, all Live-Scan systems must be operational at every USCIS location listed in Attachment G. The contractor shall have disposed of old equipment; delivered and installed new Live-Scan equipment, performed operational testing and provided required training at every USCIS location contained in Attachment A for all systems to be considered operational.		
44	The Contractor agrees to meet the Delivery Schedule (Attachment D)		
45	At the time of installation, the Contractor shall conduct on-site training of all USCIS designated Live-Scan operators.		
46	The contractor shall meet the shipping requirements as outlined in section 7.1 of the Statement Of Work (SOW).		
47	The contractor shall meet the disposal requirements as outlined in section 9.0 of the Statement Of Work (SOW).		
48	Old Live-Scan Systems will be installed in accordance with Section 10.0 of the SOW		
	Written Deliverables		
49	The Contractor shall provide all written deliverables/reports as indicated in section 14.0 of the Statement Of Work (SOW).		
	IT Security		
50	The contractor shall assist the appropriate USCIS ISSO with development and completion of all Systems Development Lifecycle (SDLC) activities and deliverables contained in the SDLC.		
51	The contractor shall comply with the DHS Management Directive 4300.1 "Information Technology Systems Security"		
52	All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as it relates to the Statement of Work		
	Operations and Maintenance (O&M) Support		
53	The Contractor shall provide hotline support via a single toll-free number		
54	The Contractor shall provide O&M support Monday through Friday 7AM to 5PM local time for each ASC (excluding federal holidays).		

55	Contractor shall provide a telephonic response within one (1) hour, at which time a resolution or plan for resolution will be provided.		
56	The contractor shall provide preventative and remedial maintenance services according to section 12.2 of the Statement of Work (SOW).		

****COMPLETED FORM MUST BE SUBMITTED WITH RFQ RESPONSE****

The following responses provided to provide contractors' disposition from the questions received from the Draft RFQ received previously. These responses are a consolidation of similar or identical questions from multiple sources.

If further questions arise, following the instructions contained in the RFQ.

1. Is USCIS considered fitting the current cabinets with new lives can and computer equipment?

Response: No current cabinets are not being reused.

2. There is a specific file naming convention for internal storage of fingerprints offered in Table C-1. Since this is just local storage or cache, why is a specific naming convention required?

Response: Specific naming convention is not required; Requirement removed from SOW.

3. Confirm that the NIST file structure, in use today at USCIS, is still required.

Response: Yes.

4. Will there be an ODC Clin? Will Travel have to be approved by the government?

Response: The fixed unit price shall be inclusive of all associated costs (labor; travel, installation and training, etc.) required to perform the requirements of the Statement of Work.

5. What is CIS' expected award and POP completion date?

Response: USCIS anticipates awarding the Delivery by the end of December 2009. Period of performance will commence upon award and continue as stated in the Statement of Work.

6. Will CIS provide a site contact for each site that can verify site conditions including delivery readiness, provide building access and site work signoff?

Response: Yes; each site location POC will be provided after award and prior to installation.

7. Security Requirements. What, if any, are the security requirements for integration personnel involved with the image deployment and packaging requirements?

Response: See the Security Requirements at Section 18 of the Statement of work.

8. SOW Section 6.2.1, Applicant biographic and demographic data shall be contained in a text file in standard .tif format. Does USCIS require this data and format in addition to the EFTS v7.0 record?

Response: USCIS requires data in the EFTS v7.0 format; SOW modified removing the requirement for .tif format.

9. SOW Section 6.2.1, each compressed fingerprint image shall be stored in a separate file named as follows: (Table referenced on Page 10). Does USCIS require this data and format in addition to the EFTS v7.0 record?

Response: No

10. SOW Section 6.2.1, all the data files shall be transferred to a specific directory on the mail server. Does USCIS plan to use FTP (or other file transfer methodologies) or SMTP as the term "mail server" implies?

Response: SMTP

11. SOW Section 6.2.1, Shall create and support transmission of an EBTS 8.001 XML file format to the USCIS Enterprise Bus. The Draft RFQ refers to EFTS 7.0 file format and specifications and EBTS 8.001 XML. Which file format and specification is required for compliance at time of award?

Response: EFTS 7.0

12. SOW Section 6.2.1, Shall create and support transmission of an EBTS 8.001 XML file format to the USCIS Enterprise Bus. The Draft RFQ refers to transmission of an EFTS v7.0 compliant file to a mail server and an EBTS 8.001 XML compliant file to the USCIS Enterprise Bus. Which transmission specification is required for compliance at time of award?

Response: Transmission of an EFTS v7.0 compliant file to a mail server

13. SOW Section 6.2.1, Shall be capable of producing fingerprint images with less than a 2% FBI reject rate. USCIS plan to verify compliance with this requirement?

Response: Standard removed from Statement of Work

14. SOW Section 6.2.1, Shall capture management information to include processing time (date and time stamp for start time and stop time for each applicant record) by machine and by operator, and for each applicant, number of reprints or rejects by machine and by operator. This management data shall, at a minimum, be saved to an ASCII text file and sent to the store-and-forward mail server or other devices. Can USCIS please provide the data file layout as well as the specifics for transmission to the mail server?

Response: Will be provided to contractor after award.

15. SOW Section 6.2.2, The photo shall be automatically sized according to the specifications listed in the FBI Appendix F. Please provide more information as to the requirement in this paragraph. Is it USCIS' requirement to be NIST Best Practices compliant?

Response: Statement of Work updated removing requirement.

16. SOW Section 6.2.2, Shall capture management information to include processing time (date and time stamp for each applicant record) by machine and by operator. This management data shall, at a minimum be sent to the store-and-forward mail server. Can USCIS please provide the data file layout as well as the specifics for transmission to the mail server?

Response: Will be provided to contractor after award.

17. SOW Section 6.2.3, Be capable of transmitting records using the latest FBI record format – EBTS 8.1 and EBTS 8.001 XML. The Draft RFQ references EFTS v7.0, EBTS 8.1, and EBTS 8.001 XML as the required file format. Is it a requirement to generate transactions for all the three specifications? Are there separate locations for each file to be transmitted to?

Response: Yes, the system must be capable of transmitting records using all three specifications. However, at time of award, only the EFTS v7.0 specification will be used to transmit records.

18. SOW Section 6.2.3, Have the ability to integrate an audit trail of the Live-Scan Operator automatically to all records generated with HSPD-12 specification with PIV capability. Does USCIS require that the Live-Scan Operators use their PIV credentials for logon and auditing? Please clarify this requirement.

Response: Requirement removed from Statement of Work

19. SOW Section 6.2.3, Have the ability to encrypt records following the FIPS 140-2 and FIPS 197 Advanced Encryption Standard 256 compliant algorithms. Does USCIS require the records be encrypted while stored locally, only during transmission, or both?

Response: Requirement removed from Statement of Work

20. SOW Section 6.2.4, The Live-Scan Systems are comprised of 3 different hardware configurations in the quantities specified in the delivery order schedule: Will DHS provide the awardee with diagrams of what the final solutions will look like or is contractor responsible for creating them?

Response: It is the responsibility of the Contractor to propose complete systems

21. SOW Section 6.2.4, A portable backdrop will be included for the purposes of capturing photographs. Can the backdrop and corresponding stand be in a separate carrying case from the enrollment system?

Response: Yes; Statement of Work modified

22. SOW Section 6.2.5, The Contractor shall perform all required Live-Scan software configurations/modifications required to interface with USCIS systems and meet USCIS data profile requirements. What detailed configuration is required above the base OS load to include software packages, customization steps, etc. required to make the final image?

Response: This is primarily related to configuring the Live-Scan software application to successfully interface with the local store and forward mail servers, the LDAP connector, and to ensure compatibility with DHS network settings and virus scanning software. USCIS Office of Information Technology will be responsible for OS configurations and settings (ex. Administrator rights, Network protocols and settings, etc.), loading device drivers, virus scan software, etc.

23. SOW Section 6.2.5 Image, Will the government provide the specs for which the COTS image will be based on?

Response: The base OS image will be based upon the Federal Desktop Core Configuration (FDCC). Specs provided in the Statement of Work

24. SOW Section 7.1, The Live-Scan Systems shall be shipped to arrive at the installation site no sooner than 72hrs prior to installation. Can the government confirm that there will be adequate space available at each location to receive and store the new equipment 72 hours in advance of the installation?

Response: Yes, each location will have ample space to receive equipment

25. SOW Section 8.0, Login and password integration (using an LDAP connector to access the Microsoft Active Directory) will also be tested. Phase 1 requires acceptance no later than 28 calendar days after award date. Will the government require that the LDAP connector to access the Microsoft active Directory be tested remotely for each system prior to shipping and installation? If so, how will the government provide access to the LDAP connector for the integrator?

Response: No, each system will not be tested remotely. The configuration and testing related to the LDAP connector will occur during the live-scan software application customization phase. The testing will be conducted using the 4-6 initially provided systems at USCIS headquarters.

26. SOW Section 8.0, This tests the communication connection between the Live-Scan system and the local store-and-forward mail server. Will the government require that access to the local store and forward mail server be tested remotely for each system prior to shipping and installation? If so, how will the government provide access to the server to the integrator?

Response: No. During the initial software testing and configuration, the 3 different Live-Scan models will be tested for transmission to the local store-and-forward mail server.

Each Live-Scan System will be tested for proper transmission during installation. This will occur by sending a test record from the Live-Scan Systems to the local store and forward mail server.

27. SOW Section 8.0, This tests the communication connection between the Live-Scan system and the ESB. The test must demonstrate that the fingerprint file generated by the Live-Scan is in the format specified by all relevant standards, compliant with ANSI/NIST and FBI EBTS specifications. Can the government specify the ANSI/NIST and FBI specifications they deem relevant for a compliant solution?

Response: EBTS 8.001 XML

28. SOW Section 9.0, Live scan systems at each specific location are to be disposed of in accordance with this SOW unless the Contractor is notified by the Government five business (5) days prior to the scheduled de-installation date that other disposal means will be utilized. Can the government specify the "other disposal means" that will be utilized?

Response: Statement of Work modified clarifying

29. SOW Section 9.0, Remove the hard drive component from the CPU of each Live-Scan system and give the hard drive components to the onsite Desktop Support Manager (DSM). Will the government require that the hard drive be cleansed of all data prior to delivery to the onsite DSM?

Response: No, the DSM will be responsible for hard drive degaussing

30. SOW Section 9.0, Dismantle and haul away each complete Live-Scan system and attached components for disposal as scrap. Can the government provide general specifications for the old systems and components that will be removed?

Response: The components are the same as those listed in section 6.2.4 Hardware Configurations in the SOW. There are currently 545 "cabinet", 45 "desktop", and 12 "mobile" Live-Scan Systems requiring disposal.

31. SOW Section 9.0, Ensure that all applicable Environmental Protection Agency (EPA) and state environmental regulations are met in disposing of the scrap property. Can the government provide a list of "all applicable Environmental Protection Agency and State Environmental regulations"?

Response: Contractor is responsible for compliance in accordance with the terms and conditions of their DHS FirstSource Contract.

32. SOW Section 10.0, The Contractor shall, in all cases, be responsible for burn-in, certification, and delivery of hardware and software not later than the delivery date specified in this delivery order, in accordance with the Schedule. What will the government require to certify that each system is completely operational prior to delivery?

Response: The government will provide this certification at the time of initial configuration using the 4-6 initially provided Live-Scan Systems. This certification will occur before deployment is allowed to commence. The government will not test each system prior to delivery.

33. SOW Section 10.0, Encrypting data for transmission to the mail server. Is this requirement in the wrong section?

Response: Statement of Work modified for clarity

34. SOW Section 10.0, The Contractor shall, in all cases, be responsible for burn-in. What are the pre-deployment burn-in requirements (Length, paperwork, etc)?

Response: Burn-in not be required; Statement of Work edited accordingly

35. SOW Section 11.0 On-Site Training, Will the government be providing a room at each location to conduct training?

Response: No, training will occur in the applicant processing area where the Live-Scan Systems are located.

36. SOW Section 14.0, The Contractor shall provide a monthly USCIS Systems Information Report to the COTR in MS Excel format via email no later than ten (10) business days following the end of the month. Will the government provide access to this system or will the integrator be required to provide via their own system?

Response: Contractor will be responsible for maintaining its own system of record.

37. SOW Section 18.0, Prior to the commencement of work, the Contractor shall ensure that all personnel involved in the operations and maintenance service, and related work thereof, meet the security requirements identified in this SOW. What Security Requirements will the government require of the deployment resources installing the new systems? Suitability only? Background Investigations?

Response: See solicitation and Statement of Work for security requirement for Suitability Determination and Background Investigations.

38. There is a specific file naming convention for internal storage of fingerprints offered in Table C-1. Since this is just local storage or cache, why is a specific naming convention required?

Response: Statement of Work modified clarifying naming convention.

39. Will the USCIS procurement consider small business (HUB Zone) credits for this program?

Response: USCIS has chosen DHS FirstSource contract vehicles; All FirstSource awardees are small businesses, no further socio-economic considerations are required.

40. Do you anticipate a bidders' conference to be held for this requirement.

Response: No conference is being held

41. What is the estimated date for orals/demonstrations?

Response: Based upon the current response date in the RFQ, USCIS anticipates conducting oral demonstration/presentation on or about November 5 thru 13, 2009

42. For oral demonstrations, where we may demonstrate our solution, will we be expected to interface directly to your system at the Massachusetts Avenue facility?

Response: No

43. Is there flexibility in the installation dates indicated in Attachment D? The number of installation teams operating during these weeks range from 3 to 15 teams. We would like to consider flattening out the installation team structures.

Response: The Deployment Schedule has been coordinated with USCIS functional elements to minimize disruptions to normal business operations. An alternate deployment schedule may be proposed, however if government review deems the schedule unacceptable, then the contractor's quotation submission may be found unacceptable.

44. Attachment D, Deployment Schedule indicates a Type of COLO or SA. Can you explain the abbreviations?

Response: COLO – stands for "Co-Located" and signifies that an Application Support Center (ASC) is located in a Government-provided facility. SA – stands for "Stand-Alone" and signifies that an Application Support Center (ASC) is located in a Contractor-leased facility.

45. SOW Section 6.2.1 and 6.2.2 in the Subject RFQ Statement of Work requires that a 10 print process take an average of 10 minutes to complete and that a non 10 print process take the same average of 10 minutes. When applicants are required to have both processes, is the average time for that to be 20 minutes?

Response: The average processing time will be 10 minutes. Although the two 2 processes contain a lot overlap, they are independent of each other.

46. For the cutover at each cabinet or desktop, will the installation team be able to remove each workstation, disabling that applicant processing desk for a short interruption in services, or will

we be required to keep the existing unit operational during the installation of the new equipment?

Response: During installation, the ASC will not be processing applicants (this will be coordinated well in advance such that a certain window of time will be allotted where no applicants will be scheduled for processing) and the existing equipment shall be allowed to be non-operational while it is removed for disposal and the new systems are installed.

47. Will the government allow the contractor to propose an incentive for early delivery?

Response: No

48. Please update the SF18 to be a small business set aside. The DHS Firstsource contract is a small business set aside.

Response: Not required, all DHS FirstSource contractors are small business.

49. Page 55 – Can tables, charts, & graphs be 10 pt font?

Response: Yes, RFQ Instructions modified accordingly.

50. Page 58 – Will there be a past performance questionnaire?

Response: Past Performance Questionnaires not required. See RFQ for Past Performance Information requirements.

51. Please confirm if the government would like the contractor to propose Key Personnel / Resumes. What is the minimum number of key personnel resumes that the offeror shall propose?

Response: Dependent upon the Contractor's management approach, it is the responsibility of the Contractor to identify any key personnel, if any, to be utilized in order to perform the work specified in the SOW. Statement of Qualifications is the preferred method of demonstrating qualifications of key personnel. See RFQ Submission instructions.

52. Assume all relocations will be priced separately since locations are unknown?

Response: Statement of Work modified clarifying relocations.

53. Can contractors provide alternative desktop / laptop/UPS OEMs?

Response: See RFQ, specifically the FAR provision 52.211-6, Brand Name or Equal and the instructions section of the RFQ.

54. The current ones provided may not meet the requirements of the new Live-Scan devices. One example is that page 16 requires ruggedized mobile units; however the Dell M6400 laptop is not a ruggedized laptop.

Response: The Statement of Work does not call for ruggedized mobile units. Only the case for transporting the mobile system shall be ruggedized.

55. Will there be payment for the 2 of each systems required for imaging / testing? Is it safe to assume that these units will be kept at CIS for the duration of this project for continued testing?

Response: Contractor may invoice for products delivered and accepted by the government. Yes these systems will be kept at USCIS for duration.

56. Is the contractor required to perform a discrete C&A on this system, or is this considered part of a USCIS General Support System?

Response: No, Contractor will be required to update the existing Live-Scan C&A

57. What level of contractor involvement will be necessary to perform C&A activities for the devices once deployed?

Response: Contractor will be required to update the existing Live-Scan C&A with new configurations. The C&A will be provided in soft copy.

58. The government has incorporated a series of disincentives into the structure of this contract. As such, this has the structure of a performance based engagement. Based on that fact, it is recommended that the government require offerors to provide a Quality Assurance Surveillance Plan to guide alignment to key metrics that define success for this program and ensure quality. If the government will require this, it is recommended to increase the page count by a minimum of 15 pages to account for this requirement.

Response: No QASP required

59. What is the government's timeline for phase 4 testing?

Response: Phase 4 testing will be conducted at the discretion the Government and will be determined after award.

60. What types of security scans are required for devices to be attached to the USCIS LAN/WAN, (2) who would perform those scans, and (3) would they be done prior to the site installation being considered complete?

Response: These configurations will be set during the software customization and USCIS operating system image configuration by OIT (with assistance from the Contractor, as required), which will be performed prior to deployment. At the point of installation, the complete Live-Scan Systems will need to be unpacked and plugged into

the network port. At which time, the local DSM will assist with port configuration, IP address configuration (if not performed previously), and sending a test record.

61. Will USCIS have available new static IP addresses for each of the new devices by the time they reach the installation site?

Response: Yes, shortly after award and prior to deployment, the Contractor will be provided with a list of static IP addresses.

62. Will USCIS personnel be responsible for any changes needed to the ASC mail servers to support the new devices (i.e. new accounts/addresses for new devices)?

Response: USCIS will be responsible for the ASC mail servers.

63. Does USCIS have a preferred method of communicating/integrating the contractor's CMDB for device configuration to the USCIS CMDB?

Response: The preferred method of communicating/integrating the contractor's CMDB for device configuration to the USCIS CMDB is XML.

64. What duration of runtime is required for the UPS devices?

Response: 15 minutes at a minimum

65. Will the USCIS encryption key authority be used for this deployment, or will the contractor be required to provide their own key management system?

Response: Statement of work modified, removing requirement.

66. Regarding Performance Deductions, will USCIS allow the contractor to propose an incentive structure for exceeding operational availability targets?

Response: No

67. In the "Basis of Award" section makes mention that this procurement is for "brand name products only". Can you please provide some clarification?

Response: Live-Scan Hardware and Software must be brand name COTS products.

68. Is it the Government's intention to evaluate Original Manufacturer Equipment?

Response: Yes

69. Will the government accept 3rd party integrators who put proprietary software on a traditional OEM platform to create an alternative solution.

Response: Yes Live-Scan Hardware and Software must be brand name COTS products.

70. Will the Government or Contractor be responsible for developing, testing and applying patches to deployed systems post installation?

Response: The Government will be responsible for virus protection, security patches/updates, etc. The Contractor will be responsible for any Live-Scan Application updates/patches, etc.

71. SOW Section 6.2.1, Paragraph 5: Each compressed fingerprint image shall be stored in a separate file named as follows; Does USCIS require this data and format in addition to the EFTS v7.0 record?

Response: No. Table C-1 and the corresponding language edited in Statement of Work

72. SOW Section 6.2.1, Paragraph 3: Shall create and support transmission of an EBTS 8.001 XML file format to the USCIS Enterprise Bus; The Draft RFQ refers to transmission of an EFTS v7.0 compliant file to a mail server and an EBTS 8.001 XML compliant file to the USCIS Enterprise Bus. Which transmission specification is required for compliance at time of award?

Response: EFTS v7.0 compliant file to a mail server

73. SOW Section 6.2.2, Paragraph 6: Have the ability to encrypt records following the FIPS 140-2 and FIPS 197 Advanced Encryption Standard 256 compliant algorithms. QUESTION: Does USCIS require the records be encrypted while stored locally, only during transmission, or both?

Response: Requirement removed from Statement of Work

74. SOW Section 6.2.4, Paragraph 23: A portable backdrop will be included for the purposes of capturing photographs: Can the backdrop and corresponding stand be in a carrying case separate from the enrollment system?

Response: Yes

75. In our opinion, section 12.1 (Page 25) is somewhat ambiguous with regards to the Technical Support Hotline. Elements of this section seem to indicate that the contractor will receive tier 1 support calls from ACS operators; however, other sections imply that a USCIS Service Desk will provide the tier 1 support and will only call the Contractors 'hot line' when it has been determined that there is a technical problem with the equipment. Furthermore, there is an implication that the contractors call center need not be staffed in a way that allows an immediate response to the USCIS query, only that the contractor provides a "telephonic response" within 1 hour. We believe the government will be best served by clarifying the contractor's requirements for provision of a "technical support hotline". Will the contractor only receive calls from the USCIS Service desk? Can the contractor utilize a "voice response unit" to receive and log the call and then provide a human response within one hour?

Response: When problems arise, the ASC staff will contact the USCIS Service Desk, which will create a ticket and call the Contractor's hotline. The Contractor's hotline will not be contacted directly by ASC staff, it will only receive calls from the USCIS Service Desk. The SOW states that the Contractor must provide a response (that includes a resolution or plan of resolution) to the ASC staff within 1hr of receipt of USCIS Service Desk call. Therefore, the Contractor's hotline must be able to accept calls from the USCIS Service Desk, receive the information (including the ticket number, description of problem, time of call, etc.), and have a technician call the ASC Staff with a resolution (or plan of resolution) within 1hr.

76. With regards to Section 12.2.1.3-1 preventative maintenance – hardware: mandatory quarterly maintenance for modern computer based equipment that has no moving parts seems excessive. We suggest that the government allow the contractor to determine a maintenance schedule that is better suited to this equipment. The government is already imposing a “fine” for equipment that exceeds a particular downtime threshold; therefore it is in the contractor's best interest to maintain the equipment in top operating condition.

