SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE	OF
	1	133

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
47QTCK18D0060	27 Feb 2020	70SBUR20F00000090	70SBUR20R000000011	02/04/2020

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	Peter Dietrich	802-872-4621	

9. ISSUED BY — CODE: CIS

USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR ☐ SET ASIDE: % FOR:

☐ SMALL BUSINESS
☐ HUBZONE SMALL BUSINESS
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
☐ EDWOSB
☐ 8(A)

NAICS:
SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION
☒ SEE SCHEDULE	Net 30	☐	☐RFQ ☐IFB ☐RFP

15. DELIVER TO — CODE: HQOIT

Department of Homeland Security
US Citizenship & Immigration Svcs
Office of Information Technology
111 Massachusetts Ave, NW
Suite 5000
Washington DC 20529

16. ADMINISTERED BY — CODE: CIS

USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

17a. CONTRACTOR/ OFFEROR — CODE: 8495509830000 — FACILITY CODE:

CRGT INC
11921 FREEDOM DRIVE
SUITE 1000
RESTON VA 201905636

TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY — CODE: WEBVIEW

See Invoicing Instructions

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

☐ 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: 849550983+0000 This order is subject to the terms and conditions of the Alliant 2 Unrestricted contract 47QTCK18D0060. [redacted] Continued ... *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA
See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*
$9,196,470.00

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.
☒ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☒ ARE ☐ ARE NOT ATTACHED.

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☒ 29. AWARD OF CONTRACT: _____ OFFER DATED 02/18/2020. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: All

30a. SIGNATURE OF OFFEROR/CONTRACTOR
[redacted]

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
STUART SELLEARS Digitally signed by STUART SELLEARS Date: 2020.02.27 15:54:36 -05'00'

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
[redacted]		Stuart Sellears	27 FEB 2020

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
[redacted]					

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL	37. CHECK NUMBER

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

NAME OF OFFEROR OR CONTRACTOR
CRGT INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)

[redacted]

NAME OF OFFEROR OR CONTRACTOR
CRGT INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)

[redacted]

U.S. Citizenship and Immigration Services

Office of Information Technology (OIT)

National Area and Transnational IT Operations and Next-Generation Support (NATIONS)

Performance Work Statement (PWS)

Performance Work Statement (PWS)

1.0 PROJECT TITLE

The United States Citizenship & Immigration Services (USCIS), Office of Information Technology (OIT) has a requirement for the continuation of a broad range of National Area and Transnational IT Operations and Next-Generation Support (NATIONS) services to all USCIS end users.

2.0 BACKGROUND

The USCIS processes applications and petitions for immigration and citizenship benefits, promotes an awareness and understanding of citizenship, and ensures the integrity of the United States immigration system. These functions and processes include employment authorization, asylum, resident alien processing, and citizenship naturalization. The USCIS OIT provides information technology (IT), expertise, and the strategic vision necessary to enable USCIS to deliver effective, efficient, and secure immigration services and products. OIT leads USCIS in the design, development, delivery, and deployment of IT services and solutions that are transforming the nation's immigration system.

OIT requires a new task order to continue service desk operational support, field services, service center services, account management services, and hardware incident resolution. The work to be performed under the General Service Administration's (GSA) Alliant Government Wide Acquisition Contracts (GWAC) is categorized as Sensitive but Unclassified (SBU).

3.0 SCOPE

OIT has a requirement to obtain broad range of IT support services to all USCIS end users. OIT End User Services (EUS) division provides USCIS user support throughout the Continental United States (CONUS) and Outside of the Continental United States (OCONUS). The support will include:

- Service Desk Support
  - Service Desk Tier 1
  - Service Desk Tier 1.5
  - Incident Management
  - Knowledge Management
  - Problem Management
  - Service Request Management
  - Specialized Support
- Field Services
  - Deskside Support (CONUS/OCONUS)
    - Asset Inventory Support
    - Disposal Preparation Support
    - Encryption Services
    - Video Conferencing and Audio/Video (A/V) Operations and Maintenance (O&M)

        - Local On-Site Cabling
        - OCONUS Site Support
    - Wireless Services
    - Deployment Services
    - Server O&M
    - Training Support
- Service Center Services
- Account Management Services
- Hardware Incident Resolution

3.1 Continuity of Operations Coordination

Continuity of Operations (COOP) is an effort within individual organizations to ensure that Mission Essential Functions and Primary Mission Essential Functions continue to be performed during a wide range of emergencies including localized acts of nature, accidents, and technological attack related emergencies. Based on the location of the emergency, any of the existing 230 domestic sites may be initiated as a temporary COOP site. There will be one COOP site in each of the six OIT support regions, National Capital Region, Northeast, Southeast, South Central, North Central, and Western.

The Contractor shall designate a staff member at every USCIS COOP site who can serve as the COOP liaison for that region (preferably Deskside Server Maintenance (DSM) staff or Regional Managers). Each designated USCIS COOP site will have their own COOP and Devolution Plan. The Contractor COOP liaison shall be required to coordinate with the selected Government COOP manager during emergencies and follow each site's COOP guidelines. USCIS Emergency Management Safety Division (EMSD) is the authority on COOP. During emergencies, additional guidance may be issued from EMSD that must be followed.

The Contractor COOP liaison shall have authority to direct their Contractor support for COOP purposes. The Contractor shall:

- When adjustments are made to the Department of Homeland Security (DHS) USCIS guidelines and conditions related to COOP, adhere to the regulations when assisting Government COOP manager(s) prepare/confirm COOP and/or Devolution Plan for their site.
- Be the Contractor COOP lead on the ground during an Event/Exercise/Emergency.