Response: Statement of Work modified for clarity.

77. The RFP does not give any indication for how the contractor will be compensated for repairs and maintenance that are caused by improper use, abuse, or accidental damage to the equipment.

Responses: Issues that are the fault of the Government (abuse, damage, etc.) would not be required of the Contractor to cover as part of the warranty or O&M

78. Section 4.0 Background states that deployment of systems to overseas sites may be required and is considered in scope. How will the contractor be compensated for these undefined services on a strictly Firm-Fixed Price contract?

Response: Statement of work edited clarifying question

79. The government should rethink the use of the term “Facial recognition software” as used on page 12 of the RFP. This term is usually associated with facial matching (1:1 or 1:N). We believe that what the government requires is Facial Quality Assessment software that will in real time provide feedback to the operator that the image in the view of the camera meets some preset quality limits for: size, centering, and skew as well as many other properties. Furthermore, the government may wish to specify a particular image quality standard such as “ICAO 9303” compliant.

Response: Term has been renamed to “Face Detection Software”. No standard will be included.

80. SOW Section 6.2.3. Technical Requirements for the Live-Scan System specifies the use of a foot pedal to allow fingerprint capture. If we propose fingerprint scanners with auto-capture

and auto-save functionality, which negates the need for the operator to interact with the livescan/application via a foot pedal, mouse, or keyboard is the foot pedal still required?

Response: No. Statement of Work edited.

81. The remedial maintenance timelines on page 27 are not consistent with the Performance Deductions timelines on page 29. Example: On-site support within 72 hours for Puerto Rico, US VI (Page 27) versus 5 days for U.S. territories (Page 29).

Response: Statement of Work edited for clarity

82. Page 36 states clearly that non-U.S. citizens are not permitted in the performance of this contract for work related to DHS IT systems. On page 44 the waiver process is described which would enable some non-U.S. citizens to support the program. Will waiver requests be accepted under this contract?

Response: Follow guidance in Statement of Work

83. SOW Section 11.0 "Site Supervisor Training" instruction on report generation is requested. What does this refer to. We did not see any requirement for report generation from the Livescan systems.

Response: Statement of Work modified



NCS Technologies, Inc. Presents
A Proposal for ASC Biometric (Live-Scan) Refresh to
Department of Homeland Security- U.S. Citizenship and Immigration Services
HSSCCG-10-Q-00025



VOLUME I
TECHNICAL PROPOSAL

Offeror

NCS Technologies, Inc.
9490 Innovation Drive

Manassas, VA 20110

Tel: (703) 621-1700

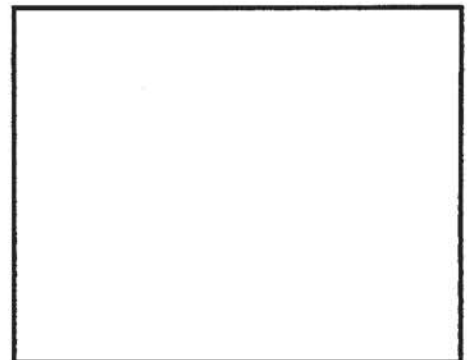
Fax: (703) 621-1701

www.ncst.com

DHS FirstSource Contract #

HSQDC-07-D-00028

NCS DHS Point of Contact



NON-DISCLOSURE PROVISION

This proposal contains data that shall not be disclosed outside of the government and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of, or in connection with the submission of this data, you shall have the right to duplicate, use, or disclose the data to the extent provisioned in the resulting contract. This restriction does not limit your right to use information contained in this document if it is obtained from another source without restriction. The data subject to this restriction is contained on the pages with the following legend: "Use or disclosure of data contained on this page is subject to the restriction on the title page of this proposal."

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO -
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)



NCS Technologies, Inc. Presents
A Proposal for ASC Biometric (Live-Scan) Refresh to
Department of Homeland Security- U.S. Citizenship and Immigration Services
HSSCCG-10-Q-00025



VOLUME II
PRICE QUOTATION

Offeror

NCS Technologies, Inc.
9490 Innovation Drive

Manassas, VA 20110

Tel: (703) 621-1700

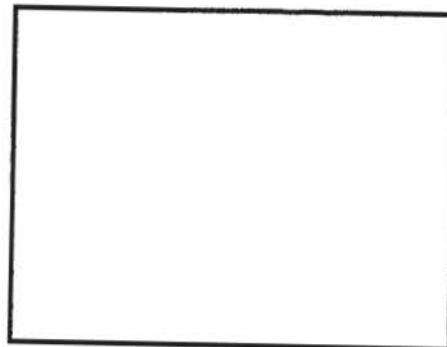
Fax: (703) 621-1701

www.ncst.com

DHS FirstSource Contract #

HSHQDC-07-D-00028

NCS DHS Point of Contact



NON-DISCLOSURE PROVISION

This proposal contains data that shall not be disclosed outside of the government and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of, or in connection with the submission of this data, you shall have the right to duplicate, use, or disclose the data to the extent provisioned in the resulting contract. This restriction does not limit your right to use information contained in this document if it is obtained from another source without restriction. The data subject to this restriction is contained on the pages with the following legend: "Use or disclosure of data contained on this page is subject to the restriction on the title page of this proposal."

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(3),(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

PAGE WITHHELD PURSUANT TO
(b)(4)

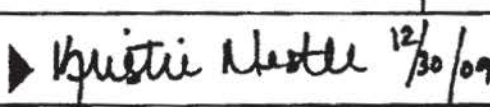
PAGE WITHHELD PURSUANT TO
(b)(4)

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 49

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER 12/30/2009		2. CONTRACT NO. (if any) HSHQDC-07-D-00028		5. SHIP TO: a. NAME OF CONSIGNEE Office of Field Operations			
3. ORDER NO. HSSCCG-10-J-00034		4. REQUISITION/REFERENCE NO. OFS-10-0008		b. STREET ADDRESS 20 Mass. Ave NW, 1st Floor Attn: Mark Jeanmaire			
5. ISSUING OFFICE (Address correspondence to) USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403				c. CITY Washington	d. STATE DC		
				e. ZIP CODE 20529			
7. TO: a. NAME OF CONTRACTOR NCS TECHNOLOGIES INC				f. SHIP VIA			
b. COMPANY NAME				8. TYPE OF ORDER <input type="checkbox"/> a. PURCHASE <input checked="" type="checkbox"/> b. DELIVERY			
c. STREET ADDRESS 9490 INNOVATION DRIVE				REFERENCE YOUR: Response to HSSCCG-10-Q-00025 Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.			
d. CITY MANASSAS		e. STATE VA	f. ZIP CODE 201102214	Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.			
9. ACCOUNTING AND APPROPRIATION DATA See Schedule				10. REQUISITIONING OFFICE			
11. BUSINESS CLASSIFICATION (Check appropriate box(es)) <input checked="" type="checkbox"/> a. SMALL <input type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input type="checkbox"/> e. HUBZone <input type="checkbox"/> f. EMERGING SMALL BUSINESS				12. F.O.B. POINT Destination			
13. PLACE OF a. INSPECTION Destination		b. ACCEPTANCE Destination		14. GOVERNMENT BAL. NO.			
				15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date) Multiple			
				16. DISCOUNT TERMS Net 30			
17. SCHEDULE (See reverse for Instructions)							
ITEM NO. (a)	SUPPLIES OR SERVICES (b)		QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	DUNS Number: 961003720+0000 Period of Performance: Base Period - 1/04/2010 to 2/28/2011 Period of Performance: Option Period 1 - 3/01/2011 to 2/29/2012 Continued ...						
18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		17(n) TOTAL (Cont. pages)	
21. MAIL INVOICE TO: a. NAME SEE PAGE 48 FOR b. STREET ADDRESS INVOICING INSTRUCTIONS (or P.O. Box) c. CITY d. STATE e. ZIP CODE						\$6,666,106.00	17(i) GRAND TOTAL
22. UNITED STATES OF AMERICA BY (Signature) 						23. NAME (Typed) Kristie Nestle TITLE: CONTRACTING/ORDERING OFFICER	

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (Rev. 4/2008)
Prescribed by GSA FPMR 48 CFR 53.213(g)

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE NO

2

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

ORDER NO.

12/30/2009

HSHQDC-07-D-00028

HSSCCG-10-J-00034

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Period of Performance: Option Period 2 - 3/01/2012 to 3/28/2013 Accounting Info: ASCLAB0 000 EX 20-01-00-000 17-40-0000-00-00-00-00 GE-25-14-00 000000				(b)(4)	
0001	Biometric (Live-Scan) Capture Systems, Cabinet Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A.	400	EA			
0002	Biometric (Live-Scan) Capture Systems, Desktop Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A.	100	EA			
0003	Biometric (Live-Scan) Capture Systems, Laptop (Mobile) Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A.	100	EA			
0004	Disposal of existing Biometric (Live-Scan) systems in conjunction with the installation of the new Live-Scan systems at all USCIS locations specified in Attachment A and in accordance with the Statement of Work.	602	EA			
1001	Option Period 1 - Biometric (Live-Scan) Continued ...	40	EA			

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

\$6,666,106.00

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 348 (Rev. 4/2006)

Prescribed by GSA FAR (48 CFR) 53.213(f)

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE NO

3

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

ORDER NO.

12/30/2009

HSHQDC-07-D-00028

HSSCCG-10-J-00034

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
(b)(4)	Capture Systems, Cabinet Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A. Amount: [REDACTED] Option Line Item) Anticipated Exercise Date:01/03/2011				(b)(4)	
1002	Option Period 1 - Biometric (Live-Scan) Capture Systems, Desktop Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A. Amount: [REDACTED] Option Line Item) Anticipated Exercise Date:01/03/2011	10	EA			
(b)(4)	Option Period 1 - Biometric (Live-Scan) Capture Systems, Laptop (Mobile) Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support systems as specified in the Statement of Work. All locations for delivery, install and training are in Attachment A. Amount: [REDACTED] Option Line Item) Anticipated Exercise Date:01/03/2011	10	EA			
1003	Option Period 1 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Cabinet Type Biometric System, as detailed in the Statement of Work. Amount: [REDACTED] Option Line Item) Anticipated Exercise Date:01/03/2011	400	EA			
(b)(4)	Option Period 1 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Desktop Type Biometric System, as detailed in the Statement of Work. Continued ...	100	EA			

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 348 (Rev. 4/2008)

Prescribed by GSA FPMR (41 CFR) 101-11.6

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE NO

4

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 12/30/2009 CONTRACT NO. HSHQDC-07-D-00028

ORDER NO. HSSCCG-10-J-00034

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
(b)(4)	Amount: [REDACTED] Option Line Item) Anticipated Exercise Date:01/03/2011				(b)(4)	
1006	Option Period 1 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Laptop (Mobile) Type Biometric System, as detailed in the Statement of Work.	100	EA			
(b)(4)	Amount: [REDACTED] Option Line Item) Anticipated Exercise Date:01/03/2011					
2001	Option Period 2 - Biometric (Live-Scan) Capture Systems, Cabinet Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work.	40	EA			
(b)(4)	Amount: [REDACTED] Option Line Item) Anticipated Exercise Date:01/02/2012					
2002	Option Period 2 - Biometric (Live-Scan) Capture Systems, Desktop Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support of systems as specified in the Statement of Work.	10	EA			
(b)(4)	Amount: [REDACTED] Option Line Item) Anticipated Exercise Date:01/02/2012					
2003	Option Period 2 - Biometric (Live-Scan) Capture Systems, Laptop (Mobile) Version - Provide systems, install systems and provide onsite user training, and Operations and Maintenance support systems as specified in the Statement of Work.	10	EA			
(b)(4)	Amount: [REDACTED] Option Line Item) Anticipated Exercise Date:01/02/2012					
2004	Option Period 2 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Cabinet Type Biometric System, as detailed in the Statement of Work.	400	EA			
(b)(4)	Amount: [REDACTED] Option Line Item) Anticipated Exercise Date:01/02/2012					
	Continued ...					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OF FORM 348 (Rev. 4/2006)
Prescribed by GSA FPMR (48 CFR) 53.213(f)

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE NO

5

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER CONTRACT NO.

12/30/2009 HSHQDC-07-D-00028

ORDER NO.

HSSCCG-10-J-00034

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
2005	Option Period 2 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Desktop Type Biometric System, as detailed in the Statement of Work. Amount: [REDACTED] Option Line Item) Anticipated Exercise Date:01/02/2012	100	EA			
(b)(4)						(b)(4)
2006	Option Period 2 - Operations and Maintenance Support (O&M) for Biometric (Live-Scan) Equipment - Laptop (Mobile) Type Biometric System, as detailed in the Statement of Work. Amount: [REDACTED] Option Line Item) Anticipated Exercise Date:01/02/2012	100	EA			
(b)(4)						
	The total amount of award: \$9,961,306.00. The obligation for this award is shown in box 17(i).					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

STATEMENT OF WORK

UNITED STATES CITIZENSHIP & IMMIGRATION SERVICES (USCIS) Application Support Center (ASC) BIOMETRICS (LIVE-SCAN) REFRESH

September 30, 2009

1.0 Title of Project

USCIS ASC Biometric (Live-Scan) Refresh

2.0 Period of Performance

The period of performance for this delivery order consists of a base period and two consecutive one year options. The base period will cover the replacement of the 602 existing biometric capturing systems (to include disposal of old equipment and delivery and installation of the new equipment), also the first year Operations & Maintenance (O&M) support will be provided as part of the new equipment purchased. In option years one and two, continued O&M support will be provided. Also, in the option years, additional Live-Scan Systems may be purchased up to a maximum of 60 units per year.

3.0 Contacts

The Contracting Officer at time of award will appoint a Contracting Officer Technical Representative (COTR) and furnish appointment information to the contractor.

4.0 Background

The United States Citizenship and Immigration Services (USCIS) utilizes Live-Scan electronic fingerprint scanning systems to digitally capture and electronically submit applicant fingerprint images to the Federal Bureau of Investigation (FBI) and US-VISIT. The fingerprints are used to conduct criminal background checks prior to USCIS making a determination whether to grant immigration benefits to applicants. Live Scan systems are currently at approximately 134 USCIS Application Support Centers (ASCs) located throughout the United States and the U.S. territories of Saipan, Guam, the Virgin Islands, and Puerto Rico. In 2001, in response to increased applicant workload resulting from the Legal Immigration Family Equity (LIFE) Act, USCIS initiated collection of digital photographs and digital signatures at the ASCs to further streamline and reduce timeframes needed to process USCIS benefits applications. Live-Scan systems acquired under this delivery order are expected to be used predominately at domestic ASCs and other domestic USCIS sites to replace existing Live-Scan technology that has become worn and outdated. Deployment of Live Scan devices and applicable support to overseas sites may be required under this delivery order, and is considered to be within scope. The existing live scan systems are to be replaced by newer model Live-Scan systems (approximately 400 "cabinet" style machines, 100 "desktop" style machines, and 100 "mobile" style machines) in early 2010. As new systems are deployed at each site, the old systems must be de-installed and disposed. USCIS intends for the contractor to dispose of 602 live scan systems at the ASC sites. This solution will continue to support USCIS' biometrics capturing goals of:

- Improving efficiencies,
- Preventing fraud,
- Ensuring accurate biographic/demographic data,
- Validating the biometrics data, and
- Meeting FBI image quality standards.

5.0 Scope

A description of the application process and the USCIS operating environment and resources available to the Contractor is provided below. Based on the current environment, the Contractor shall provide a turn-key Live-Scan system that can be connected to the USCIS LAN/WAN and which includes all the turn-key Live-Scan components and configurations to meet the operational requirements of this SOW. Live-Scan systems and components must have "plug and play" capability to capture and transmit FD-258 type 14 and type 4 fingerprint impressions, biographic and demographic data, and digital signatures in standard TIFF image format, and Joint Photographic Experts Group (JPEG) photograph images. As Citizenship and Immigration Services' requirements evolve, the Live-Scan systems provided under this delivery order shall be capable of capturing and transmitting additional biometrics data (e.g., iris, pressed 2-print images, etc.) with minor component and configuration changes, if required by the Government. The Contractor shall also provide, as a minimum, Live-Scan system hardware and software installation and integration services, remote VPN software maintenance, remedial hardware maintenance, technical support (toll-free telephone hotline), training (on-site user/ on-site systems administrator), standard commercial warranty, shipping, and removal/disposal of old equipment. The Contractor shall furnish all necessary personnel, materials, and other supplies/services as may be required to perform the work set forth in this SOW.

5.1 Current Environment

USCIS collected biometrics data from 2.5 million immigration benefits applicants in Fiscal Year 2009, of which approximately 1 million required ten-print fingerprinting and the remainder required collection of single flat impression (press) fingerprints, photographs, and digital signatures. USCIS will continue to use Live-Scan systems for electronic submission of FD-258 fingerprint images to the FBI and US-VISIT for use in searching criminal history databases for records that may disqualify an applicant for benefits. USCIS currently operates 602 Live-Scan devices at 134 ASC sites. **Attachment A** lists current ASC sites. Site locations are subject to change by the Government and the contractor will be notified via modification of specific location changes. Some location changes may require placement of equipment at overseas locations. These overseas locations, when added, will require O&M support. When the government requires relocation of Live Scan systems provided under this delivery order, the government may require the contractor to accomplish the equipment relocation. Any changes to the Live-Scan locations will be conducted through a contract modification and negotiated separately.

Live-Scan systems installed at ASCs will be interfaced to Government-provided store-and-forward mail servers, which in turn interface with USCIS Service Centers. The USCIS Service

Centers are the connectivity points to the Criminal Justice Information System (CJIS) WAN for submitting fingerprints and other biometrics data to the FBI, US-VISIT's IDENT, as well as interfacing with other internal USCIS systems. The ASCs use static Internet Protocol (IP) addresses that require Live-Scan Contractor personnel to maintain and change IP addresses in the field in coordination with the USCIS Help Desk.

The process for capturing biometrics data for immigration benefits is as follows (see **Attachment C** for diagram): The applicant submits an application to USCIS to request an immigration benefit. Application requirements vary for each specific benefit, and therefore require different biometrics collection requirements. Depending on the application being processed, USCIS generates either a 1D bar coded or 2D bar coded scheduling notice informing the applicant where and when to go to get processed for benefits. A 2D barcode is usually generated when FD-258 ten-print processing is required, and a 1D barcode is usually generated when only single press prints, photographs, and signatures are required. When notified, the applicant will go to an ASC to have fingerprints, photographs, signatures, and potentially other data captured using Live-Scan technology.

The normal data capture at the ASCs involves the Live-Scan system operator collecting biographic and demographic data including USCIS-specific identification numbers, name, date of birth, social security number, and other data, either by scanning the scheduling notice 1D or 2D barcode to populate the Live-Scan device data fields, using pull-down menus, or by manually entering the data using the keyboard. Current immigration benefits application requirements call for one of the following scenarios: the application requires FD-258 fingerprints (ten-prints) only; the application requires photograph, single press print (optional), and signature (optional) only; or, the application requires ten-print, photograph, single press fingerprint (optional), and signature (optional).

FD-258 fingerprints (ten-prints) taken at individual Live-Scan devices are forwarded in an Electronic Fingerprint Transmission Specification (EFTS) v7.0 compliant transaction to the local ASC store-and-forward mail server. EFTS is a National Institute of Standards and Technology (NIST) standard used by the law enforcement community (local, state, and federal) and civilian agencies to transmit demographic and image files using a common format. If required, a single press fingerprint image that meets FBI image quality standards is captured of the right index finger, or other finger if necessary. A digitally captured signature in standard TIFF image format is then recorded into the Live-Scan system followed by a facial photograph in standard JPEG image compression format. All the data and images captured can be reviewed and updated at the Live-Scan device before accepting and transmitting to the ASC mail server.

From the local store-and-forward mail server, the EFTS formatted applicant data files (biographic/demographic masthead data and EFTS formatted FD-258 ten-print images) are transmitted to the applicable USCIS Service Center. The Service Center server electronically sends all EFTS formatted applicant data files to the FBI. Applicant data files that include a photograph, press fingerprint, signature image, and associated biographic data are sent to the applicable USCIS service center.

The local ASC mail servers store the EFTS formatted applicant data file records for up to 30 days for reporting and resubmission. Each Live-Scan device currently deployed has minimum

capacity to store and retrieve at least 300 EFTS formatted applicant data files. (Note – This SOW requires a minimum storage and retrieval capacity of 500 each of FD-258 Ten-print files and Biometrics Capture files (total is 1,000). The primary objective of the storage of biometrics on the capture devices is to ensure continuity of operations and not to provide a fail safe for biometric data that gets lost in transmission in the store and forward process.

Neither the Live-scan device nor the local store-and-forward mail server communicates directly with the FBI.

ASC personnel are a mix of Government and contracted labor trained in the taking of quality fingerprints through Live-Scan and manual methods. ASC staffs are non-technical: the level of computer knowledge and abilities of the staff varies from location to location, but is generally very limited. The Live-Scan Contractor is advised that tasks including basic Live-Scan equipment set-up/configuration, basic computer file maintenance, account management, calibrating of systems, basic and preventive maintenance, installation of hardware components, etc. are not within the functional areas and technical abilities required of the ASC staff.

6.0 Live-Scan System Requirements

6.1 FBI Certification

All Live-Scan systems and components delivered by the Contractor shall be capable of transmitting FBI NIST/EFTS images to a local store-and-forward server. Live-Scan systems and components provided under this contract shall be FBI certified to comply with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) Image Quality Specifications (IQS) (See Appendix F) and the US-VISIT IDENT System.

6.2 Functional Requirements

The Live-Scan systems provided by the Contractor shall meet all the functional requirements in Section 6.2 and its sub-sections.

6.2.1 FD-258 Ten-Print Capture Requirements

The Live-Scan system:

- Shall process a minimum of six (6) ten-print applicants per hour (i.e., total time for a skilled fingerprint technician to process one FD-258 applicant shall be 10 minutes or less). The process begins when the Live-Scan system scans the 2D bar code with its scanner, entering FD-258 biographic and demographic masthead data, and ends with the submission of the record to the local store-and-forward mail server.
- Shall create an EFTS transaction containing 14 fingerprint images and biographic masthead data.

The applicant data files transmitted by the Live-Scan system to the local store-and-forward mail server shall include: (a) biographic and site operations text data,

and (b) Wavelet Scalar Quantization (WSQ) compressed fingerprint images (14 blocks) corresponding to fingerprint boxes on the applicant fingerprint card.

The applicant data shall include name, date of birth, sex, race, height, weight, eye and hair color, place of birth, residence, country of citizenship, and all other applicable biographic and demographic data as contained in the masthead of the FD-258 Fingerprint Card. Site operations data shall include fields such as an ASC site identifier; machine code, operator code, and Live-Scan make and model. Text data fields shall conform to EFTS v7.0. Information that populates the EFTS standard will be provided to the vendor after award of the delivery order.

Currently, the fingerprint image records shall include the ten rolled fingerprints, two flat impressions of four fingers (left and right hands) and two flat thumb prints. The image sizes shall be consistent with the fingerprint boxes on the standard FD-258 fingerprint card. The transmitted fingerprint images shall be in compliance with ANSI/NIST Standards identified in the attached FBI Appendix F. The compression algorithms used in the Live-Scan system for compressing the fingerprint images must comply with FBI approved WSQ gray scale compression standards.

- Shall support EFTS v7.0 specifications for maximum sizes of fingerprint images (provided in Table C-2).

Fingerprint	Width Pixels (inches)	Height Pixels (inches)
Rolled impressions Fingers 1 – 10	800 (1.6)	750 (1.5)
Plain Thumb impression	500 (1.0)	1000 (2.0)
4 Finger Plain impression	1600 (3.2)	1000 (2.0)

Table C-2 Maximum Sizes for Fingerprint Images

- Shall support transmission of an EFTS v7.0 file format fingerprint image to the local store-and-forward mail server. **Attachment B** lists typical USCIS server configurations. All the data files shall be transferred to a specified directory on the mail server. All the data files transmitted by the Live-Scan systems shall comply with all applicable FBI, ANSI/NIST and NIST/EFTS standards for the data interchange.
- Shall create and support transmission of an EBTS 8.001 XML file.
- Shall meet the basic format requirements for Logical Record types as defined by the EBTS message set forth in the ANSI standards which are also applicable to transmissions to the FBI.
- Shall create an alpha/numeric identification number in a specified FD-258 field in the event that the applicant does not have either an A-number or a social security

number. The alpha/numeric identification number will consist of a unique applicant identifier appended with a 12-digit date and time stamp in the format CCYYMMDDHHMM. The unique applicant identifier may be a "Z number", which is a 10-digit number generated randomly by the Live-Scan device, an "F number", which is a manually entered number with F in the first position followed by nine numeric numbers, or another unique number specified by USCIS.

- Shall store and transmit a unique site code on each submission in a FD-258 field specified by USCIS.
- Shall read both 1D and 2D bar codes.
- Shall capture type 14 and type 4 fingerprints.
- Shall be capable of capturing quality (FBI-acceptable) fingerprint images for a complete spectrum of skin pigmentation.
- Shall be capable of performing data entry of demographic information using pull down menus/tables.
- Shall be capable of performing instant preview and editing capabilities.
- Shall capture information used for quality control (QC) checks (user ID of the QC checker).
- **Shall capture management information to include processing time (date and time stamp for start time and stop time for each applicant record) by machine and by operator. This management data shall, at a minimum, be saved to an ASCII text file and sent to the store-and-forward mail server or other devices.**
- Shall have the capacity to store a minimum of 500 ten-print fingerprint records in each machine and 500 biometric records.
- Shall have the capability to purge records from the Live-Scan system upon demand by the user.
- Shall have the capability at the Live-Scan device to query the records stored in the Live-Scan device on an applicant's name, A-number, social security number, or date fingerprinted, and retrieve records and fingerprints (that have not been purged).
- Shall be capable of displaying retrieved records and fingerprints at the Live-Scan device.
- Shall have the capability to edit, modify, and resubmit retrieved records that replace the modified record.

6.2.2 Requirements for Other Biometrics Capture

This subsection specifies requirements for non-tenprint Biometric Capture Only (Single Pressed Print, Photograph, and Signature)

The Live-Scan system:

- Shall process a minimum of six (6) non-tenprint applicants per hour (i.e., total time for a skilled technician to process one applicant shall be 10 minutes or less.) The process begins when the Live-Scan system scans the 2D bar code with its scanner, entering biographic and demographic data, captures a single press fingerprint image, a digital signature, and a digital facial photograph, and ends with the submission of the record to the local store-and-forward mail server.
- Shall allow specified biographic data fields to be entered through the use of 1D and 2D bar code scanners/light pens.
- Shall capture an applicant's signature using a digital signature pad.
- Shall allow the single press-print image and/or digital signature capture to be optional.
- Shall require the digital photograph capture of a single facial photo per record for applicants whose press print, photo and signature are captured.
- The digital camera shall be controlled using the fingerprinting station's keyboard and will utilize face detection software that locates an applicant's face and automatically centers it in the photo. The photo shall be automatically sized to 300 pixels x 300 pixels and saved in the jpeg format.
- Shall create a file containing one facial photograph, biographic data, and an optionally captured digital signature and/or single press fingerprint image.
- The applicant data files transmitted by the Live-Scan system to the local store-and-forward mail server shall include: (a) demographic and site operations data (b) Wavelet Scalar Quantization (WSQ) compressed fingerprint images (one block), (c) FAX4 compressed signature image, and (d) JPEG compressed facial photographic image.
- The applicant data shall include name, alien registration number, social security number and other applicable biographic and demographic data as directed by the ASC Program. Site operations data shall include fields such as an ASC site code, machine code, operator id, and Live-Scan make and model. Text data fields shall conform to EFTS v7.0. Information that populates the EFTS standard will be provided to contractor by the Government after award of the delivery order.
- Shall produce a single press fingerprint .wsq image with maximum dimensions 500 pixels (1.0 inch) wide by 500 pixels (1.0 inch) high.

- Shall support transmission to the local store-and-forward mail server of fingerprint images that meet FBI image quality standards. All the data files transmitted by the Live-Scan systems shall comply with all applicable FBI, ANSI/NIST and NIST/EFTS standards for the data interchange.
- The Live-Scan System shall create an alpha/numeric identification number called a Transaction Control Number (TCN) on each submission in a field specified by the Government. The TCN shall consist of a receipt number (3 alpha characters, 10 numerics) followed by a zero, and followed by a date CCYYMMDD.
- Shall store and transmit a unique site code on each submission in a field specified by the ASC Program.
- The Live-Scan System shall be capable of performing data entry of demographic information using pull down menus. Data entry shall be done using touch screen displays to speed up the processing of the masthead data.
- Shall be capable of performing instant preview and editing capabilities.
- Shall capture management information to include processing time (date and time stamp for each applicant record) by machine and by operator. This management data shall, at a minimum be sent to the store-and-forward mail server.
- Each applicant record shall include demographic data; one JPEG compressed photograph image; one optionally captured fingerprint; and one optionally captured signature.

6.2.3. Technical Requirements for the Live-Scan System

The Live-Scan system provided by the Contractor shall:

- Comply with all applicable FBI, ANSI/NIST, NIST/EFTS Standards outlined in the FBI Appendix F for the data interchange and list such standards in its documentation.
- Be capable of transmitting records using the latest FBI record format – Electronic Biometric Transmission Specification (EBTS) 8.1 and EBTS 8.001 XML.
- Provide the run time licenses for its local applications (e.g., database).
- Include a standard 1yr warranty or better.
- Incorporate standard system security features (e.g., operator log-on, passwords).

- Use Commercial Off The Shelf (COTS) software to allow for the customization of data entry and menu screens. The COTS software should run on a variety of hardware platforms to ensure all devices have the same look and feel to the operators.
- Use Computer equipment (Workstations, laptops, etc.) that meets USCIS Office of Information Technology (OIT) specifications to ensure a consistent platform across USCIS. The workstations and laptops shall be the same or equivalent (brand name or equal) to:

The current OIT-Approved Workstation configuration is: a DELL Optiplex 760 Small Form Factor with an Intel Core 2 Duo E7300 2.66 GHz Processor, 4 GB Memory (2 X 2GB Modules), 160 GB Hard Drive, 8x DVD +/-RW Slimline Drive, 256 MB ATI Radeon HD 3450 Dual DVI/VGI Graphics Card with TV-out, and a 10/100/1000 MB Network Interface Card.

The current OIT-Approved Laptop configuration is: a DELL Precision M6400 with an Intel Core 2 Duo T9550 2.66 GHz Processor, 4 GB Memory (2 X 2GB Modules), 160 GB Hard Drive, 8x DVD +/-RW Drive, 17 inch WUXGA LCD Wide Screen, 9 Cell/85 WHr Primary Battery, 100/1000 MB Network Interface Card, Bluetooth Wireless and 802.11 a/b/g/n Mini-Card, and Internal Backlit Keyboard.

- Use an Uninterrupted Power Supply (UPS) that meets USCIS Office of Information Technology (OIT) specifications to ensure a consistent platform across USCIS (applicable to "cabinet" and "desktop" systems). The UPS shall be the same or equivalent (brand name or equal) to:

The current OIT-Approved UPS is: a Smart Pro LCD UPS with a Network Monitoring USB Port, 4 UPS Battery Support Outlets, and Additional 4, Surge Suppression-Only Outlets.

- Be designed to function in an office environment of 60 to 90 degrees Fahrenheit and 20 to 80 percent relative humidity, non-condensing, and shall not require any special air conditioning.
- Meet or provide equivalent facilitation for applicable Section 508 Electronic and Information Technology Accessibility standards for the disabled (see Section 16.0, Electronic and Information Technology Accessibility).
- Be upgradeable such that it is capable of capturing a variety of biometric data including type 14, type 4 fingerprint images, iris, photos, and signature using plug and play devices.

- Be capable of adjusting the height of the scanner decks, and shall have **angled** keyboards to make the fingerprint equipment ergonomic; for ease of use by the fingerprint technicians (pertains to "cabinet" systems).
- Allow fingerprint capture by use of a foot pedal. The Live-Scan Operator shall be able to capture an applicant's fingerprint images by pressing a foot pedal so that he/she has full use of his/her hands to assist in rolling an applicant's fingers for print capture (applicable to "Mobile", "Desktop" and "Cabinet" systems). This requirement may be omitted if the Live-Scan System allows the Live-Scan Operator full use of his/her hands to assist in rolling an applicant's fingers for print capture.

6.2.4. Hardware Configurations

All components, such as the uninterrupted power supply, fingerprint scanner, foot pedal, touchscreen monitor, 1D & 2D barcode reader, digital camera, and digital signature pad, that may require device drivers shall be consistent across all Live-Scan Systems, without deviation in make and model. This ensures a consistent Live-Scan System across USCIS, which is critical for USCIS operating system image configuration.

The Live-Scan Systems are comprised of 3 different hardware configurations in the quantities specified in the delivery order schedule:

1. Cabinet System:

- A standalone system that has the computer, uninterrupted power supply, fingerprint scanner, foot pedal, touchscreen monitor, 1D & 2D barcode reader, digital camera, and digital signature pad supported by a "cabinet" structure.
- A stand may be substituted for a cabinet as long as it meets all of the requirements of the cabinet.
- The "cabinet" or stand shall no larger than 30"deep X 24" wide.
- The "cabinet" or stand shall be robust enough to support all of the above mentioned equipment and withstand full-time operational use for a 5yr lifecycle.
- The "cabinet" or stand shall have locking wheels.
- The fingerprint scanner is easily adjustable for height so that scanner can be raised or lowered to fit the height of the fingerprint technicians and to allow for handicapped access.
- The foot pedal rests on the floor and allows the Live-Scan Operator to capture an applicant's fingerprint images by pressing a foot pedal so that he/she has full use of his/her hands to assist in rolling an applicant's fingers for print capture (applicable to "Mobile", "Desktop" and "Cabinet" systems). This requirement may be omitted if the Live-Scan System allows the Live-Scan Operator full use of his/her hands to assist in rolling an applicant's fingers for print capture.
- The camera is affixed to the cabinet to prevent it from being knocked over.
- The keyboard is angled to help prevent injuries to the operators.
- The CPU and UPS shall be located in a locking enclosure to prevent tampering.

- Computer cables are hidden or are secured to avoid entanglement with the operator or applicant.
- Cable connections are secured to prevent damage if the cabinet is moved.
- Components will be plug and play compatible.

2. Desktop System:

- Composition is the same as the cabinet system, excluding the cabinet itself.
- Hardware is capable of being used on existing tables and or system furniture.
- Camera has to be secured to prevent it from being knocked over or knocked out of position.
- Table top version has all the same functionality as the cabinet version except for height-adjustable scanner deck and angled keyboard.
- Components will be plug and play compatible for ease of setup and removal.

3. Mobile System:

- Composition is the same as the cabinet system with the addition of a ruggedized case and the exclusion of the cabinet, UPS, computer (laptop as substitute), touchscreen monitor, height-adjustable scanner deck, and angled keyboard.
- Camera will be secured to a tripod for easy set up.
- Portable system will be capable of being packed into a single contractor-provided ruggedized case for transport. System must be capable of meeting all airline travel requirements.
- External battery power is provided to allow equipment to be operated in remote locations without electricity.
- All devices will be plug and play compatible for ease of setup and removal.
- A portable backdrop will be included for the purposes of capturing photographs and shall be off-white in color.

6.2.5. Software Configurations

The Contractor shall perform all required Live-Scan software configurations/modifications required to interface with USCIS systems and meet USCIS data profile requirements. The Contractor shall submit the modified software for USCIS approval prior to placement on live-scan systems. Immediately following contract award, USCIS will provide the Contractor with the specifications for data fields and types, screen layouts, and the local store-and-forward mail server connection information. The Contractor will then be responsible for customizing its COTS Live-Scan application software and submitting it to USCIS (Attention: Hugh Jordan) for testing and approval. Testing will occur at USCIS HQ (111 Massachusetts Ave, NW, Washington DC, 20001) in the 2nd floor ASC lab.

As part of the software customization, the Contractor shall be required to maintain USCIS software tables that include demographic information used in processing USCIS Live-Scan transactions. Tables are accessed by the Live-Scan operator through the use of pull-down menus

on the Live-Scan device. USCIS will provide USCIS-specific tables (e.g., Originating Agency Indicator (ORI) Code, Reason Fingerprinted, Place of Birth, and Country of Citizenship) to the Contractor after award for incorporation into the Contractor's Live-Scan software. USCIS will validate all tables during the software approval process.

In addition to the USCIS software configurations, the software requires customization for the processing of UKvisas applicants. See **Attachment E** for the customization requirements for UKvisas.

The Live-Scan application must operate on a USCIS-provided Windows XP operating system with the Federal Desktop Core Configuration (FDCC). The National Institute of Standards and Technology (NIST) FDCC guidelines and specifications are available at the following link: http://csrc.nist.gov/itsec/download_WinXP.html

The USCIS operating system "image" will be provided to the contractor upon award of the delivery order. As part of the USCIS image, the software (to include the operating system), corresponding licenses, and maintenance will be provided by the government via Enterprise License Agreements.

The Live-Scan System shall support a Lightweight Directory Access Protocol (LDAP) connector such that the scanner application software utilizes the Microsoft Active Directory for user accounts and login.

7.0 Delivery

The Contractor shall provide the COTR with one central point of contact for all activities related to initial setup and deployment.

The Contractor must provide two (2) of each type of Live-Scan System ("cabinet", "desktop", and "mobile") to USCIS Headquarters (Attention: Hugh Jordan, Office of Field Operations, 111 Massachusetts Avenue, Washington, DC 20001) within five (5) business days following contract award. A business day is defined as Monday – Friday, 8AM to 5PM. The systems shall include all peripherals and the COTS software (if the "cabinet" and "desktop" configurations include identical computers and peripherals, then only one (1) "cabinet" system and one (1) "desktop" system shall need to be provided). These systems will be used for the purpose of systems configuration/compatibility testing and solidifying the USCIS operating system "image" to be used by the Live-Scan Systems.

No later than 28 calendar days after the delivery order award date, all software configurations and testing must be completed and final acceptance by the government must be received. The Contractor will be required to work on-site with USCIS staff at USCIS Headquarters to solidify the customization of the Live-Scan Application and the operating system images (one for each computing platform). Any time saved on the 28 calendar days will also be added to the 100 calendar day deployment schedule (up to 14 calendar days). After final acceptance of the software customization by the government, an additional 14 calendar days will be required to complete the USCIS image. Once complete, the government will provide the Contractor a copy

of the USCIS Image. **The deployment period shall begin 10 calendar days after the Government provides the USCIS image to the contractor.**

All 400 "cabinet" and 100 "desktop" Live-Scan Systems Live-Scan Systems shall be operational at all USCIS locations identified in **Attachment A** no later than 100 calendar days from the start of the deployment period. The contractor shall dispose of all old equipment; deliver and install new Live-Scan equipment, perform operational testing, and provide required training at every USCIS location, listed in **Attachment A**, in order for the systems to be considered operational.

"Mobile" Live-Scan Systems will not require installation and training. The 100 mobile systems shall be delivered to the USCIS Sites as specified in **Attachment A**, except for the laptop/computing devices themselves, which shall be shipped to USCIS Headquarters (111 Massachusetts Ave, Washington D.C. 20001) no later than 100 days from the beginning of the deployment period, where the government will install the USCIS operating system image, application software, and deliver them to the USCIS locations. The government will be responsible for the installation of the 100 "mobile" systems.

The deployment schedule is included as **Attachment D**. The contractor is to provide a written deployment plan immediately following contract award addressing the deployment schedule to include the disposal of old equipment, installation of new equipment, and training of users by USCIS Site. (**Attachment A** identifies the quantity and types of Live-Scan Systems to be installed at each USCIS location)

Operations and Maintenance (O&M) Support provided with the purchased equipment shall commence when all Live-Scan Systems are operational. Any installed systems, prior to all systems being operational, shall be supported by the contractor and any service shall be considered part of the installation. Inside delivery will be required for all shipments and curbside delivery (drop-shipping is not allowed and/or acceptable).

7.1 Shipping

The Live-Scan Systems shall be shipped to arrive at the installation site no sooner than 72hrs prior to installation. Live-Scan Systems shall be shipped as complete systems as opposed to shipping separate components. Live-Scan assembly shall be completed prior to shipment. The operating system and necessary software shall be installed and configured prior to shipment. Shipment dates shall be coordinated with the COTR. Shipping shall be considered FOB Destination and acceptance of the Live-Scan Equipment will occur upon receipt of a G504 Form. Shipping, packaging, and packing materials shall use recycled/recyclable materials to the maximum extent practicable. The Contractor is responsible for removing all shipping, packaging, and packing materials during installation and disposal.

7.2 Milestone Chart

MILESTONE CHART

Milestone	Description	Due Date
1	Deliver 2 of each Live-Scan System model to USCIS HQ (111 Massachusetts Ave, Washington DC 20001)	5 business days after award
2	Submit Final Systems Deployment Plan and Final Program Management Plan	5 business days after award
3	Appoint a senior official to act as the Corporate Security Officer Provide the COTR with one central point of contact for all activities related to initial setup and deployment	5 business days after award
4	Successful completion of Test Phases 1-3. Complete Live-Scan Software Customization	28 calendar days after contract award
5	Prospective Contractor employees shall submit completed background investigation forms to OSI through the COTR	No less than 30 days before the starting date of the contract or 30 days prior to entry on duty of any employees (approx 5 days after award)
6	Submit IT Security Plan for approval	Within 30 calendar days after contract award
7	Favorable entry on duty (EOD) determination received Contractor employees shall submit LAN account and GFE request forms	After favorable entry on duty (EOD) determination (approx 35 calendar days after award)
8	Submit MAC Address List	Prior to systems deployment (approx 36 calendar days after award)
9	USCIS Operating System Image completed and distributed to Contractor	42 calendar days after contract award
10	LAN Accounts and GFE received	43 calendar days after contract award
11	Begin deployment of Live-Scan Systems	52 calendar days after contract award
12	Complete Computer Security Awareness Training (CSAT)	60-days from the date of entry on duty (EOD)

13	All Live-Scan Systems Fully Operational (mobile unit cases and peripherals deployed and laptops sent to USCIS HQ)	152 calendar days after award
14	End of Deployment Phase & Operations and Maintenance Support begins	153 calendar days after award

8.0 Test and Acceptance

The test and acceptance evaluation shall occur in four (4) phases (and will be performed on the 4-6 systems provided immediately following contract award):

Phase 1 - Acceptance of the customization required of the COTS biometrics software application. The test will ensure all necessary data capture fields and corresponding data entry screens have been added in order to process UKvisas and Code 1-3 applicants. Login and password integration (using an LDAP connector to access the Microsoft Active Directory) will also be tested. Phase 1 requires acceptance no later than 28 calendar days after award date. Testing shall be performed at the USCIS ASC Lab (111 Massachusetts Avenue, 2nd floor, Washington D.C. 20001)

Phase 2 - This tests the communication connection between the Live-Scan system and the local store-and-forward mail server. The test must demonstrate that the fingerprint file generated by the Live-Scan is in the format specified by all relevant standards, compliant with ANSI/NIST and FBI specifications, and stored in the proper directory on the local store-and-forward mail server. Processing an USCIS application will test the file format for acceptability. Phase 2 requires acceptance no later than 28 calendar days after award date. Additionally, at time of installation at each USCIS location, this must be reconfirmed in order for each system to be considered operational. Testing shall be performed at the USCIS ASC Lab (111 Massachusetts Avenue, 2nd floor, Washington D.C. 20001).

Phase 3 - This test provides for acceptance of the encrypted file format and external media (such as a DVD-ROM) format by the Government. The file format originates from the Live-Scan systems and is forwarded to the local store-and-forward mail server, which forwards a daily batch to the Government's applicable store-and-forward transaction manager. Data is written to the external media (such as a DVD-ROM) using the same EFTS 7.0 format as the file format. Phase 3 requires acceptance no later than 28 calendar days after award date. Additionally, at time of installation at each USCIS location, this must be reconfirmed in order for each system to be considered operational.

Phase 4 - This tests the communication connection between the Live-Scan system and the ESB. The test must demonstrate that the fingerprint file generated by the Live-Scan is in the format specified by all relevant standards, compliant with ANSI/NIST and FBI EFTS specifications. Processing a USCIS application will test the file format for acceptability. This phase shall be conducted after deployment, and at the discretion of the Government.

9.0 Disposal

For all systems requiring disposal, the Contractor shall:

a. De-install existing Live-Scan systems in coordination with the installation of the new Live-Scan systems per the deployment schedule. Live scan systems at each specific location are to be disposed of in accordance with this SOW.

b. Remove the hard drive component from the CPU of each Live-Scan system and give the hard drive components to the onsite Desktop Support Manager (DSM). If the onsite DSM is absent, the ASC Manager or Site Supervisor shall suffice. The Contractor is responsible for providing written proof that the DSM, ASC Manager, or Site Supervisor certified in writing that the hard drive components for each specific machine have been removed and placed in custody of a government representative.

c. Dismantle and haul away each complete Live-Scan system and attached components for disposal as scrap.

d. Complete and Sign Form G-504, Report of Property Shipped/Received. The ASC Manager or Site Supervisor will also sign and take possession of the Form G-504 to acknowledge transfer of scrap property to the Contractor representative.

e. Ensure the following information included on and/or attached to the G-504 for each scrap system is correct:

- (1) Live-Scan System Property Control Number (PCN)
- (2) Component PCNs, if applicable
- (3) Live-Scan System Serial Number
- (4) Live-Scan Model Number

f. Remove all DHS PCN Labels from the Live-Scan Equipment and attach them to the back of the G-504. There are typically 3 labels on each Live-Scan system: 1 on the cabinet or computer, 1 on the barcode reader, and 1 on the digital camera.

g. Make all arrangements for transportation and disposal of scrap property, including inside pick-up, truck lift gate, shipping, and payment of disposal facility handling and disposal fees.

h. Ensure that all applicable Environmental Protection Agency (EPA) and state environmental regulations are met in disposing of the scrap property. Components of the scrap equipment contain hazardous materials. Prior to disposal, the Contractor shall obtain written certification and/or other proof from the waste disposal facility that the disposal facility is fully certified for hazardous waste disposal.

i. Following disposal, verify in writing to the ASC Program Contracting Officer Technical Representative (COTR) that the equipment has been disposed of as scrap material

through proper waste disposal procedures and facilities in accordance with all applicable government regulations. The Contractor shall provide the information listed in paragraph e, above, to describe the disposed scrap in the scrap disposal verification letter(s).

9.1. Performance of Services: The Contractor shall coordinate the de-installation and removal of scrap Live-Scan systems with the HQ, USCIS ASC Branch and local USCIS ASC/District staff.

9.2. Reselling Prohibition: The Contractor shall not resell any equipment that contains a memory component. Such components shall be disposed of in accordance with MD4300.1.

10.0 Installation

The contractor shall be responsible for all aspects of installation. Installation includes the following activities:

- Install and/or integrate Live-Scan hardware
- Install and/or integrate Live-Scan software, to include the USCIS image (provided by USCIS)
- Install and/or integrate component pieces as required to meet the requirements of this SOW
- Install DHS Property Control Number (PCN) Labels on Live-Scan Systems
- Complete a Form G-504 for the installation at each USCIS site.

The Government is responsible for installation site modifications, if required, to prepare the facility to receive the equipment, to include cabling, wiring, construction, and mail server installation.

The Contractor shall integrate all the hardware and load all necessary software and conduct a complete configuration test sufficient to ensure that the Live-Scan system is fully functional in each USCIS ASC site. The configuration for each ASC Live-Scan system shall be identical. The Contractor shall be responsible for setup and integration of devices. The Contractor shall certify each system as completely operational following installation and integration, in accordance with all terms and conditions of this delivery order.

Installation of the operating system on the fixed-disk drives in its own subdirectory; USCIS will provide the contractor with the USCIS operating system image. The contractor will be responsible for installing the image on each Live-Scan System. The USCIS image (containing the operating system and necessary software) shall be installed and configured prior to installation at a USCIS site.

The Contractor shall, in all cases, be responsible for certification, and delivery of hardware and software not later than the delivery date specified in this delivery order, in accordance with the Schedule. The Contractor shall adequately package Live-Scan systems to prevent shipping damage, make all arrangements for transportation, shipping, insurance, and commercial Bills of

Lading, and unpack and install systems at the receiving USCIS fingerprinting locations. Shipping costs shall be included in the price of the Live-Scan systems.

After contract award and prior to deployment, USCIS shall provide the Contractor with approximately 1,800 PCN Labels. While in the care of the Contractor, the Contractor shall be responsible for the PCN labels. The Contractor shall install the PCN labels on the Live-Scan Systems as follows:

Each model ("cabinet", "desktop", and "mobile") shall have a total of 3 PCN Labels:

- 1) One on the cabinet (if applicable) else on the computer
- 2) One on the Barcode Reader
- 3) One on the Digital Camera

Upon successful Live-Scan System installation at a USCIS site, the Contractor shall complete and Sign Form G-504, Report of Property Shipped/Received. The ASC Manager or Site Supervisor will also sign and take possession of the completed Form G-504 to acknowledge transfer of new property to the Government.

The Contractor shall ensure the following information included on the G-504 for each new system is correct:

- (1) Live-Scan System Property Control Number (PCN)
- (2) Component PCNs, if applicable
- (3) Live-Scan System Serial Number
- (4) Live-Scan Model Number

11.0 On-Site Training

At the time of installation, the Contractor shall conduct on-site training of all USCIS designated Live-Scan operators. The anticipated total number of individuals requiring initial training is approximately 1,000. Training shall be conducted at each ASC site (**Attachment A**). On-site training includes User training and Site Supervisor training. User Manuals and User Systems Administrators Manuals shall be provided at delivery and reviewed/used to facilitate training.

User Training includes the following:

- Operational instruction to identified Live-Scan operators.
- Review and familiarization with User Manual documentation (e.g., manual, video).
- Instruction on the systems' plug and play capabilities.
- Instruction on the setup and disassembly of portable systems.
- Basic instruction on general maintenance such as calibration and system restart.

Site Supervisor Training includes User Training plus the following activities:

- Basic troubleshooting/depot component replacement.
- Train the trainer instruction.

- Review and familiarization with User Manual documentation (e.g., manual, video).
- Instruction on software setup, if applicable.

12.0 Operations and Maintenance (O&M) Support

12.1 Technical Support Services (Hotline)

The Contractor shall provide a system of technical support for all Live-Scan systems delivered by the Contractor. The Contractor shall provide 24/7 hotline support via a single toll-free number in order to support the following hours of operation:

Sunday	Closed
Monday	7 am – 5 pm (local time at each USCIS site as listed in Attachment A)
Tuesday	7 am – 5 pm (local time at each USCIS site as listed in Attachment A)
Wednesday	7 am – 5 pm (local time at each USCIS site as listed in Attachment A)
Thursday	7 am – 5 pm (local time at each USCIS site as listed in Attachment A)
Friday	7 am – 5 pm (local time at each USCIS site as listed in Attachment A)
Saturday	Closed

The USCIS Service Desk will use the hotline to report technical problems for all ASC sites. The Contractor shall provide a telephonic response within one (1) hour, at which time a resolution or plan for resolution will be provided.

The Contractor shall provide the most effective method of providing responsive technical troubleshooting and resolution support, to include VPN remote access support. USCIS will provide VPN connections via the use of USCIS-issued laptops and SecureID tokens.

12.2 Remedial and Preventive Maintenance Services

The Contractor shall be responsible for hardware and software maintenance support for Live-Scan systems provided under this delivery order. The Contractor shall provide all maintenance coverage necessary to meet the requirements of this SOW. The Contractor shall coordinate warranty information and warranty services with the manufacturer of the hardware or software. At a minimum, the Contractor shall provide remedial maintenance coverage. Subject to security policies, regulations and procedures, the Government will permit on-site access to the equipment that is to be maintained.

12.2.1 General Maintenance Requirements

The Contractor shall provide all necessary personnel, materials, parts, tools, diagnostic and test equipment, technical manuals/publications and other services as may be required for the hardware maintenance support.

- Maintenance support shall include technical troubleshooting, problem resolution and component repair or replacement in order to maintain and keep the equipment covered under the order in full operating condition.

- The Contractor shall provide data concerning all maintenance activities. A service incident report (SIR) shall be available to the Government for any maintenance rendered by the Contractor under this delivery order (See Section 13.2.1.4. Responsibilities of the Contractor).

12.2.1.1 Periods of Maintenance

The Principal Period of Maintenance (PPM) and Official Operation Hours for equipment covered under this delivery order is 7 a.m. through 5 p.m., local time for each location as identified in **Attachment A**, Monday through Friday (five (5) days per week), excluding Federal Holidays.

12.2.1.2 Software Maintenance

The Contractor shall remotely load all revised software configurations and table updates down to the individual Live-Scan system from a central location utilizing the USCIS issued laptops and SecureID tokens. Remote access to the individual Live Scan systems can only be accomplished through the SecureID VPN token connections. VPN connections via SecureID tokens is the only means of performing certain types of maintenance to include software and hardware maintenance or system troubleshooting.

12.2.1.3 Hardware Maintenance

1. Preventive Maintenance

Preventive Maintenance is defined as regularly scheduled activities to maintain hardware in full operating condition. The frequency of preventive maintenance shall be at the discretion of the Contractor). The preventative maintenance shall be performed during remedial maintenance calls and/or during a mutually acceptable time during the specified PPM, unless otherwise agreed to by the Contractor and the Government. The Contractor shall provide the Government with a Preventative Maintenance schedule for Government review and approval.

2. Remedial Maintenance

Remedial maintenance is defined as identifying the source of an equipment or software malfunction and either repairing or replacing the malfunctioned component or subsystem. The Contractor shall provide the parts and equipment required for the diagnosis and repair of malfunctioning components of the Live-Scan system at the most cost effective manner available which will also minimize the downtime of the system. Remedial maintenance shall include transportation, labor and parts required for return of a malfunctioning system or equipment to full operating condition.

Repaired and/or replaced parts and labor shall be warranted for the standard 1 year warranty period from the date all systems are operational. If additional calls are required during the warranty period, for the warranted repair, they shall be made at no additional

cost to the Government. The contractor shall submit a copy of the Live-Scan warranty in writing to the COTR upon award of the delivery order.

The Contractor's responsibilities for remedial maintenance shall include:

- The administration and management of all warranties associated with the Live-Scan systems.
- Tracking the status and invoking the use of all applicable warranties of the Live-Scan systems.
- Telephonic responses to the originator within 1 hour of trouble call
- When on-site support is not required, the support must be completed within one (1) business day or three (3) business days if the shipping of parts is required.
- When on-site support is required, the support must be completed within three (3) business days for ASCs located within the Contiguous United States.
- When on-site support is required, the support must be completed within four (4) business days for ASCs located in Puerto Rico, U.S. Virgin Islands, and five (5) business days for ASCs located in Hawaii, Guam, Saipan, and Alaska.

Remedial maintenance shall be performed after notification that the system is inoperative (down). The Contractor shall provide USCIS with a designated point of contact and make arrangements to enable its maintenance representative to receive such notification and provide continuous telephone coverage within the PPM to permit USCIS to make such contact (See Section 13.1, Technical Support Services (Hotline)). Within one (1) hour of notification, the Contractor shall provide a telephonic response that assesses the situation, identifies the problem, and proposes the resolution and the time to fix the problem. Resident on-site maintenance at the USCIS sites is not required.

Downtime is that time in which the Contractor maintained equipment is inoperable due to a hardware malfunction. If the failure of one device causes other devices to be inoperable, these other devices may, at the Government's option, be considered down also. A determination of downtime will be made solely by the Government. Downtime for each failure shall start at the time the Government notifies the Contractor of a failure and shall run until the failed equipment is returned to full operating condition.

Types of Coverage Required

The Contractor shall provide all maintenance coverage necessary to meet the requirements of this SOW, to include system performance requirements in SOW Section 14.0. At a minimum, the Contractor must provide remedial hardware maintenance services that meet all maintenance requirements of this SOW.

12.2.1.4 Responsibilities of the Contractor

1. Parts Quality

The Contractor shall use only new standard parts or refurbished parts, certified as equal in performance to new parts by the Original Equipment Manufacturer, in performed

repairs. Parts that have been replaced shall become the property of the Contractor. The Contractor shall maintain a replacement parts policy consistent with supporting the performance requirements as stated in this SOW.

2. Protection of Information During Equipment Maintenance

The Contractor shall prevent loss of hard drive information during all maintenance activities by taking steps to protect and, at the Government's option, restore as necessary, any information residing in the equipment being maintained. The Contractor is responsible for the erasing or wiping of information from all hard drives removed or replaced by the Contractor. Hard drives must be wiped under the supervision of the Government Computer Systems Security Officer (CSSO). The Contractor shall be responsible for notifying the Contracting Officers Technical Representative (COTR) or designated representative if a hard drive containing information has been removed from an USCIS facility without erasing the data contained on the hard drive.

3. Remote System Access for Maintenance

A VPN connection via SecureID tokens is the only means of remote system access to perform required hardware maintenance or system troubleshooting.

4. Service Incident Reports (SIRs)

The Contractor shall maintain an electronic database of all SIRs to respond to Government inquiries regarding specific problems and issues. The SIR shall contain at a minimum, the following information:

- (1) Name of person requesting service
- (2) Location, including site code, office, city and state/country
- (3) Phone number of the person requesting service
- (4) Type of equipment
- (5) Serial number and USCIS property control number (PCN) of component being serviced
- (6) Date and time of request for service
- (7) Date and time of arrival of maintenance personnel (if applicable)
- (8) Date and time replacement part shipped (if applicable)
- (9) Description of problem
- (10) Parts replaced (including serial number and PCN if applicable)
- (11) Date and time problem was resolved
- (12) Reason problem not resolved within required timeframe (if applicable)
- (13) Any required follow-up actions
- (14) USCIS ticket number and vendor ticket number
- (15) Name of individual at affected site certifying the repair was completed

13.0 System Performance

The Contractor shall ensure that the Live-Scan systems meet the following availability and reliability requirements:

Live-Scan Systems:

- 95% availability per machine

Availability is defined as a system that is technically operational and supporting the mission of fingerprinting applicants for immigration benefits. The Live-Scan System is "unavailable" if it is unable to support the mission of capturing and transmitting complete applicant biometric data. Availability per machine is calculated as follows: number of business days/year that the machine was available divided by the number of total business days/per year x 100%. A machine is considered unavailable for one day when the machine is unavailable for over 50% of the day's total operational hours.

(Example: $255 / (365 \times (5/7)) \times 100\% = 247/260 \times 100\% = 95\%$)

At the Government's request, the Contractor shall replace systems that do not meet the stated requirements, above, at no cost to the Government.

13.1 Performance Deductions

The USCIS has determined that the Live-Scan equipment provided under this delivery order will perform functions that require assessment of payment deductions if the Contractor fails to correct technical malfunctions within the Government's timeframes specified below.

When on-site support is required, the Contractor shall provide all remedial action necessary to correct technical failures in Live-Scan equipment at USCIS sites within the 48 contiguous United States within three (3) business days of the trouble call, within four (4) business days for ASCs located in Puerto Rico, U.S. Virgin Islands, and five (5) business days for ASCs located in Hawaii, Guam, Saipan, and Alaska. The Contractor shall incur a \$100 invoice deduction per machine per day for each machine that remains down beyond these required timeframes.

When on-site support is not required, the Contractor shall provide all remedial action necessary to correct system issues/failures in Live-Scan equipment within one (1) business day of the trouble call. The Contractor shall incur a \$100 invoice deduction per machine per day for each machine that remains down beyond these required timeframes.

Availability shall be assessed by the COTR on a semi-annual basis. For each Live-Scan System found to be available less than 95% of the total operational time, an invoice deduction (taken in the following month) in the amount of \$100 per machine per day over the 95% threshold shall occur.

The Contractor shall not incur deductions when Acts of God (e.g. weather), Government actions (e.g., denial of facilities access), or other events outside of Contractor control prevent the Contractor from providing remedial action within the required timeframes.

14.0 Written Deliverables/Reports

a) The Contractor shall provide a written Systems Deployment Plan in electronic format to the COTR via email no later than five (5) business days following contract award. The Systems Deployment Plan shall incorporate the deployment schedule (**Attachment D**) and address the disposal of old equipment, installation of new equipment, and training of users by USCIS Site. (**Attachment A** identifies the quantity and types of Live-Scan Systems to be installed at each USCIS location). The Systems Deployment Plan shall be in electronic format and shall not be longer than 30 pages in length.

b) The Contractor shall provide a Program Management Plan in electronic format to the COTR via email no later than five (5) business days following contract award. The Program Management Plan shall address at a minimum, a risk management plan, a communication plan, key personnel (to include résumés), and subcontractor teaming arrangements. The Program Management Plan shall not be longer than 30 pages in length.

c) The Contractor shall provide a monthly utilization report in MS Excel format to the COTR via email no later than ten (10) business days following the end of the month. This report shall detail the number of calls received, time to respond to messages, time of arrival if an on-site maintenance call, technician's name, time to resolve, length of time a machine is "unavailable", type of problem, solution, corresponding USCIS ticket number, corresponding machine's serial number, location of problem, and point of contact.

d) Prior to the commencement of deployment, the contractor shall deliver (to the COTR) via email an updated **Attachment A**, which includes the Media Access Control (MAC) addresses of each Live-Scan System to be installed at each location. The MAC addresses must be provided so that port security settings may be set by USCIS to allow for the installation of the new machines.

e) The Contractor shall provide a preventative maintenance schedule to the COTR in MS Excel format via email no later than ten (10) business days prior to performing preventative maintenance. The schedule shall identify the date of preventative maintenance for each Live-Scan System.

f) The Contractor shall provide a preventative maintenance report to the COTR in MS Excel format via email no later than ten (10) business days following the end of a preventative maintenance cycle. The report shall identify each Live-Scan System by serial number and the corresponding dates when preventative maintenance was performed.

g) The Contractor shall provide a quarterly inventory report to the COTR in MS Excel format via email no later than ten (10) business days following the end of the quarter. During the deployment of the new Live-Scan Systems, the contractor shall provide the report on a weekly-basis. The report shall consist of a list of all system locations, serial numbers, DHS Property Control Numbers (PCN), as well as IP addresses and other network information necessary to maintain the systems on the USCIS Network.

h) In Lieu of submitting individual Service Incident Reports (SIR), the Contractor shall provide a monthly Service Incident Report (SIR) that aggregates the SIRs from the month into

one report. The report shall be delivered to the COTR in MS Excel format via email no later than ten (10) business days following the end of the month.

i) The Contractor shall provide a monthly USCIS Systems Information Report to the COTR in MS Excel format via email no later than ten (10) business days following the end of the month. The report shall contain at a minimum, the following information:

1. ASC Location
2. Type (Stand Alone or Co-Located)
3. ASC Site Code (i.e. X-code)
4. Live-Scan Model
5. Live-Scan System Name
6. IP Address
7. Live-Scan System Serial Number
8. Software Version
9. Software Modified Date
10. Live-Scan System Code
11. Mail Server IP Address
12. Gateway IP Address
13. Subnet Mask
14. Network IP
15. ORI Code

j) The Contractor shall provide a monthly Service Desk Report to the COTR in MS Excel format via email no later than ten (10) business days following the end of the month. The report shall contain at a minimum, the following information:

1. Remedy Ticket Number
2. Service Desk Ticket Number
3. Date Ticket Opened
4. Date Ticket Closed
5. Number of Business Days Ticket was Open
6. System Down (Yes or No)
7. ASC Site Code (i.e. X-code)
8. ASC Site Name
9. Problem Type
10. Summary (i.e. description of problem)
11. Status (Open or Closed)

k) The Contractor shall reconcile the USCIS Remedy Monthly Report, provided to the Contractor by USCIS, with the monthly Service Desk Report on a monthly-basis and submit to the COTR via email within ten (10) business days following the receipt of the USCIS Remedy Report. The USCIS Remedy Monthly Report contains the following data:

1. Remedy Ticket Number
2. ASC Site Code (i.e. X-Code)

3. ASC Location
4. Date Ticket was Opened
5. Issue/Problem
6. Ticket Assignment (miss assigned or not)
7. Status (Open or Closed)

14.1 Written Deliverables Schedule

WRITTEN DELIVERABLES SCHEDULE

Deliverable	Due Date	Format
Systems Deployment Plan	5 business days after award	Electronic
Program Management Plan	5 business days after award	Electronic
Monthly Utilization Report	10 business days following the end of the month	MS Excel
MAC Address List	Prior to Deployment	MS Excel
Preventative Maintenance Schedule	10 business days prior to performing preventative maintenance	MS Excel
Preventative Maintenance Report	10 business days following the end of the month	MS Excel
Quarterly Inventory Report	10 business days following the end of the quarter (weekly-basis during deployment)	MS Excel
Service Incident Report	10 business days following the end of the month	MS Excel
Systems Information Report	10 business days following the end of the month	MS Excel
Monthly Service Desk Report	10 business days following the end of the month	MS Excel
Reconciled USCIS Remedy Monthly Report	10 business days following receipt of Remedy Report	MS Excel

15.0 Government Furnished Equipment (GFE)

Upon contract award and after the issuance of proper EOD clearances, the government shall provide a maximum of five (5) USCIS Laptops and five (5) SecureID VPN Tokens to the Contractor. A laptop and a VPN token each must be assigned to a single individual. The laptops and VPN tokens may only be distributed upon successful completion of the security clearance paperwork (see section 18.0 Security Requirements) resulting in a favorable Entry On Duty (EOD) determination. Additionally, the Contractor shall submit the following forms for each individual prior to attainment/use of the GFE:

- Information Technology Service Request (ITSR) Form

- USCIS HQ LAN Account Request Form
- A New Laptop User Registration Form
- USCIS VPN Request Form
- G504 Property Receiving and Acceptance Form

16.0 Electronic and Information Technology Accessibility

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 EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable 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, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then “1194.21 Software” standards also apply to fulfill functional performance criteria.

36 CFR 1194.23 – Telecommunications Products, 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, 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 is through the use of a Web or Software application interface having 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.

36 CFR 1194.26 – Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) 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 DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

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 meets 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 of 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.

17.0 Facility Access Control

The Contractor shall observe all internal building security regulations that apply to any and all buildings concerned with this contract. The Contractor shall only enter the facility or building

with continuous escort service. When entering and departing the facility or building each Contractor must sign in and out as required at the site.

Equipment and Materials Dismantling, Handling, and/or Hauling: The Contractor shall coordinate the route of moving equipment and materials within the facility before dismantling, handling and/or hauling same with the COTR or authorized Government representative. The Contractor shall notify the COTR or authorized Government representative to reach a mutually acceptable time and date corrective action will be completed for work required in response to an emergency or urgent service call within the response time specified herein. The Government reserves the right to inspect the equipment before, during and after any work performed.

Temporary Outages: The Contractor shall coordinate all temporary outages of any equipment with the COTR/authorized representative not less than 72 hours in advance of such outages.

18.0 Security Requirements

Prior to the commencement of work, the Contractor shall ensure that all personnel involved in the operations and maintenance service, and related work thereof, meet the security requirements identified in this SOW.

SECURITY REQUIREMENTS

GENERAL

U.S. Citizenship & Immigration Services (USCIS) has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to sensitive but unclassified information, and that the Contractor will adhere to the following.

SUITABILITY DETERMINATION

USCIS shall have and exercise full control over granting, denying, withholding or terminating access to government facilities and/or access of Contractor employees to sensitive but unclassified information, based upon the results of a background investigation. USCIS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by USCIS, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a USCIS facility without a favorable EOD decision or suitability determination by the Office of Security and Integrity (OSI).

BACKGROUND INVESTIGATIONS

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information, shall undergo a

position sensitivity analysis based on the duties, outlined in the Position Designation Determination (PDD) for Contractor Personnel, each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI. Prospective Contractor employees shall submit the following completed forms to OSI through the COTR no less than 10 days after award of delivery order or 30 days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1. Standard Form 85P, "Questionnaire for Public Trust Positions"
2. DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement"
3. FD Form 258, "Fingerprint Card" (2 copies)
4. Form DHS-11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
5. Position Designation Determination for Contract Personnel Form
6. Foreign National Relatives or Associates Statement

Required forms will be provided by USCIS at the time of award of the contract. Only complete packages will be accepted by OSI. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive but unclassified information has resided in the US for three of the past five years, OSI may not be able to complete a satisfactory background investigation. In such cases, USCIS retains the right to deem an applicant as ineligible due to insufficient background information.

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to or development of any DHS IT system. USCIS will consider only U.S. Citizens for employment on this contract. USCIS will not approve LPRs for employment on this contract in any position that requires the LPR to access or assist in the development, operation, management or maintenance of DHS IT systems. By signing this contract, the contractor agrees to this restriction. In those instances where other non-IT requirements contained in the contract can be met by using LPRs, those requirements shall be clearly described.

EMPLOYMENT ELIGIBILITY

The Contractor must agree that each employee working on this contract will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to USCIS for acts and omissions of his own employees and for any Subcontractor(s) and their employees to include financial responsibility for all damage or injury to persons or property resulting from the acts or omissions of the contractor's employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or with this contract. The Contractor will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the COTR will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

USCIS reserves the right and prerogative to deny and/ or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom USCIS determines to present a risk of compromising sensitive but unclassified information to which he or she would have access under this contract.

The Contractor will report any adverse information coming to their attention concerning contract employees under the contract to USCIS OSI. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employees' name and social security number, along with the adverse information being reported.

OSI must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and building passes, or those of terminated employees to the COTR. If an identification card or building pass is not available to be returned, a report must be submitted to the COTR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card.

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OSI through the COTR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COTR and OSI shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COTR determine that the Contractor is not complying with the security requirements of this delivery order, the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

COMPUTER AND TELECOMMUNICATIONS SECURITY REQUIREMENTS

Security Program Background

The DHS has established a department wide IT security program based on the following Executive Orders (EO), public laws, and national policy:

- Public Law 107-296, Homeland Security Act of 2002.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.

- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Executive Order 12829, *National Industrial Security Program*, January 6, 1993.
- Executive Order 12958, *Classified National Security Information*, as amended.
- Executive Order 12968, *Access to Classified Information*, August 2, 1995.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001.
- National Industrial Security Program Operating Manual (NISPOM), February 2001.
- DHS Sensitive Systems Policy Publication 4300A v2.1, July 26, 2004
- DHS National Security Systems Policy Publication 4300B v2.1, July 26, 2004
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*.
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems (U)*, July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.
- Title 36 Code of Federal Regulations 1236, *Management of Vital Records*, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

GENERAL

Due to the sensitive nature of USCIS information, the contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The contractor's security program shall adhere to

the requirements set forth in the DHS Management Directive 4300 IT Systems Security Pub Volume 1 Part A and DHS Management Directive 4300 IT Systems Security Pub Volume I Part B. This shall include conformance with the DHS Sensitive Systems Handbook, DHS Management Directive 11042 Safeguarding Sensitive but Unclassified (For Official Use Only) Information and other DHS or USCIS guidelines and directives regarding information security requirements. The contractor shall establish a working relationship with the USCIS IT Security Office, headed by the Information Systems Security Program Manager (ISSM).

IT SYSTEMS SECURITY

In accordance with DHS Management Directive 4300.1 "Information Technology Systems Security", USCIS Contractors shall ensure that all employees with access to USCIS IT Systems are in compliance with the requirement of this Management Directive. Specifically, all contractor employees with access to USCIS IT Systems meet the requirement for successfully completing the annual "Computer Security Awareness Training (CSAT)." All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter.

CSAT can be accessed at the following: <http://otcd.uscis.dhs.gov/EDvantage.Default.asp> or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

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

SECURITY REVIEW

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 organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. 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 data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

The USCIS SDLC Manual documents all system activities required for the development, operation, and disposition of IT security systems. Required systems analysis, deliverables, and security activities are identified in the SDLC manual by lifecycle phase. The contractor shall assist the appropriate USCIS ISSO with development and completion of all SDLC activities and deliverables contained in the SDLC. The SDLC is supplemented with information from DHS and USCIS Policies and procedures as well as the National Institute of Standards Special

Procedures related to computer security and FISMA compliance. These activities include development of the following documents:

- *Sensitive System Security Plan (SSSP)*: This is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures. The SSSP shall be based upon the completion of the DHS FIPS 199 workbook to categorize the system of application and completion of the RMS Questionnaire. The SSSP shall be completed as part of the System or Release Definition Process in the SDLC and shall not be waived or tailored.
- *Privacy Impact Assessment (PIA) and System of Records Notification (SORN)*. For each new development activity, each incremental system update, or system recertification, a PIA and SORN shall be evaluated. If the system (or modification) triggers a PIA the contractor shall support the development of PIA and SORN as required. The Privacy Act of 1974 requires the PIA and shall be part of the SDLC process performed at either System or Release Definition.
- *Contingency Plan (CP)*: This plan describes the steps to be taken to ensure that an automated system or facility can be recovered from service disruptions in the event of emergencies and/or disasters. The Contractor shall support annual contingency plan testing and shall provide a Contingency Plan Test Results Report.
- *Security Test and Evaluation (ST&E)*: This document evaluates each security control and countermeasure to verify operation in the manner intended. Test parameters are established based on results of the RA. An ST&E shall be conducted for each Major Application and each General Support System as part of the certification process. The Contractor shall support this process.
- *Risk Assessment (RA)*: This document identifies threats and vulnerabilities, assesses the impacts of the threats, evaluates in-place countermeasures, and identifies additional countermeasures necessary to ensure an acceptable level of security. The RA shall be completed after completing the NIST 800-53 evaluation, Contingency Plan Testing, and the ST&E. Identified weakness shall be documented in a Plan of Action and Milestone (POA&M) in the USCIS Trusted Agent FISMA (TAF) tool. Each POA&M entry shall identify the cost of mitigating the weakness and the schedule for mitigating the weakness, as well as a POC for the mitigation efforts.
- *Certification and Accreditation (C&A)*: This program establishes the extent to which a particular design and implementation of an automated system and the facilities housing that system meet a specified set of security requirements, based on the RA of security features and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation). As appropriate the Contractor shall be granted access to the USCIS TAF and Risk Management System (RMS) tools to support C&A and its annual assessment requirements. Annual assessment activities shall include completion of the NIST 800-26 Self Assessment in TAF, annual review of user accounts, and annual review of the FIPS categorization. C&A status shall be reviewed for each incremental system update and a new full C&A process completed when a major system revision is anticipated.

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES

(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 5.5, September 30, 2007) 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.

CONTRACTOR EMPLOYEE ACCESS

(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 SSI," 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, and 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, sensitive information, or resources.

(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.

(1) 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 ASSURANCES

DHS Management Directives 4300 requires compliance with standards set forth by NIST, for evaluating computer systems used for processing SBU information. The Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards and applicable legislation and regulatory requirements. Systems shall offer the following visible security features:

- *User Identification and Authentication (I&A)* – I&A is the process of telling a system the identity of a subject (for example, a user) (*I*) and providing that the subject is who it claims to be (*A*). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All USCIS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the USCIS standard system in use at the time of a systems development.
- *Discretionary Access Control (DAC)* – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- *Object Reuse* – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- *Audit* – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the USCIS IT Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.

- *Banner Pages* – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

DATA SECURITY

SBU systems shall be protected from unauthorized access, modification, and denial of service. The Contractor shall ensure that all aspects of data security requirements (i.e., confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the DHS Sensitive Systems Handbook and USCIS policies and procedures. These requirements include:

- *Integrity* – The computer systems used for processing SBU shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated by either the sender or the receiver of the information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.
- *Confidentiality* – Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis and vulnerability assessment shall be performed to determine if threats to the SBU exist. If it exists, data encryption shall be used to mitigate such threats.
- *Availability* – Controls shall be included to ensure that the system is continuously working and all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.
- *Data Labeling* – The contractor shall ensure that documents and media are labeled consistent with the DHS *Sensitive Systems Handbook*.

19.0 Homeland Security Enterprise Architecture (HLS EA) Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as it relates to this Statement of Work. Specifically, the Contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware or software shall be compliant with the HLS EA Technology Reference Model (TRM) Standards and Products Profile.
- 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.

The Contractor shall provide, the full range of business and technical management services that assist in the development and implementation, of IT products and services that are compliant with the USCIS Enterprise Architecture, as well as the DHS Enterprise Architecture policies, procedures, guidelines, and directives (e.g., EA reference models, Investment Review Process). All IT products and services provided by the Contractor shall be subject to EA governance oversight performed by USCIS Office of Information Technology (OIT).

The contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirement:

- In compliance with OMB mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

20.0 List of Attachments

Attachment A – List of Existing Live-Scan Systems for Disposal and New Equipment for Installation, by USCIS Location

Attachment B – ASC Store and Forward Configurations

Attachment C – Biometrics Capture Flow Chart

Attachment D – Live-Scan Deployment Schedule

Attachment E – UKvisas Software Requirements

Attachment F – FBI Appendix F

Additional Delivery Order Terms and Conditions

52.252-2 Clauses Incorporated by Reference. (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address (es): <http://www.acquisition.gov/far>

(End of clause)

52.217-9 Option to Extend the Term of the Contract (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 3 years.

(End of clause)

52.251-1 Government Supply Sources (APR 1984)

The Contracting Officer may issue the Contractor an authorization to use Government supply sources in the performance of this contract. Title to all property acquired by the Contractor under such an authorization shall vest in the Government unless otherwise specified in the contract. Such property shall not be considered to be "Government-furnished property," as distinguished from "Government property." The provisions of the clause entitled "Government Property," except its paragraphs (a) and (b), shall apply to all property acquired under such authorization.

(End of clause)

Homeland Security Acquisition Regulation (HSAR) clauses and provisions incorporated by reference.

FAR clause 52.252-2, this contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of HSAR clauses may be accessed electronically at this internet address:

http://www.dhs.gov/xlibrary/assets/opnbiz/cpo_hsar_finalrule.pdf

3052.242-71 Dissemination of Contract Information (DEC 2003)

3052.242-72 Contracting officer's technical representative (DEC 2003)

Homeland Security Acquisition Regulation Clauses & Provisions in Full Text

3052.204-71, 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 SSI," 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, and 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, sensitive information, or resources.

(End of clause)

Performance Reporting

For active contracts valued in excess of simplified acquisition threshold, the Federal Acquisition Regulation (FAR) 42.1502 requires federal agencies to prepare Contractor performance evaluations. Performance evaluations are completed and forwarded to the Contractor for review within thirty (30) calendar days from the time the work under the contract is completed for each contract year. Interim evaluations by the Contracting Officer may be completed as necessary. The Contractor has thirty (30) days to reply with comments, rebutting statements, or additional information that will be made part of the official record.

Invoicing Requirements

The Statement of Work contains the invoicing requirement instructions. The invoice shall be sent via e-mail to the USCIS COTR and the USCIS Contracting Officer. The payment office address is as follows:

Dallas Finance Center
PO Box 561547
Dallas, TX 75356-1547

Advertisements, Publicizing Awards & News Releases

All Press releases or announcements about agency programs, projects, and contract awards need to be cleared by the Program Office and the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity news release or

commercial advertising without first obtaining explicit written consent to do so from the Program Office and the Contracting officer.

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

Organizational Conflict of Interest

(a) The Contractor warrants that, to the best of the Contractor's knowledge and belief, there are no relevant facts or circumstances which could give rise to an organizational conflict of interest, as defined in FAR Subpart 9.5, or that the Contractor has disclosed all such relevant information.

(b) Prior to commencement of any work, the Contractor agrees to notify the CO immediately that to the best of its knowledge and belief, no actual or potential conflict of interest exists or to identify to the CO any actual or potential conflict of interest the firm may have. In emergency situations, however, work may begin but notification shall be made within five (5) working days.

(c) The Contractor agrees that if an actual or potential organizational conflict of interest is identified during performance, the Contractor shall immediately make a full disclosure in writing to the CO. This disclosure shall include a description of actions which the Contractor has taken or proposes to take, after consultation with the CO, to avoid, mitigate, or neutralize the actual or potential conflict of interest. The Contractor shall continue performance until notified by the CO of any contrary action to be taken.

(d) Remedies – USCIS may terminate this contract for convenience, in whole or in part, if it deems such termination necessary to avoid organizational conflict of interest. If the Contractor was aware of a potential organizational conflict of interest prior to award or discovered an actual or potential conflict after award and did not disclose it or misrepresented relevant information to the CO, the Government may terminate the contract for default, debar the Contractor from Government contracting, or pursue such other remedies as may be permitted by law or this contract.

Contractor Employee Suitability Determinations

In accordance with the Security Requirements contained the Statement of Work, employees requiring USCIS Information System access for installation of images or system configuration require Suitability Determinations. The Security Requirement section of the SOW details the requirements of the Suitability Determinations. **To expedite processing of appropriate suitability documentation, contractor is required to submit documentation within 10 calendar days of award.**

HSSCCG-10-J-00034 ATTACHMENT A - List of USCIS Locations with Current Live-Scan Systems for Disposal and New Live-Scan Systems for Installation												
Type	Site Name	Site Code	Street	City	State	Zipcode	Disposal			Installation		
							Cabinet	Desktop	Mobile	Cabinet	Desktop	Mobile
NORTHEAST REGION												
DISTRICT 1												
SA	Boston	XBD	170 Portland St	Boston	MA	02114-1706	9			7		1
SA	Providence	XBF	105 Sockanosset Cross Rd, Suite 210	Cranston	RI	02920-5580	4			3		1
COLO	Manchester	XBG	803 Canal St	Manchester	NH	03101-1226	2			2		
COLO	Portland, ME	XPJ	176 Gannett Drive	South Portland	ME	04106-6909	1			2		
COLO	Lawrence	XBK	2 Mill Street	Lawrence	MA	01840-1602	2			2	1	
DISTRICT 2												
COLO	Buffalo	XBH	130 Delaware Ave	Buffalo	NY	14202-2498	2			2		1
COLO	Albany	XBI	1086 Troy-Schenectady Hwy	Latham	NY	12110-1024	2			2		
COLO	St. Albans, VT	XPK	64 Gricebrook Rd	St. Albans	VT	05478-9500	1			1	1	
SA	Hartford	XBE	467 Silver Lane	East Hartford	CT	06118-1104	4			3		1
COLO	Syracuse	XBJ	412 S. Warren St	Syracuse	NY	13202-2604	2			2		
DISTRICT 3												
SA	New Rochelle	XNG	246 North Ave	New Rochelle	NY	10801-6405	7			4	1	1
SA	Brooklyn	XNI	1250-1278 60th St	Brooklyn	NY	11219-4929	15			9	1	1
SA	Bronx	XNJ	1827 Westchester Ave	Bronx	NY	10472-3017	9			5	1	1
COLO	Manhattan	XNK	201 W Houston St. Street Entrance send mail & DHL to 201 Varick St, Suite 1023	New York	NY	10014-4811	11			7	1	
SA	Hicksville (Hempstead)	XNL	87 Bethpage Road	Hicksville	NY	11801-1503	6			4		1
SA	Queens/Jamaica	XNM	153-01 Jamaica Ave	Jamaica	NY	11432-4910	10			5	2	
SA	Woodside	XNN	63-05 Roosevelt Ave	Woodside	NY	11377-3841	9			6	1	1
DISTRICT 4												
SA	Elizabeth	XNO	285 North Broad St	Elizabeth	NJ	07206-2303	18			11	1	1
SA	Hackensack	XNP	116 Kansas Street, Main Floor	Hackensack	NJ	07601-7103	4			3		1
DISTRICT 5												
SA	Philadelphia	XPA	10300 Drummond Rd, Suite 100	Philadelphia	PA	19154-3804	9	1		6	1	1
SA	Pittsburgh	XPB	800 Penn Ave, Suite 101	Pittsburgh	PA	15222-3615	2			2		1
COLO	Charleston, WV	XPC	210 Kanawha Blvd West	Charleston	WV	25302-2201	1			1	1	
SA	Dover	XPD	250 Gateway South Blvd, Suites 260 & 270	Dover	DE	19901-4899	2	1		1	1	1
COLO	York	XPE	3400 Concord Rd, Old Farm House	York	PA	17402-9007	2			2		
DISTRICT 6												
SA	Baltimore	XBA	100 South Charles St, Suite 201	Baltimore	MD	21201-2701	6			4	1	1
SA	Glenmont	XBB	12331 Georgia Ave, Glenmont Plaza, Suite C	Wheaton	MD	20906-3646	7			4	1	1
SA	Salisbury	XBC	2040 Shipley Drive Suite C2	Salisbury	MD	21801-7874	1			1	1	1
DISTRICT 7												
SA	Alexandria	XDE	6850 Richmond Hwy, Suite 100	Alexandria	VA	22309-1586	11	1		8	1	1
SA	Norfolk	XDF	2500 Alameda Ave, Suite 114	Norfolk	VA	23513-2503	1	1		2		1

Type	Site Name	Site Code	Street	City	State	Zipcode	Cabinet	Desktop	Mobile	Cabinet	Desktop	Mobile
SOUTHEAST REGION												
DISTRICT 8												
SA	Atlanta	XAC	1255 Collier Road, Suite 100	Atlanta	GA	30318-2308	10	1		7	2	1
SA	Birmingham	XAB	529 Beacon Parkway, Suite 106	Birmingham	AL	35209-3126	2			2	1	1
SA	Charlotte	XAD	4801 Chastain Ave, Building 10, Suite 175	Charlotte	NC	28217-2231	5			3	1	1
COLO	Charleston, SC	XAE	1 Poston Rd, Suite 130 Parkshore Center	Charleston	SC	29407-3424	1	1		2		1
COLO	Raleigh	XAF	301 Roycroft Drive	Durham	NC	27703-8228	2	1		3	1	1
DISTRICT 9												
COLO	Hialeah	XMA	5880 NW 183rd St	Hialeah	FL	33015-6023	11			7	1	
COLO	Miami	XMB	8801 NW 7th Ave	Miami	FL	33150-2303	8			6	1	1
COLO	Kendall	XMC	14675 SW 120th St	Miami	FL	33186	7			5	1	
COLO	Oakland Park	XMD	4451 NW 31st Ave	Oakland Park	FL	33308	8			5	1	
ASC	San Juan	XPM	Metro Office Park TLD Building, 2nd Street, Suite 200	Guaynabo	PR	00968	3			2	1	1
COLO	St. Thomas	XPO	8000 Nisky Center, Suite 1A, Lower Level South, 1st Floor	S St. Thomas	VI	00802-5838	1			1	1	
COLO	St. Croix	XPP	5-8A Sunny Isle Shopping Center, Christiansted	St. Croix USVI	VI	00821-1468	1			1	1	
DISTRICT 10												
SA	Tampa	XMF	9325 Bay Plaza Blvd, Suite 215	Tampa	FL	33619-4463	6			4	1	1
SA	Orlando	XME	5449 S. Semoran Blvd, #18C	Orlando	FL	32822-1778	5	1		4	1	1
COLO	Jacksonville	XMG	4121 Southpoint Blvd.	Jacksonville	FL	32216-0930	2	2		3		
COLO	West Palm Beach	XMH	2711 Exchange Ct	W Palm Beach	FL	33409-4017	5	1		4	1	1
SA	Fort Myers	XMJ	3850 Colonial Blvd, Suite 100	Fort Myers	FL	33968	2			2	1	1
DISTRICT 11												
COLO	New Orleans	XMA	2424 Edenborn Ave, Suite 300	Metairie	LA	70001-1845	0	2		2	1	1
COLO	Fl. Smith	XNB	4977 Old Greenwood Rd	Fl. Smith	AR	72903-6906	1			1	1	
COLO	Jackson, MS	XNC	100 W. Capitol St, Suite 727	Jackson	MS	39269-1602	1			1	1	
COLO	Memphis	XND	842 Virginia Run Cove	Memphis	TN	38122-4419	2	1		2	1	1
SA	Nashville	XNE	1400 Donelson Pike, Suite B-13	Nashville	TN	37217-0000	2	1		2	1	1
CENTRAL REGION												
DISTRICT 12												
COLO	Detroit	XDK	11411 East Jefferson Ave	Detroit	MI	48214-3332	4	2		4	1	1
SA	Grand Rapids	XDM	4484 Breton Rd	Kentwood	MI	49608-5270	4			2	1	1
DISTRICT 13												
COLO	Cleveland	XCI	1240 E 9th St, Room 1259	Cleveland	OH	44199-2085	3			2		1
COLO	Cincinnati	XCJ	550 Main St, Room 1524	Cincinnati	OH	45202-5298	2	1		2		1
SA	Columbus	XCK	50 W. Broad St, Suite 650	Columbus	OH	43215-5903	3			2		1
COLO	Louisville	XNF	601 W. Broadway, Room 22	Louisville	KY	40202-2250	2			2		1
COLO	Indianapolis	XCG	950 N. Meridian St, Room 400	Indianapolis	IN	46204-3915	2	1		2		

Type	Site Name	Site Code	Street	City	State	Zipcode	Cabinet	Desktop	Mobile	Cabinet	Desktop	Mobile
DISTRICT 14												
SA	Normal	XCA	4701 N. Cumberland, 1-3 BCD	Normal	IL	60708-2905	5			3	1	1
SA	Pulaski	XCB	5180 S. Pulaski Rd, Suite 101	Chicago	IL	60632-4253	5	1		3	1	1
SA	Broadway	XCC	4853 N. Broadway	Chicago	IL	60640-3603	5	1		3	1	1
SA	Naperville	XCD	888 South Route 59, Suite 124	Naperville	IL	60540-0962	5			3	1	1
SA	Waukegan	XCE	25 S. Greenbay Rd	Waukegan	IL	60085-4815	4			2	1	1
SA	Michigan City	XCF	284 Dunes Plaza	Michigan City	IN	46360-7340	3			2	1	1
COLO	Milwaukee	XCH	310 E. Knapp St, Room 154	Milwaukee	WI	53202-4504	3	1		3		
DISTRICT 15												
COLO	Kansas City	XKA	9747 N. Constant Ave	Kansas City	MO	64153-1833	2	1		2	1	1
COLO	Wichita	XKB	271 W. 3rd St. North, Suite 1050	Wichita	KS	67202-1212	1			1	1	
COLO	St. Louis	XKC	1222 Spruce St, Room 1.208	St. Louis	MO	63103-2815	2	2		2	1	1
COLO	Omaha	XKA	1717 Avenue H	Omaha	NE	68110-2752	2			2		
COLO	Des Moines	XOB	210 Walnut St, Room 949	Des Moines	IA	50309-2110	2			2		1
SA	St. Paul	XSI	1360 University Ave	St. Paul	MN	55104-4086	4			3	1	1
SA	Rapid City	XSJ	2255 Haines Ave, Suite 214	Rapid City	SD	57701-0411	1			1	1	
COLO	Fargo	XSK	657 2nd Ave. North, Room #248	Fargo	ND	58102-4727	1			1	1	
COLO	Sioux Falls	XSL	300 E. 8th St	Sioux Falls	SD	57103-7023	1			1	1	
COLO	Duluth	XSM	515 W. First St, Suite 208	Duluth	MN	55802-1301	1			1	1	
DISTRICT 16												
SA	Dallas North	XDA	10051 Whitehurst Dr, Suite 200	Dallas	TX	75243-0637	5	1		4	1	1
SA	Fl. Worth	XDB	4200 S. Freeway, Suite 1309	Fl. Worth	TX	76115-1400	3	2		3	1	1
SA	Lubbock	XDC	3502 Slide Rd, Suite A-24	Lubbock	TX	79414-2547	2			2		1
COLO	Oklahoma	XDD	4400 S.W. 44th St, Suite A	Oklahoma City	OK	73119-2800	1	1		2		1
SA	Dallas South	XDL	7334 South Westmoreland Rd	Dallas	TX	75237-2908	3			2	1	1
DISTRICT 17												
SA	Houston SE	XHH	8505 Gulf Freeway, Suite A	Houston	TX	77017-5043	5			3	2	1
SA	Houston SW	XHI	11777 State Hwy 8 South	Sugar Land	TX	77498-5721	5	1		4	1	1
SA	Houston NW	XHU	10555 Northwest Freeway, Suite 150	Houston	TX	77062-8209	4	1		4		1
DISTRICT 18												
SA	San Antonio	XSA	5121 Crestway, Suite 112	San Antonio	TX	78239-1975	4	1		3	1	1
SA	Austin	XSN	Parkline Plaza Shopping Center 11301 Lakeline Blvd, Suite 150	Austin	TX	78717	2			2	1	1
SA	Laredo	XDX	707 E. Calton Rd, Suite 301	Laredo	TX	78041-3638	2			3		1
SA	El Paso	XEA	10500 Montwood	El Paso	TX	79935-2703	4			3		1
SA	Albuquerque	XEC	1605 Isleta Blvd SW, Suite C	Albuquerque	NM	87105-4793	2			2		1
SA	McAllen	XHA	220 South Bicentennial, Suite C	McAllen	TX	78501-7051	3			2	1	1
COLO	Haringen	XHB	1717 Zoy St	Haringen	TX	78552-3220	2			2		

Type	Site Name	Site Code	Street	City	State	Zipcode	Cabinet	Desktop	Mobile	Cabinet	Desktop	Mobile
DISTRICT 18												
SA	Denver	XDG	15037 E. Colfax Ave. Unit G	Aurora	CO	80011-6777	5			4	1	1
SA	Grand Junction	XDH	2454 Hwy 6 and 50, Valley Plaza, Suite 115	Grand Junction	CO	81505-1111	1			1	1	1
COLO	Casper	XDI	150 East B St, Room 1014	Casper	WY	82601-7005	1			1	1	1
SA	Salt Lake City	XDJ	6636 S. 1900 West St, Bldg C	Taylorville	UT	84118-9007	3			2	1	1
COLO	Helena	XHC	2900 Skyway Dr	Helena	MT	59602-1230	1			1	1	1
COLO	Boise	XHD	1185 South Vinnell Way	Boise	ID	83709-1656	1			1	1	1
SA	Idaho Falls	XHE	2265 W. Broadway, Suite A	Idaho Falls	ID	83402-2996	1			1	1	1
WESTERN REGION												
DISTRICT 20												
COLO	Seattle	XSE	12500 Tukwila International Blvd	Seattle	WA	98168-2506	6	1		4	2	1
COLO	Spokane	XSF	920 West Riverside, Room 691	Spokane	WA	99201-1090	1			1	1	1
COLO	Yakima	XSH	415 N. 3rd St	Yakima	WA	98901-2331	1	1		2		
COLO	Anchorage	XAA	620 E. 10th Ave, Suite 106	Anchorage	AK	99501-3799	1			1	1	1
SA	Portland, OR	XPL	721 SW 14th Ave	Portland	OR	97205-1840	4	1		3	1	1
DISTRICT 21												
SA	San Francisco	XTD	250 Broadway	San Francisco	CA	94111-1506	9			5	1	1
SA	Oakland	XFB	2040 Telegraph Ave	Oakland	CA	94612-2306	9	1		6	1	1
SA	Santa Rosa	XFC	1401 Guerneville Rd, Room 100	Santa Rosa	CA	95403-4174	3			2		1
SA	Salinas	XFD	1854 N. Main St	Salinas	CA	93906-2305	2			2		1
SA	San Jose	XTE	122 Charcot Ave	San Jose	CA	95131-1101	7			5	1	1
DISTRICT 22												
SA	Sacramento	XFE	825 Riverside Pkwy, Suite 100	West Sacramento	CA	95605-1502	6	1		4	1	1
SA	Modesto	XFF	901 N. Carpenter Rd, Suite 14	Modesto	CA	95351-1199	4			2	1	1
SA	Fresno	XFG	4883 E. Kings Canyon	Fresno	CA	93727-3811	6			3	1	1
SA	Bakersfield	XFI	14701 Plantz Rd, Suite A12	Bakersfield	CA	93309-6349	2	1		2	1	1
DISTRICT 23												
SA	Pomona	XLB	435 W. Mission Blvd, Suite 110	Pomona	CA	91766-1601	3			2	1	1
SA	El Monte	XLC	9251 Garvey Ave, Suite Q	S. El Monte	CA	91733-4611	11			7		1
SA	Gardena	XLD	15715 Crenshaw Blvd, Room B-112	Gardena	CA	90249-4529	7			4	1	1
SA	Van Nuys	XLE	14615 Hamlin St, Suite 200	Van Nuys	CA	91411-1608	11			7	1	1
SA	Bellflower	XLF	17610 Bellflower Blvd, Suite A110	Bellflower	CA	90705-8002	5			3	1	1
SA	Fairfax	XLG	5949 West Pico Blvd	Fairfax	CA	90035-2653	4			4		1
SA	Santa Ana	XLH	1666 N. Main St, Suite 100A	Santa Ana	CA	92701-7417	8			4	1	1
SA	Buena Park	XLJ	8381 La Palma Ave, Suite A	Buena Park	CA	90620-3207	6			3	1	1
SA	Riverside	XLK	10082 Magnolia Ave	Riverside	CA	92503-3530	9			5	1	1
SA	Oxnard	XLK	2000 Outlet Center Drive, Suite 200	Oxnard	CA	93036-0609	4			3	1	1
SA	Goleta	XLL	6831-B Hollister Ave	Goleta	CA	93117-3015	3			0		1
SA	Wilshire	XLN	1015 Wilshire Blvd	Los Angeles	CA	90017-2602	9			5	1	1

Type	Site Name	Site Code	Street	City	State	Zipcode	Cabinet	Desktop	Mobile	Cabinet	Desktop	Mobile
DISTRICT 24												
SA	San Diego	XSB	1261 Third Ave, Suite H	Chula Vista	CA	91911-3262	5	2		4	1	1
SA	San Marcos	XSC	727 W. San Marcos Blvd, Suite 101-103	San Marcos	CA	92078-1244	4			3		1
COLO	Imperial	XSD	509 Industry Way	Imperial	CA	92251-7503	2			2		
DISTRICT 25												
SA	Phoenix	XPO	2545 E. Thomas Rd	Phoenix	AZ	85016-7941	8	1		5	2	1
SA	Las Vegas	XPF	6175 S. Pecos Rd	Las Vegas	NV	89120-6284	2	2		4		1
SA	Tucson	XPG	1835 S. Alvernon, Suite 216	Tucson	AZ	85711-6693	3			2		1
COLO	Reno	XPH	1351 Corporate Blvd	Reno	NV	89502-7146	1	1		2		
SA	Yuma	XPI	3250 S. 4th Avenue, Suite E	Yuma	AZ	85365-4051	1			1	1	1
DISTRICT 28												
SA	Honolulu	XHF	677 Ala Moana Blvd, Suite 102 & 103	Honolulu	HI	96813-4999	3	1		2	1	1
COLO	Aqana	XHG	Sirena Plaza, 108 Herman Cortez Ave, Suite 100	Honolulu	GU	96910-5009	1			1	1	1
SA	Saipan	XHS	TSL Plaza Building, Beach Rd South	Gaerpen	MP	MP-96950	1			1	1	1
USCIS	ASC Lab	HQ					544	45		399	98	98
USCIS	Image Lab	HQ					1		12	1	1	1
										0	1	1
Current Total							545	45	12	400	100	100
Total Available										400	100	100
Number of Sites =		134										

ASC STORE AND FORWARD CONFIGURATIONS

ASC Software:

Microsoft Windows 2003 Server
Microsoft SMTP
POP3
Query and Report software not required; use Crystal Reports executables

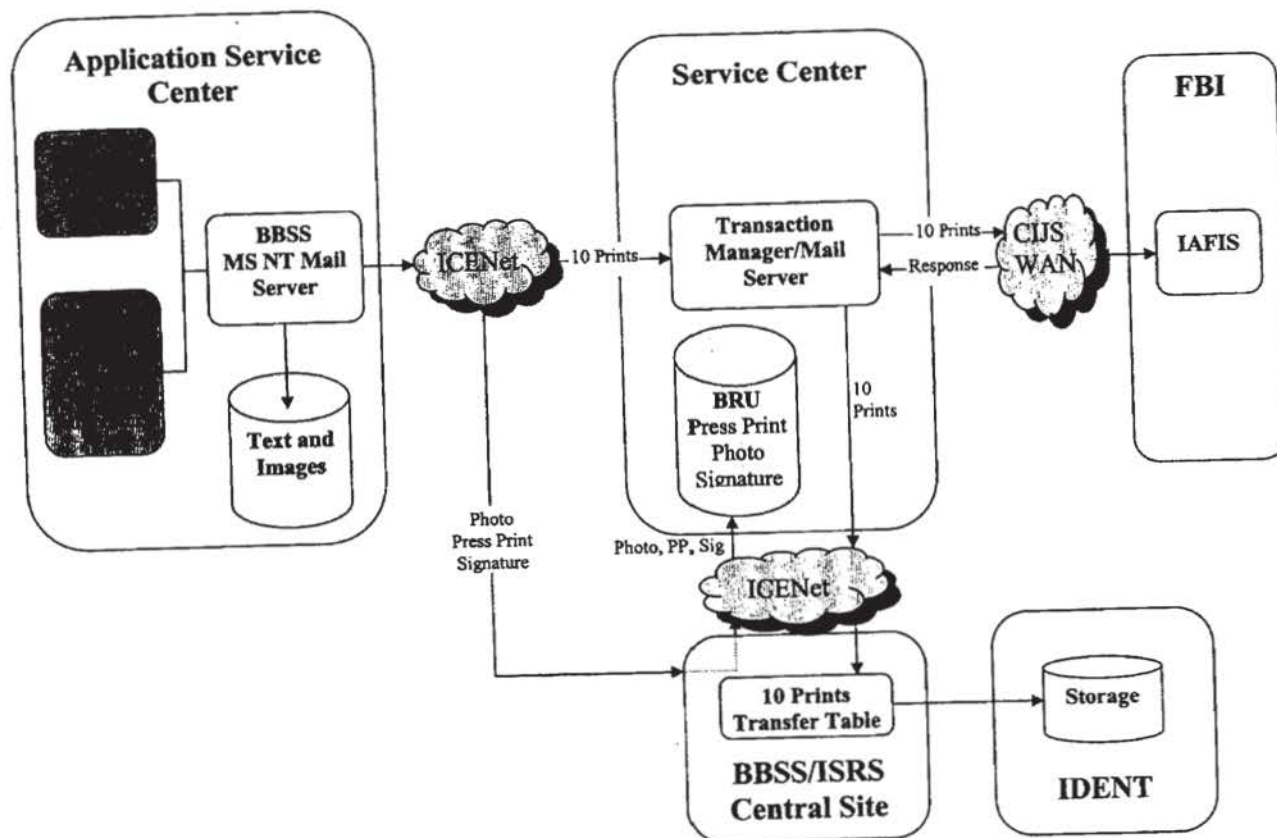
ASC Hardware:

Dell PowerEdge Server (typically 2950)
4 GB RAM
8 GB Hot Swappable RAID 5 storage (at least 14GB at larger ASCs)
CD-ROM
100 Base-T NIC
Monitor

Data Storage Requirements:

ASC Size:

Largest ASC 7GB
Medium ASC 4GB
Smallest ASC <1GB



Type	Site Name	Site Code	Address	City	ST	Zip	Cabinet	Desk top	Mobile	Total to be Installed	Day	Notes
COLO	Detroit	XDK	11411 East Jefferson Ave	Detroit	MI	48214-3332	4	1	1	5	1 & 2	
SA	Boston	XBD	120 Portland St	Boston	MA	02114-1705	2		1	7	1 & 2	
COLO	Cleveland	XBK	2 MRI Street	Lakewood	MA	01840-1902	2	1		3	3	
SA	Grand Rapids	XDM	4454 Byron Rd	Kentwood	MI	49508-5270	2	1	1	3	3	
SA	Providence	XBF	109 South Main Street, Room 210	Cranston	RI	02920-5560	3		1	3	4	
COLO	Cleveland	XCI	1240 E 9th St, Room 1259	Cleveland	OH	44189-2095	2		1	2	4 & 5	
COLO	Manchester	XBG	803 Canal St	Manchester	NH	03101-1226	2			2	5	
		# SITES Scheduled WK 1 - 12	3 North East Region 3 South East Region 3 Central Region 3 Western Region	Total # sites Scheduled to date	12				# Machines Installed WK 1	45	CUMMULATIVE	45
COLO	Portland, ME	XBU	178 Gehring Drive	South Portland	ME	04108-9909	2			2	6	
SA	Columbus	XCK	50 W. Broad St, Suite 650	Columbus	OH	43215-9903	2		1	2	6	
COLO	Buffalo	XBH	1300 Delaware Ave	Buffalo	NY	14202-2696	2		1	2	7	
COLO	Cincinnati	XCU	550 Main St, Room 1524	Cincinnati	OH	45202-5298	2		1	2	7	
COLO	Albany	XBI	1088 Troy Schenck Rd Hwy	Latham	NY	12110-1024	2		1	2	8	
COLO	Louisville	XBF	601 W. Broadway, Room 22	Louisville	KY	40202-2250	2		1	2	8	
COLO	St Albans, VT	XPK	84 Oriskany Rd	St Albans	VT	05478-9900	1	1		2	9	
COLO	Indianapolis	XCG	650 N. Meridian St, Room 400	Indianapolis	IN	46204-3915	2			2	9	
SA	Hartford	XBR	457 Silver Lane	East Hartford	CT	06118-1104	3		1	3	10	
SA	Michigan City	XCF	284 Dunes Plaza	Michigan City	IN	46360-7340	2	1	1	3	10 & 11	
		# SITES Scheduled WK 2 - 15	5 North East Region 3 South East Region 5 Central Region 2 Western Region	Total # sites Scheduled to date	27				# Machines Installed Wk 2	48	CUMMULATIVE	93
COLO	Syracuse	XBU	412 S. Warren St	Syracuse	NY	13202-2604	2			2	11	
SA	Norridge	XCA	4701 N. Cumberland, 1-3 BCD	Norridge	IL	60708-2905	3	1	1	4	12 & 13	
SA	New Rochelle	XNG	248 North Ave	New Rochelle	NY	10801-0405	4	1	1	5	12 & 13	
										7	12 & 13	
SA	Pleasant	XCB	5100 S. Pleasant Rd, Suite 101	Chicago	IL	60632-4293	3	1	1	4	14 & 15	
SA	Brooklyn	XNJ	1250-1273 60th St	Brooklyn	NY	11219-4929	9	1	1	10	14 & 15	
		# Sites Scheduled WK 3 - 10	3 North East Region 2 South East Region 2 Central Region 3 Western Region	Total # sites Scheduled to date	37				# Machines Installed WK 3	47	CUMMULATIVE	140
SA	Broadway	XCC	4653 N. Broadway	Chicago	IL	60640-3603	3	1	1	4	16 & 17	
SA	Brooklyn	XNU	1627 West 10th St	Brooklyn	NY	10472-3017	5	1	1	6	16 & 17	
										5	16 & 17	
SA	Nashville	XCD	1866 South Route 69, Suite 124	Nashville	IL	60540-0982	3	1	1	4	18 & 19	

Type	Site Name	Site Code	Address	City	ST	Zip	Cabinet	Desk top	Mobile	Total to be Installed	Day	Notes
COLO	Manhattan	XNN	201 W. Houston St. Great Entrance and mail in	New York	NY	10014-4511	7	1		8	18 & 19	
SA	Waukegan	XCE	25 S. Greenway Rd	Waukegan	IL	60085-4815	2	1	1	3	20 & 21	
SA	Hickoryville (Hammetts)	XNL	878 Bathpage Road	Hickoryville	NY	14801-1503	4	2	1	4	20 & 21	
		# Sites Scheduled WK 4 - 12	3 North East Region 3 South East Region 3 Central Region 3 Western Region	Total # sites Scheduled to date	49				WK 4	59	CUMMULATIVE	199
COLO	Milwaukee	XCH	310 E. Knepp St. Room 154	Milwaukee	WI	53202-4504	3			3	22	
SA	Queens/Manhattan	XNM	155 Old Jerusalem Ave	Jamaica	NY	11432-4610	5	2		7	22 & 23	
SA	St. Paul	XSI	1360 University Ave	St. Paul	MN	55104-4066	3	1	1	4	23 & 24	
SA	Woodstock	XNN	6306 Roosevelt Ave	Woodstock	NY	11377-3641	8	1	1	7	24 & 25	
COLO	Duluth	XSM	515 W. First St. Suite 208	Duluth	MN	55802-1901	1	1		2	25 & 26	
		# Sites Scheduled WK 5 - 10	2 North East Region 2 South East Region 3 Central Region 3 Western Region	Total # sites Scheduled to date	58				WK 5	39	CUMMULATIVE	238
SA	Elizabeth	XND	285 North Broad St	Elizabeth	NJ	07208-2303	11	1	1	12	26 & 27 & 28	
COLO	Fargo	XSK	657 2nd Ave. North, Room #248	Fargo	ND	58102-4727	1	1		2	27 & 28	
SA	Hackensack	XND	1166 Keniloe Street, Main Floor	Hackensack	NJ	07601-27103	3		1	3	29	
SA	Rapid City	XSI	2255 Haines Ave. Suite 214	Rapid City	SD	57701-0411	1	1		2	29 & 30	
SA	Philadelphia	XPA	10300 Chestnut Rd. Suite 100	Philadelphia	PA	19154-3804	8	1	1	7	30 & 31	
		# Sites Scheduled WK 6 - 10	3 North East Region 3 South East Region 2 Central Region 2 Western Region	Total # sites Scheduled to date	68				WK 6	46	CUMMULATIVE	284
COLO	Sioux Falls	XSI	300 E. 8th St	Sioux Falls	SD	57103-7023	1	1		2	31 & 32	
SA	Pittsburgh	XPS	600 Penn Ave. Suite 101	Pittsburgh	PA	15222-3815	2		1	2	32	
COLO	Chattanooga, WV	XPC	210 Knoxville Blvd. West	Chattanooga	WV	25302-2201	1	1		2	33	
COLO	Des Moines	XOB	210 Walnut St. Room 949	Des Moines	IA	50309-2110	2		1	2	33 & 34	
SA	Dover	XPD	280 S. New York St. Bldg. 200 & 270	Dover	DE	19901-1000	1	1	1	2	34	
COLO	York	XPE	3400 Concord Rd. Old Farm House	York	PAS	17402-9007	2			2	35	
COLO	Omaha	XOA	1717 Avenue H	Omaha	NE	68110-2752	2			2	35 & 36	

Type	Site Name	Site Code	Address	City	ST	Zip	Cabinet	Desk top	Mobile	Total to be Installed	Day	Notes
		# Sites Scheduled WK 7 - 13	4 North East Region 3 South East Region 3 Central Region 3 Western Region	Total # sites Scheduled to date	82				WK 7	36	CUMMULATIVE	320
SA	Baltimore	XBA	1000 South Chelton St, Suite 201	Baltimore	MD	21201-2701	4	1	1	5	35 & 37	
COLO	Kansas City	XKA	9747 N. Conant Ave	Kansas City	MO	64153-1833	2	1	1	3	37 & 38	
SA	Overland Park	XOB	14337 22nd St, Suite 200	Overland Park	KS	66206-3446	4	1	1	5	38 & 39	
COLO	St. Louis	XOC	1222 Spruce St, Room 1-200	St. Louis	MO	63103-2815	2	1	1	3	39 & 40	
SA	Salisbury	XBO	2040 Bishop Drive, Suite C2	Salisbury	MD	21801-7874	1	1	1	2	40	
		# Sites Scheduled WK 8 - 9	3 North East Region 2 South East Region 2 Central Region 2 Western Region	Total # sites Scheduled to date	91				WK 8	36	CUMMULATIVE	356
COLO	Wichita	XKB	271 W. 3rd St, North, Suite 1050	Wichita	KS	67202-1212	1	1	1	2	41 & 42	
SA	Alameda	XDB	5500 Richmond Hwy, Suite 100	Alameda	VA	22304-1536	6	1	1	9	41 & 42 & 43	
SA	Denver	XDG	15037 E. Colfax Ave, Unit G	Denver	CO	80011-5777	4	1	1	5	42 & 43	
SA	Dallas North	XDA	10061 Whitehurst Dr, Suite 200	Dallas	TX	75243-0637	4	1	1	5	43 & 44	2nd Central Team
SA	Houston SE	XDE	2500 Alameda Drive, Suite 114	Houston	TX	77062-2503	2	1	1	2	44	
SA	Grand Junction	XDH	2454 Hwy 5 and 50, Valley Plaza, Suite 115	Grand Junction	CO	81506-1111	1	1	1	2	44 & 45	
SA	Dallas South	XDL	7334 South Westmontland Rd	Dallas	TX	75237-2908	2	1	1	3	45	2nd Central Team
		# Sites Scheduled WK 9 - 12	2 North East Region 1 South East Region 5 Central Region 4 Western Region	Total # sites Scheduled to date	103				WK 9	48	CUMMULATIVE	404
SA	Fl. Worth	XDB	4200 S. Freeway, Suite 1309	Fl. Worth	TX	76115-1400	3	1	1	4	46	2nd Central Team
SA	Salt Lake City	XDU	5538 S. 1900 West St, Bldg C	Taylorsville	UT	84116-9007	2	1	1	3	46 & 47	
SA	Lubbock	XDC	3502 Slide Rd, Suite A-24	Lubbock	TX	79414-2547	2	1	1	2	47 & 48	2nd Central Team
COLO	Casper	XDI	150 East B St, Room 1014	Casper	WY	82601-7005	1	1	1	2	48 & 49	
COLO	Oklahoma	XDD	4400 S.W. 44th St, Suite A	Oklahoma City	OK	73119-2800	2	1	1	2	49 & 50	2nd Central Team
SA	Idaho Falls	XHE	2205 W. Broadway, Suite A	Idaho Falls	ID	83402-2995	1	1	1	2	50 & 51	
		# Sites Scheduled WK 10 - 9	5 Central Region 3 Western Region	Total # sites Scheduled to date	112				WK 10	32	CUMMULATIVE	436
SA	Houston SE	XDH	10555 Northwest Freeway, Suite 150	Houston	TX	77092-8209	3	2	1	5	51 & 52	2nd Central Team
COLO	Boise	XHO	1185 South Vinnell Way	Boise	ID	83709-1656	1	1	1	2	52 & 53	
SA	Houston NW	XHU	10555 Northwest Freeway, Suite 150	Houston	TX	77092-8209	4	1	1	4	53 & 54	2nd Central Team
COLO	Helena	XHC	2800 Skyway Dr	Helena	MT	59602-1230	1	1	1	2	54 & 55	
SA	Houston SW	XHI	11777 State Hwy 6 South	Sugar Land	TX	77498-5721	4	1	1	5	55 & 56	2nd Central Team

[illegible]

Type	Site Name	Site Code	Address	City	ST	Zip	Cabinet	Desktop	Mobile	Total to be Installed	Number of Days	Day	Notes
NORTHEAST REGION							INSTALL	INSTALL	STORE				
DISTRICT 1													
SA	Boston	XBD	170 Portland St	Boston	MA	02114-1708	7		1	7	2	Day 1 & 2	
SA	Providence	XBF	105 Sockanosset Cross Rd, Suite 210	Cranston	RI	02920-5560	3		1	3	1	Day 4	
COLO	Manchester	XBG	803 Canal St	Manchester	NH	03101-1226	2			2	1	Day 5	
DISTRICT 2													
COLO	Buffalo	XBH	130 Delaware Ave	Buffalo	NY	14202-2498	2		1	2	1	Day 7	
COLO	Albany	XBI	1086 Troy-Schenectady Hwy	Latham	NY	12110-1024	2			2	1	Day 8	
SA	Hartford	XBE	467 Silver Lane	East Hartford	CT	06118-1104	3		1	3	1	Day 10	
COLO	Syracuse	XBJ	412 S. Warren St	Syracuse	NY	13202-2604	2			2	1	Day 11	
DISTRICT 3													
SA	New Rochelle	XNG	246 North Ave	New Rochelle	NY	10801-6405	4	1	1	6	1	Day 12 & 13	
SA	Brooklyn	XNI	1260-1278 60th St	Brooklyn	NY	11219-4928	9	1	1	10	3	Day 14 & 15	
SA	Bronx	XNJ	1827 Westchester Ave	Bronx	NY	10472-3017	5	1	1	6	2	Day 16 & 17	
COLO	Manhattan	XNK	201 W Houston St. Street Entrance send mail & DHL to 201 Varick St. Suite 1023	New York	NY	10014-4811	7	1		8	2	Day 18 & 19	
SA	Hicksville (Hempstead)	XNL	87 Bethpage Road	Hicksville	NY	11801-1503	4		1	4	1	Day 20 & 21	
SA	Queens/Jamaica	XNM	153-01 Jamaica Ave	Jamaica	NY	11432-4910	5	2		7	2	Day 22 & 23	
SA	Woodside	XNN	63-05 Roosevelt Ave	Woodside	NY	11377-3641	6	1	1	7	2	Day 24 & 25	
DISTRICT 4													
SA	Elizabeth	XNO	285 North Broad St	Elizabeth	NJ	07208-2303	11	1	1	12	3	Day 26 & 27 & 28	
SA	Hackensack	XNP	116 Kansas Street, Main Floor	Hackensack	NJ	07601-7103	3		1	3	1	Day 29	
DISTRICT 5													
SA	Philadelphia	XPA	10300 Drummond Rd, Suite 100	Philadelphia	PA	19154-3804	6	1	1	7	2	Day 30 & 31	
SA	Pittsburgh	XPB	800 Penn Ave, Suite 101	Pittsburgh	PA	15222-3615	2		1	2	1	Day 32	
SA	Dover	XPD	250 Gateway South Blvd, Suites: 260 & 270	Dover	DE	19901-4699	1	1	1	2	1	Day 34	
COLO	York	XPE	3400 Concord Rd, Old Farm House	York	PA	17402-9007	2			2	1	Day 35	
DISTRICT 6													
SA	Baltimore	XBA	100 South Charles St, Suite 201	Baltimore	MD	21201-2701	4	1	1	5	2	Day 36 & 37	
SA	Glenmont	XBB	12331 Georgia Ave, Glenmont Plaza, Suite C	Wheaton	MD	20906-3646	4	1	1	5	2	Day 38 & 39	
DISTRICT 7													
SA	Alexandria	XDE	8650 Richmond Hwy, Suite 100	Alexandria	VA	22309-1586	8	1	1	9	3	Day 41 & 42 & 43	
SA	Norfolk	XDF	2500 Alameda Ave, Suite 114	Norfolk	VA	23513-2503	2		1	2	1	Day 44	
SOUTHEAST REGION							111	17		128	44		

HSSCCG-10-J-00034 - ATTACHMENT E

UKvisas Software Requirements

1 Background

UKvisas has embarked on a global rollout of biometric capabilities to record fingerprints and photographs for all UK visa applicants (with limited exceptions and exemptions) since December 2008. This element of the application process requires visa applicants to physically present themselves so their biometrics can be recorded. UKvisas has been aware of the network of Department of Homeland Security (DHS) Application Support Centers (ASCs) in place for similar biometric recording for US immigration purposes.

In September 2006, Tony Mercer, Director UKvisas Network Operations, formally wrote to Stewart Baker, DHS Assistant Secretary for Policy, requesting formal exploration and analysis for UKvisas use of the ASCs for UK visa applicants to appear for fingerprinting and photograph recording.

In November 2006, Stewart Baker responded positively with agreement to conduct a joint feasibility or viability report considering the legal, policy, cost, technical, and operational factors as a determination and basis for future agreements for UKvisas use of the ASCs.

A joint viability report has been concluded between UKvisas and DHS as agreed to in above referenced letters. The viability report analysis has identified significant benefits for DHS and UKvisas through the use of ASCs and the data sharing opportunities this presents. Both UKvisas and DHS have committed to the implementation of Phase 1a identified in the viability report by November 30, 2007. Phase 1a includes the joint enrolment capabilities for UK visa applicants to appear at ASCs for biometric enrolment and the data being transmitted by DHS to UKvisas.

2 UKvisas Software Requirements

2.1 Introduction

The Live-Scan software is to: 1) include a screen to be used for processing UKvisas applicants, 2) include required data fields necessary for submitting UKvisas applicant information, 3) capture digital photographs, and 4) be capable of recording and enrolling all the data necessary for submission to the UK Immigration and Asylum Fingerprint System (IAFS).

The ASC enrolment software must be capable of enrolling the following data for UK visa applicants age five (5) and older:

- UKvisas Global Web Form (GWF) number

- Minimum enrolment set (family name, other names, date of birth, sex, passport number, and nationality)
- Exemption/Exception details
- Fingerprints
- Digital photo
- Audit data

The following requirements will need to be satisfied in the development of the ASC software for processing UK visa applicants.

2.2 General Requirements

- R1 Biometric recording shall be record-centric. For each applicant the operator shall be able to create a new biometric submission file to be populated with biometrics and biographic data.
- R2 The operator shall have capability to cancel or void a record at any stage prior to confirmation and submission of the record.
- R3 Only one record shall be open at one time per ASC workstation.
- R4 When the enrolment set is complete the software shall prompt the operator to confirm that they are content for the data set to be submitted. Once the operator has confirmed the software shall lock the record and begin the process for transmitting data to UKvisas.
- R5 The software shall not allow the biometric or biographic details to be edited or accessed once confirmed by the operator.
- R6 Each record shall be date/time stamped on creation. Standard format and time zone for date/time stamp to be agreed between UKvisas and DHS.
- R7 The software shall allow for the creation of metadata relating to each enrolment set. Examples include the enrolment post, the enrolment workstation, the operator's log on ID, time stamp etc. This data will be used for Management Information (MI) purposes as well as for IAFIS and is identified in detail in later sections.
- R8 In the event that a network connection is not available, the software shall be capable of locally storing records in a secure manner.
- R9 The software shall submit all locally stored records immediately following a network connection being re-established.
- R10 The software shall allow operators to re-take fingerprints where necessary prior to submission, but only up until the point the operator confirms the record to lock and submit the data.

- R11 The software shall have capability to identify and flag the record as an UK visa applicant for appropriate processing different than DHS applicants.

2.3 Login Requirements

UKvisas accepts that the current requirements for the ASC personnel to login and authenticate their use of the software are more than likely adequate, however UKvisas desires the following minimal requirements are met:

- R12 The software shall restrict access to its function to operators that successfully authenticate themselves by username and password.
- R13 All actions by system administrators regarding UKvisas records shall be logged for auditing purposes.

2.4 Minimum Data Set Entry Requirements

- R14 The software shall accept the minimum data set for biometric enrolment including GWF, Family name, Other Names, Date of Birth, Sex, Travel Document Number, and Nationality.
- R15 The software shall allow for manual data entry of the minimum data set.
- R16 The software shall allow for entry of the minimum data set via a 2D bar code reader using PDF417 standard.
- R17 All fields of the minimum enrolment set listed in R14 shall be mandatory with the exception of "Other Names," which is optional.

The following chart provides an overview of the biographic data entry requirements as detailed in the next sub sections.

Field Name	Condition	Size	Permissible Values
GWF Number	Mandatory	12	"GWF" followed by 9 unique numeric characters
Family Name	Mandatory	1-35	Alphabetical and special characters
Other Names	Optional	0-35	Alphabetical and special characters
Date of Birth	Mandatory	8	MMDDCCYY format
Sex	Mandatory	1	M, F, or U only
Nationality	Mandatory	3	List of country codes provided by UKvisas
Travel Document Number	Mandatory	1-15	Any alphabetical, numeric, or special characters.
Exemption/Exception	Optional	1	Available values: 1 – Amputee (less than two fingers available) 2 - Medically Incapable

Table 1: Summary of Biographic Data Requirements

2.4.1 GWF Entry Requirements

- R18 The software shall accept by reading from bar code or by manual entry the GWF number generated by visa4uk in the format of 12 alphabetical and numeric characters.
- R19 The GWF shall always be in format of the GWF followed by 9 numeric characters (e.g., GWF123456789).
- R20 Operators shall have capability to edit GWFs in case of incorrect data or misreads from bar code until the record is confirmed.
- R21 The GWF field shall be a mandatory field.
- R22 Intelligence shall be placed on the field to verify the length and format of any GWF entered into the software as stated in R19.

2.4.2 Family Names

The software shall accept by reading from bar code or by manual entry the Family Names as shown on the UK visa applicant's valid travel document (Note: last names in U.S. terms or Surnames usually shown on most passports).

- R23 The length and format of the Family Names field shall be any alphabetical or special characters with minimum of 1 character and maximum of 35 characters.
- R24 Operators shall have capability to edit Family Names in case of incorrect data or misreads from bar code until the record is confirmed.
- R25 The Family Names field shall be a mandatory field.
- R26 Intelligence shall be placed on the field to verify the length and format of any Family Names entered into the software as stated in R24.

2.4.3 Other Names

The software shall accept by reading from bar code or by manual entry the Other Names as shown on the UK visa applicant's valid travel document (Note: combination of first and middle names in U.S. terms or given names usually shown on most passports).

- R27 The length and format of the Other Names field shall be any alphabetical or special characters with minimum of 0 characters and maximum of 35 characters.
- R28 Operators shall have capability to edit Other Names in case of incorrect data or misreads from bar code until the record is confirmed.
- R29 The Other Names field shall be an optional field.
- R30 Intelligence shall be placed on the field to verify the length and format of any Other Names entered into the software as stated in R29.

2.4.4 Date of Birth

The software shall accept by reading from bar code or by manual entry the Date of Birth as shown on the UK visa applicant's valid travel document.

- R31 The length and format of the Date of Birth field shall be any numeric character 8 characters in format of MMDDCCYY (e.g., 12201976).
- R32 Operators shall have capability to edit Date of Birth field in case of incorrect data or misreads from bar code until the record is confirmed.
- R33 The Date of Birth field shall be a mandatory field.
- R34 Intelligence shall be placed on the field to verify the length and format of any Date of Birth entered into the software as stated in R31.
- R35 Intelligence shall be available on the date of birth field to identify those applicants who are below the age of 5 years.
- R36 Where a child under the age of 5 years has been identified, the software shall provide a message to the operator informing that the child is not required to be enrolled and not allow operator to continue with the enrolment.

2.4.5 Sex

- R37 The software shall accept by reading from bar code or by manual entry the Sex as shown on the UK visa applicant's valid travel document.
- R38 The length and format of the Sex field shall be 1 character with "M," "F," or "U" as the only allowable characters.
- R39 Operators shall have capability to edit Sex field in case of incorrect data or misreads from bar code until the record is confirmed.
- R40 The Sex field shall be a mandatory field.
- R41 Intelligence shall be placed on the field to verify the length and format of any Sex entered into the software as stated in R38.

2.4.6 Nationality

The software shall accept by reading from bar code or by manual entry the Nationality as shown on the UK visa applicant's valid travel document.

- R42 The length and format of the Nationality field shall be 3 alphabetical characters and allowable Nationality codes are available in Appendix A.
- R43 Operators shall have capability to edit Nationality field in case of incorrect data or misreads from bar code until the record is confirmed.
- R44 The Nationality field shall be a mandatory field.
- R45 Intelligence shall be placed on the field to verify the length and format of any Nationality entered into the software as stated in R42.

2.4.7 Travel Document Number

The software shall accept by reading from bar code or by manual entry the Travel Document Number as shown on the UK visa applicant's valid travel document.

- R46 The length and format of the Travel Document Number field shall be any alphabetical, numeric, or special characters with minimum of 1 character and maximum of 15.
- R47 Operators shall have capability to edit Travel Document Number field in case of incorrect data or misreads from bar code until the record is confirmed.
- R48 The Travel Document Number field shall be a mandatory field.
- R49 Intelligence shall be placed on the field to verify the length and format of any Travel Document Number entered into the software as stated in R46.

2.4.8 Exemptions/Exceptions

The operator shall have capability to select an exemption/exception for two cases: 1) Amputee with less than two fingers of the middle 8 fingers available (middle 8 fingers are defined as all fingers and thumbs excluding the little fingers); or 2) Physically unable to provide fingerprints (e.g., severe arthritis).

- R50 The supervisor approval capability shall have ability to disallow exemption/exception returning the use to the normal workflow.

2.5 Fingerprint Enrolment Requirements

The software shall be capable of recording up to 10 individual rolled fingerprint images.

- R51 The software shall be capable of recording up to 4 slap fingerprint images consisting of up to 4 left fingers, up to 4 right hand fingers, right thumb, and left thumb.
- R52 The software shall have capability to measure quality of fingerprints images recorded.
- R53 The software shall have capability to inform operator when desired quality measurement has not been achieved to re-take images to improve quality.
- R54 The software shall have capability to allow operator to re-take fingerprints images until an acceptable quality threshold is met or operator determines the best quality possible has been recorded.
- R55 The software shall have capability to record a date/time stamp at the point when all fingerprints have been successfully recorded. Standard format and time zone for date/time stamp to be agreed between UKvisas and DHS.
- R56 The system shall display the fingerprint images to the operator for visual review.

- R57 The software shall have capability to perform a sequence check to ensure rolled images are in proper order.
- R58 The software shall have capability to allow operators to identify missing fingers (e.g., amputees), bandaged, or permanently damaged (e.g., scars/deformity).
- R59 All fingerprints images shall be compressed using Wavelet Scalar Quantisation (WSQ) 15:1 ratio.

2.6 Digital Photograph Enrolment Requirements

- R60 The system shall record a digital facial image of the UK visas applicant with goal of meeting International Civil Aviation Organisation (ICAO) compliance standards, however the measurement of ICAO compliance is NOT required. Best practices for photograph capture shall be implemented from ICAO such as no hats, no smiling, full frontal with minimal horizontal or vertical misalignment, etc.
- R61 The system shall record a date/time stamp at the point when photo is taken. Standard format and time zone for date/time stamp to be agreed between UKvisas and DHS.
- R62 The system shall record a true rendition of the image collected free from image enhancement or resolution mapping.
- R63 The software shall display the image to the operator to perform a visual check of the image.
- R64 The operator shall be allowed to cancel or re-take an image capture without cancelling or deleting the entire record.

3 Transmission of Data from ASCs to UKvisas Requirements

The following requirements are for the transmission of the data from DHS ASCs to UKvisas in the Phase 1a of the project.

- R65 The biometric and biographic data for each UK visa applicant shall be provided in the FBI Electronic Fingerprint Transmission Specification (EFTS) by DHS to UKvisas.
- R66 The EFTS file with contain for each visa applicant (1) Type-1 record (message header), one (1) Type-2 record (biographical, demographic, etc. data), up to 14 Type-4 records (10 individual rolled images and 4 slap images), and one (1) Type-10 record (digital photograph).
- R67 The EFTS file shall be transmitted as e-mail attachments using Simple Mail Transfer Protocol (SMTP) over a secure Internet connection between DHS and UKvisas.
- R68 The EFTS file shall be delivered to UKvisas within 12 hours of the completion of the biometric enrolment process at the ASCs.

- R69 DHS shall temporarily retain the EFTS file until USCIS confirms successful delivery of the file using native SMTP capabilities.
- R70 After successful delivery of EFTS file, UKvisas shall return a receipt notification to DHS for deletion of the files.
- R71 Upon successful receipt, UKvisas will translate the EFTS records to Extensible Markup Language (XML) based records required for submittal to IAFS.
- R72 The EFTS files shall include the following fields with mandatory and optional fields marked appropriately. Additional fields may be added at later date based on discussions between DHS and UKvisas.

1. Unique ID (Mandatory)
2. Family Name (Mandatory)
3. Other Names (Optional)
4. Date of Birth (Mandatory)
5. Sex (Mandatory)
6. Nationality (Mandatory)
7. Travel Document Number (Mandatory)
8. Exemption/Exception Code (Optional – default could be null)
9. ASC Location (Mandatory)
10. Workstation ID (Mandatory)
11. Operator ID (Mandatory)
12. Fingerprint Scanner ID (Optional)
13. Camera ID (Optional)
14. Fingerprint Recording Completion Date/Time Stamp (Mandatory)
15. Photograph Recording Completion Date/Time Stamp (Mandatory)
16. Fingerprint Presence for Each Finger (Mandatory)
17. WSQ Compressed Fingerprint Images (Mandatory for all available fingers)
18. Fingerprint Image Horizontal Line Length (Mandatory)
19. Fingerprint Image Vertical Line Length (Mandatory)
20. Photograph (Mandatory)
21. Photograph Width (Mandatory)
22. Photograph Length (Mandatory)
23. Quality Control (QC) ID (Optional)

Appendix A: Nationality Codes

CODE	NATIONALITY
AFG	AFGHANISTAN
ALB	ALBANIA
DZA	ALGERIA
ASM	AMERICAN SAMOA
AND	ANDORRA
AGO	ANGOLA
ATG	ANTIGUA AND BARBUDA
ARG	ARGENTINA
ARM	ARMENIA
ABW	ARUBA
AUS	AUSTRALIA
AUT	AUSTRIA
AZE	AZERBAIJAN
BHS	BAHAMAS
BHR	BAHRAIN
BGD	BANGLADESH
BRB	BARBADOS
BLR	BELARUS
BEL	BELGIUM
BLZ	BELIZE
BEN	BENIN
BTN	BHUTAN
BOL	BOLIVIA
BIH	BOSNIA AND HERZEGOVINA
BWA	BOTSWANA
BVT	BOUVET ISLAND
BRA	BRAZIL
GBR	GREAT BRITAIN
VGB	BRITISH VIRGIN ISLANDS
BRN	BRUNEI DARUSSALEM
BGR	BULGARIA
BFA	BURKINA FASO
BDI	BURUNDI
CMR	CAMEROON
CAN	CANADA
CPV	CAPE VERDE
CAF	CENTRAL AFRICAN REPUBLIC
TCD	CHAD
CHL	CHILE
CHN	CHINA
CXR	CHRISTMAS ISLAND
CCK	COCOS (KEELING) ISLANDS
COL	COLOMBIA
COM	COMOROS
COG	CONGO
COD	CONGO (DEMOCRATIC REP OF)
COK	COOK ISLANDS
CRI	COSTA RICA
CIV	COTE D'IVOIRE (IVORY COAST)
HRV	CROATIA

CODE	NATIONALITY
CUB	CUBA
CYP	CYPRUS
CZE	CZECH REPUBLIC
DNK	DENMARK
DJI	DJIBOUTI
DMA	DOMINICA
DOM	DOMINICAN REPUBLIC
ECU	ECUADOR
EGY	EGYPT
SLV	EL SALVADOR
GNQ	EQUATORAL GUINEA
ERI	ERITREA
EST	ESTONIA
ETH	ETHIOPIA
FJI	FIJI
FIN	FINLAND
FRA	FRANCE
GUF	FRENCH GUIANA
FXX	FRENCH METROPOLITAN
PYF	FRENCH POLYNESIA
ATF	FRENCH SOUTHERN TERRITORIES
GAB	GABON
GMB	GAMBIA
GEO	GEORGIA
D	GERMANY
GHA	GHANA
GRC	GREECE
GRL	GREENLAND
GRD	GRENADA
GLP	GUADELOUPE
GUM	GUAM
GTM	GUATEMALA
GIN	GUINEA
GNB	GUINEA-BISSAU
GUY	GUYANA
HTI	HAITI
HMD	HEARD AND MCDONALD ISLANDS
VAT	HOLY SEE (VATICAN CITY STATE)
HND	HONDURAS
HKG	HONG KONG SPECIAL ADMINISTRATIVE REGION OF CHINA
HUN	HUNGARY
ISL	ICELAND
IND	INDIA
IDN	INDONESIA
IRN	IRAN
IRQ	IRAQ
IRL	IRELAND
ISR	ISRAEL
ITA	ITALY
JAM	JAMAICA
JPN	JAPAN
JOR	JORDAN
KHM	KAMPUCHEA

CODE	NATIONALITY
KAZ	KAZAKHSTAN
KEN	KENYA
KIR	KIRIBATI
UNK	KOSOVO RESIDENT - UN ISSUED TRAVEL DOCUMENT
KWT	KUWAIT
KGZ	KYRGYZSTAN
LAO	LAOS
LVA	LATVIA
LBN	LEBANON
LSO	LESOTHO
LBR	LIBERIA
LBY	LIBYA
LIE	LIECHTENSTEIN
LTU	LITHUANIA
LUX	LUXEMBOURG
MAC	MACAO SPECIAL ADMINISTRATIVE REGION OF CHINA
MKD	MACEDONIA (FORMER YUGOSLAV REP OF)
MDG	MADAGASCAR
MWI	MALAWI
MYS	MALAYSIA
MDV	MALDIVES
MLI	MALI
MLT	MALTA
MHL	MARSHALL ISLANDS
MTQ	MARTINIQUE
MRT	MAURITANIA
MUS	MAURITIUS
MYT	MAYOTTE
MEX	MEXICO
FSM	MICRONESIA (FEDERATED STATES OF)
MDA	MOLDOVA (REP OF)
MCO	MONACO
MNG	MONGOLIA
MAR	MOROCCO
MOZ	MOZAMBIQUE
MNE	REPUBLIC OF MONTENEGRO
MMR	MYANMAR
NAM	NAMIBIA
NRU	NAURU
NPL	NEPAL
NLD	NETHERLANDS
ANT	NETHERLANDS ANTILLES
NCL	NEW CALEDONIA
NZL	NEW ZEALAND
NIC	NICARAGUA
NER	NIGER
NGA	NIGERIA
NIU	NIUE
NFK	NORFOLK ISLAND
PRK	NORTH KOREA (DEMOCRATIC PEOPLE'S REP OF)
MNP	NORTHERN MARIANA ISLANDS
NOR	NORWAY
OMN	OMAN

CODE	NATIONALITY
PAK	PAKISTAN
PLW	PALAU
PSE	PALESTINIAN AUTHORITY
PAN	PANAMA
PNG	PAPUA NEW GUINEA
PRY	PARAGUAY
PER	PERU
PHL	PHILIPPINES
POL	POLAND
PRT	PORTUGAL
PRI	PUERTO RICO
QAT	QATAR
XXB	REFUGEE - ARTICLE 1 OF THE 1951 CONVENTION
REU	REUNION
ROU	ROMANIA
RUS	RUSSIAN FEDERATION
RWA	RWANDA
WSM	SAMOA
SMR	SAN MARINO
STP	SAO TOME AND PRINCIPE
SAU	SAUDI ARABIA
SEN	SENEGAL
SRB	REPUBLIC OF SERBIA
SYC	SEYCHELLES
SLE	SIERRA LEONE
SGP	SINGAPORE
SVK	SLOVAKIA
SVN	SLOVENIA
SLB	SOLOMON ISLANDS
SOM	SOMALIA
ZAF	SOUTH AFRICA
KOR	SOUTH KOREA (REP OF KOREA)
ESP	SPAIN
LKA	SRI LANKA
KNA	ST KITTS AND NEVIS
LCA	ST LUCIA
SPM	ST PIERRE AND MIQUELON
VCT	ST VINCENT AND THE GRENADINES
XXA	STATELESS PERSON (ARTICLE 1 OF 1951 CONVENTION)
SDN	SUDAN
SUR	SURINAME
SJM	SVALBARD AND JAN MAYEN ISLANDS
SWZ	SWAZILAND
SWE	SWEDEN
CHE	SWITZERLAND
SYR	SYRIA (ARAB REP)
TWN	TAIWAN (REP OF CHINA)
TJK	TAJIKISTAN
TZA	TANZANIA (UNITED REP OF)
THA	THAILAND
TLS	TIMOR-LESTE
TGO	TOGO
TKL	TOKELAU

CODE	NATIONALITY
TON	TONGA
TTO	TRINIDAD AND TOBAGO
TUN	TUNISIA
TUR	TURKEY
XXT	TURKISH REPUBLIC OF NORTHERN CYPRUS
TKM	TURKMENISTAN
TUV	TUVALU
UGA	UGANDA
UKR	UKRAINE
ARE	UNITED ARAB EMIRATES
UNO	UNITED NATIONS
UNA	UNITED NATIONS AGENCY
UMI	UNITED STATES MINOR OUTLYING ISLANDS
USA	UNITED STATES OF AMERICA
VIR	UNITED STATES VIRGIN ISLANDS
XXX	UNSPECIFIED NATIONALITY
URY	URUGUAY
UZB	UZBEKISTAN
VUT	VANUATU
VEN	VENEZUELA
VNM	VIETNAM
WLF	WALLIS AND FUTUNA ISLANDS
ESH	WESTERN SAHARA
YEM	YEMEN
ZMB	ZAMBIA
ZWE	ZIMBABWE

IAFIS IMAGE QUALITY SPECIFICATIONS

1.0 SCOPE AND PURPOSE

These specifications apply to fingerprint scanner systems and printers that will supply fingerprint data to the Integrated Automated Fingerprint Identification System (IAFIS), and to printers and displays within the IAFIS. They provide objective criteria for insuring image quality.

Electronic images must be of sufficient quality to allow for: (1) conclusive fingerprint comparisons (identification or non-identification decision); (2) fingerprint classification; (3) automatic feature detection; and (4) overall Automated Fingerprint Identification System (AFIS) search reliability.

The fingerprint comparison process requires a high fidelity image without any banding, streaking or other visual defects. Finer detail such as pores and incipient ridges are needed since they can play an important role in the comparison. Additionally, the gray-scale dynamic range must be captured with sufficient depth to support image enhancement and restoration algorithms.

The image quality requirements have associated test procedures, which are described in the document Test Procedures for Verifying IAFIS Scanner Image Quality Requirements. These procedures will be used by the Government in acceptance testing to ensure compliance with the requirements, and in performance capability demonstrations as an indication of capability to perform. Equipment shall be tested to meet the requirements in normal operating modes, e.g., scanners shall not be tested at slower than normal operating speeds to meet modulation transfer function specifications. A vendor may recommend alternate testing methods.

2.0 FINGERPRINT SCANNERS

The following subsections describe the image quality performance characteristics required for a fingerprint scanner (live scan and card scan). These specifications require that the scanner shall capture fingerprints at a minimum resolution in both the detector row and detector column directions (also known as 'along-scan' and 'cross-scan' directions) of 500 pixels/inch, plus or minus 5 pixels per inch. The final output delivered image from the scanner system shall have a resolution of 500 pixels/inch, plus or minus 5 pixels per inch, and each pixel shall be gray level quantized to 8 bits. [Requirement

described in the ANSI standard: Data Format for the Interchange of Fingerprint Information, ANSI/NIST-CSL 1-1993.]

CJIS-RS-0010 (V7)

101

January 29, 1999

2.1 Geometric Image Accuracy

The absolute value of the difference "D", between the actual distance "X" between any two points on a target and the distance "Y" between those same two points as measured on the output scanned image of that target, shall meet the following requirements for the value D:

D 0.0007, for 0 X 0.07

D 0.01X, for 0.07 X 1.50

where: D, X, Y are in inches and $D = Y - X$

The requirement corresponds to a positional accuracy of $\pm 1\%$ for distances between 0.07 and 1.5 inches, and a constant ± 0.0007 inches (1/3 pixel) for distances less than or equal to 0.07 inches. The geometric image accuracy shall be measured using precision 1 cycle per millimeter Ronchi targets on white Mylar reflective base manufactured by Applied Image, Inc.⁴

2.2 Modulation Transfer Function

The measured modulation transfer function (MTF) of the scanner, in both the detector row and detector column directions, and over any region of the scanner's field of view, shall have modulation values which fall within the ranges given in the following MTF table, at the given spatial frequencies:

cyc/mm MTF

1 .905 to 1.00

2 .797 to 1.00

3 .694 to 1.00

4 .598 to 1.00

5 .513 to 1.00

6 .437 to 1.00

8 .312 to 1.00

10 .200 to 1.00

The MTF shall be measured using test chart number M-13-60-1X manufactured by Sine Patterns, Inc.5. The single, representative sine wave modulation in each imaged sine wave frequency pattern is determined from the sample modulation values collected from within that pattern. The sample modulation values are computed from the maximum and minimum levels corresponding to the 'peak' and adjacent 'valley' in each sine wave period. These maximum and minimum levels represent the corresponding locally averaged image gray levels mapped through a calibration curve into target reflectance space, where the local average of gray levels is computed in a direction orthogonal to the sinusoidal variation direction. Sample image modulation is then defined as:

4Applied Image, 1653 East Main Street, Rochester, NY 14526, Phone (716) 482-0300

5Sine Patterns, 236 Henderson Drive, Penfield, NY 14526, Phone (716) 248-5338

CJIS-RS-0010 (V7)

102

January 29, 1999

$(\text{maximum} - \text{minimum}) / (\text{maximum} + \text{minimum})$

The calibration curve is constructed by performing a least squares linear regression curve fit between the image gray levels of the 14 density patches in the test target and the corresponding target reflectance values. The scanner MTF at each frequency is then defined as:

$\text{MTF} = \text{representative image modulation} / \text{target modulation}$

[Target modulations and target density patch values are supplied with the test target by the manufacturer.]

2.3 Signal-to-Noise Ratio

Both the ratio of signal to white noise standard deviation and the ratio of signal to black noise standard deviation of the digital scanner shall be greater than or equal to 125 using the following procedure:

1) A random 0.25 inch x 0.25 inch test field within the image area is chosen and the white reference target, Munsell6 N9-white matte, is placed in the test field.

2) A white test population of 8-bit reflectance values from at least 1000 samples within the test field are collected. The average value and standard deviation are computed from this test population.

3) Steps 1 and 2 are repeated for the black reference target, Munsell N3 - black matte.

4) The signal to noise ratio (SNR) is computed as the difference between average white and average black values, alternately divided by the white noise standard deviation ('white SNR') and the black noise standard deviation ('black SNR').

Note: The scanner shall be set up such that the white reference target is below scanner saturation level, and the black reference target is above scanner dark current level. Also, care should be taken, via direct visual or visual display observation, to avoid areas of dust, pinholes, scratches, or other imperfections on the target when selecting the sub-area for the 1000 samples.

6 Munsell-Macbeth, P.O. Box 230, Newburgh, NY 12551, Phone (914) 565-7660

CJIS-RS-0010 (V7)

103

January 29, 1999

2.4 Gray-Scale Range of Image Data

At least 80% of the captured individual fingerprint images shall have a gray-scale dynamic range of at least 200 gray levels and at least 99% shall have a dynamic range of at least 128 gray levels. For this requirements section, 'dynamic range' is defined as the total number of gray levels that have signal content from the fingerprint image. Fingerprint card format lines, boxes, and text shall be excluded from the dynamic range computation and white surround in the immediate vicinity of a given fingerprint shall be

included in the dynamic range computation (dashed box at right). Compliance with these dynamic range requirements shall be verified using a stratified sample of fingerprint cards assembled by the Government.

The intent is to avoid excessively low contrast images. Live-scan systems and card scanners at a booking station can control dynamic range by rolling the prints properly. However, with central site or file conversion systems, where a variety of card types and image qualities are encountered, adaptive processing may be necessary. The 8-bit quantization of the gray-scale values for very low contrast fingerprints needs to more optimally represent the reduced gray-scale range of such fingerprints. In the example histogram accompanying this section, the gray-scale values divide up the range from A to B. The parameters A and B are stored with the image to provide an audit trail.

2.5 Gray-scale Linearity

Using the 14 gray patches in the Sine Patterns, Inc. test target M-13-60-1X as the scanner input (independent variable), with their manufacture-supplied reflectance values, none of the corresponding 14 scanner output gray levels (dependent variable) shall deviate by more than 7.65 gray levels from a linear, least squares regression line fitted between the two variables. The output sample values within an area of at least 0.25 x 0.25 inches shall be utilized to compute the average output gray level for each patch.

2.6 Output Gray Level Uniformity

Output gray level uniformity shall be determined by scanning both a white reference target, Munsell N9 - white matte, and a black reference target, Munsell N3 - black matte. The scanner shall be set up such that the white reference target is below scanner saturation level, and the black reference target is above scanner dark current level in the respective tests. Using the white target as the scanner input, the following three requirements shall be met:

CJIS-RS-0010 (V7)

104

January 29, 1999

(1) The outputs of any two adjacent rows or columns of length 9 pixels or greater shall not have mean gray levels that differ by more than 2.5 gray levels.

(2) For all pixels within a 0.25 inch x 0.25 inch area ('quarter inch area') located in any region of the total scanner field of view, no individual pixel's gray level shall vary from the mean gray level by more than 22.0 gray levels.

(3) For any two non-contiguous quarter inch areas located anywhere in the total scanner field of view, the mean gray levels of the two quarter inch areas shall not differ by more than 12.0 gray levels.

And, using the black target as the scanner input, the following three requirements shall be met:

(1) The outputs of any two adjacent rows or columns of length 9 pixels or greater shall not have mean gray levels that differ by more than 1.0 gray levels.

(2) For all pixels within a 0.25 inch x 0.25 inch area ('quarter inch area') located in any region of the total scanner field of view, no individual pixel's gray level shall vary from the mean gray level by more than 8.0 gray levels.

(3) For any two non-contiguous quarter inch areas located anywhere in the total scanner field of view, the mean gray levels of the two quarter inch areas shall not differ by more than 3.0 gray levels.

CJIS-RS-0010 (V7)

105

January 29, 1999

3.0 LATENT PRINT SCANNERS

The following subsections describe the image quality performance characteristics required for a latent print scanner operating in a 1000 pixels/inch mode. These specifications require that the scanner shall capture fingerprints at a minimum resolution in both the detector row and detector column directions (also known as 'along-scan' and 'cross-scan' directions) of 1000 pixels/inch. The final output delivered image from the scanner system (at the 1000 ppi setting) shall have a resolution of 1000 pixels/inch, plus or minus 10 pixels per inch, and each pixel shall be gray level quantized to a minimum of

8 bits. The complete latent print specification consists of all requirements given in this Section, plus all non-conflicting requirements given in Section 2.0 Fingerprint Scanners.

3.1 Geometric Image Accuracy

The absolute value of the difference "D", between the actual distance "X" between any two points on a target and the distance "Y" between those same two points as measured on the output scanned image of that target, shall meet the following requirements for the value D:

D 0.0005, for 0 X 0.07

D 0.0071X, for 0.07 X 1.50

where: D, X, Y are in inches and $D = Y - X$

The requirement corresponds to a positional accuracy of $\pm .71\%$ for distances between 0.07 and 1.5 inches, and a constant ± 0.0005 inches ($\frac{1}{2}$ pixel) for distances less than or equal to 0.07 inches. The geometric image accuracy shall be measured using precision 1 cycle per millimeter Ronchi targets on white Mylar reflective base manufactured by Applied Image, Inc.⁷

3.2 Modulation Transfer Function

The measured modulation transfer function (MTF) of the scanner, in both the detector row and detector column directions, and over any region of the scanner's field of view, shall have modulation values which fall within the ranges given in the following MTF table, at the given spatial frequencies:

cyc/mm MTF

1 0.925 to 1.00

2 0.856 to 1.00

3 0.791 to 1.00

4 0.732 to 1.00

5 0.677 to 1.00

6 0.626 to 1.00

8 0.536 to 1.00

⁷Applied Image, 1653 East Main Street, Rochester, NY 14526, Phone (716) 482-0300

CJIS-RS-0010 (V7)

106

January 29, 1999

cyc/mm MTF

10 0.458 to 1.00

12 0.392 to 1.00

14 0.336 to 1.00

16 0.287 to 1.00

18 0.246 to 1.00

20 0.210 to 1.00

The MTF shall be measured using test chart number M-13-60-1X manufactured by Sine Patterns, Inc.⁸. The single, representative sine wave modulation in each imaged sine wave frequency pattern is determined from the sample modulation values collected from within that pattern. The sample modulation values are computed from the maximum and minimum levels corresponding to the 'peak' and adjacent 'valley' in each sine wave period. These maximum and minimum levels represent the corresponding locally averaged image gray levels mapped through a calibration curve into target reflectance space, where the local average of gray levels is computed in a direction orthogonal to the sinusoidal variation direction. Sample image modulation is then defined as:

$$(\text{maximum} - \text{minimum}) / (\text{maximum} + \text{minimum})$$

The calibration curve is constructed by performing a least squares linear regression curve fit between the image gray levels of the 14 density patches in the test target and the corresponding target reflectance values. The scanner MTF at each frequency is then defined as:

$$\text{MTF} = \text{representative image modulation} / \text{target modulation}$$

[Target modulations and target density patch values are supplied with the test target by the manufacturer.]

⁸Sine Patterns, 236 Henderson Drive, Penfield, NY 14526, Phone (716) 248-5338

CJIS-RS-0010 (V7)

107

January 29, 1999

4.0 IAFIS DISPLAY SPECIFICATIONS

Two types of displays are required. One is for the ten-print examiner and document processing. The other is for the latent examiner.

4.1 Ten-print / Document Processing Display

The ten-print/document processing display shall meet the following performance levels:

Parameter Value Comments

Colors 256 8 bits/pixel

Number of addressable pixels 1280 x 1024

Pixel size 0.28 mm (max) width at 50% amplitude at center of display

Active display area 14" x 10.5" (min) Landscape mode

Display refresh at least 72 Hz noninterlaced Minimizes flicker rate

Video bandwidth at least 100 MHz

Luminance 33 fL (min) of white area

Video pulse rise & fall time 3 nanosec. (max) ensures no visible smearing

Geometric pixel location error $\pm 1.5\%$ (max) No point varies more than 1.5% from its correct position

Operator controls brightness, contrast on front panel

Brightness Uniformity $\pm 15\%$ of mean deviation (max) over entire display at low, medium and high brightness

CJIS-RS-0010 (V7)

108

January 29, 1999

4.2 Latent Print Comparison Display

The other display is for use by the FBI's latent fingerprint examiners. Because this display will be used to support latent fingerprint comparisons, the resolution and brightness (luminance) requirements are higher. The display shall be a monochrome cathode ray tube display, which shall meet the following performance levels:

Parameter Value Comments

Gray levels 8 bits/pixel @ CRT video input

Number of addressable pixels 1600 x 1200

Pixel size 0.19 mm (max) width at 50% amplitude at center of display

Active display area 14" x 10.5" (min) Landscape mode

Display refresh rate at least 72 Hz noninterlaced Minimizes flicker

Video bandwidth at least 100 MHz

Luminance 50 fL (min) of white area

Video pulse rise & fall time 3 nanosec. (max) ensures no visible smearing
Geometric pixel location error $\pm 1.5\%$ (max) No point varies more than 1.5% from its correct position
Operator controls brightness, contrast on front panel
Brightness Uniformity $\pm 15\%$ of mean deviation (max) over entire display at low, medium and high brightness

The ambient lighting in the work area is expected to be a combination of natural and fluorescent lighting.

CJIS-RS-0010 (V7)

109

January 29, 1999

5.0 PRINTER SPECIFICATIONS

The fingerprint examiners in the IAFIS environment will depend upon softcopy images to make comparisons and will require hardcopy images in certain instances. Some contributors will print cards from live scan or card scan devices for submission to the FBI. In all such cases the images will be mapped from their digital form to high resolution printing devices. The printed images must be of sufficient quality to support all phases of identification, including conclusive fingerprint comparisons (identification or non-identification decision).

Two classes of printing devices are required. The first is intended to support fingerprint card reproduction. These printers will be used within the IAFIS environment and by submitters who choose to print and mail their live scan results. The printers should provide high throughput, low-cost-per-copy, non-fading output. This monochrome printer shall perform at the following minimum levels:

Gray levels 16

Paper size 8" x 8" (min)

Resolution 500 dots/inch (min.), where each pixel is capable of producing 16 gray levels

A second class of printer is required to support the investigative fingerprint comparison function. Continuous tone monochrome output is required. This printer shall perform at the following minimum levels:

Gray levels 8-bit continuous-tone gray-scale

Paper Production of output paper print shall not require liquid processing

Paper size 8" x 11"

Resolution At least 500 pixels per inch, where each pixel is capable of producing 256 gray levels from an 8 bits/pixel input

CJIS-RS-0010 (V7)

110

January 29, 1999