4.0 APPLICABLE DOCUMENTS

The Contractor shall be responsible for being knowledgeable and familiar with the most current version of the following Technical Reference Documents. The Government will be responsible for ensuring the Contractor is properly notified (via Email) when updates and/or changes are issued. The documents identified within Table 1 and throughout the Performance Work Statement (PWS) are current as of issuance of the task order solicitation.

Table 1 Applicable Documents

Document Name	Description/Applicable Web Site
DHS COOP Plan	Due to the sensitivity of the document, this will be available upon award. Website: *http://dhsconnect.dhs.gov/org/comp/plcy/frontofc/epp/Documents/Office%20of%20Policy%20COOP%20Plan.pdf*
Section 508 Compliance	Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220) Located at Web Site: http://www.section508.gov/index.cfm?%20%20FuseAction=Content&ID=12
DHS Management Directive (MD) 4010.2 – Section 508	Identified under Topic: Information and Technology Management Section 508 Program Management Office & Electronic and Information Technology Accessibility Web Site: *http://dhsconnect.dhs.gov/policies/Pages/directives.aspx*
DHS MD 4300A – Sensitive Systems Policy Handbook, Attachment G	Attachment G: Rules of Behavior Web Sites: *http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/4300A%20Attachment%20G%20-%20Rules%20of%20Behavior.doc*
DHS MD 4300A – Sensitive Systems Policy Handbook, Attachment F	Attachment F: Incident Response and Reporting Website: *http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/4300A%20Attachment%20F%20-%20Incident%20Response.doc*
DHS MD 4300A – Sensitive Systems Policy Handbook	Sensitive Systems Policy Handbook – Latest version on DHS Connect Website: *http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/4300A%20DHS%20Sensitive%20Systems%20Handbook.DOC*
DHS MD 4300A – Sensitive Systems Policy	Sensitive Systems Policy – Latest version on DHS Connect Website: *http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/4300A%20Sensitive%20Systems%20Policy.pdf*
DHS MD 4300B – National Security Systems Policy	National Security Systems Policy – Latest version on DHS Connect Website: *http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/4300B%20National%20Security%20Systems%20Policy.docx*
DHS MD 4400.1 - DHS Web (Internet, Intranet, and Extranet Information) and Information Systems	Identified under Topic: Information and Technology Management Website: *http://dhsconnect.dhs.gov/policies/Instructions/4400.1%20DHS%20Web%20(Internet,%20Intranet,%20and%20Extranet%20Information)%20and%20Information%20Systems.pdf*
DHS MD 4600.1 – Personal Use of Government Office Equipment	Identified under Topic: Information and Technology Management Website: *http://dhsconnect.dhs.gov/policies/Instructions/4600.1%20Personal%20Use%20of%20Government%20Office%20Equipment.pdf*
DHS MD 4700.1 - Personal Communications Device Distribution	Identified under Topic: Information and Technology Management Website: *http://dhsconnect.dhs.gov/policies/Instructions/4700.1%20Personal%20Communications%20Device%20Distribution.pdf*
DHS MD 4900 - Individual Use and Operation of DHS Information Systems – Computers	Identified under Topic: Information and Technology Management Website: *http://dhsconnect.dhs.gov/policies/Pages/directives.aspx*
DHS MD 11005 - Suspending Access to DHS Facilities, Sensitive Information, and IT Systems	Identified under Topic: Security Website: *http://dhsconnect.dhs.gov/policies/Instructions/11005%20Suspending%20Access*

Document Name	Description/Applicable Web Site
	%20to%20DHS%20Facilities,%20Sensitive%20Information,%20and%20IT%20Systems.pdf
DHS MD 11052 - Internal Security Program	Identified under Topic: Security Website: *http://dhsconnect.dhs.gov/policies/Instructions/11052%20Internal%20Security%20Program.pdf*
USCIS Leadership and Site List	Website: *http://connect.uscis.dhs.gov/Documents/leadershipdirectory.pdf*
USCIS Structured Cable Plant Standard	Website: http://connect.uscis.dhs.gov/org/MGMT/OIT/Documents/USCIS%20Structured%20Cable%20Plant%20Standard.pdf
DHS Technical Reference Model (TRM)	Website: *http://dhsconnect.dhs.gov/org/comp/mgmt/cio/oat/Documents/EAPMO/HLS%20EA%202010/compliance/comp_trm.htm*
USCIS OIT Change, Configuration, and Release Management (CCRM) Process	Website: *http://connect.uscis.dhs.gov/org/mgmt/oit/end%20user%20services/ccrm/Pages/default.aspx*
Employee and Contractor Exit Clearance Procedures - MD No. 257-001	Website: http://connect.uscis.dhs.gov/org/MGMT/HCT/Pages/ExitClearance.aspx
USCIS MD 140-001 – Handling Sensitive and Non-Sensitive Personally Identifiable Information (PII)	Website: *http://connect.uscis.dhs.gov/org/EXSO/Documents/Management%20Directives/MD-140-001.pdf*
DHS Systems Engineering Life Cycle (SELC) Guide	Website: *http://dhsconnect.dhs.gov/org/comp/mgmt/cio/ebmo/Pages/SELC.aspx*
USCIS MD 119-002, Personal Property Management	Website: *http://connect.uscis.dhs.gov/org/MGMT/ADMIN/AMCS/Documents/MD%20119-002%20Personal%20Property%20Mgmt.pdf*
USCIS-ADM-5350, Accountability of Sensitive Personal Property	Website: *http://connect.uscis.dhs.gov/org/MGMT/ADMIN/Documents/MD%20USCIS%20ADM%205350%20Accountability%20of%20Sen%20Per%20Prop%20Apr%202020 06.pdf*
Excess Policy and Procedures	To be provided after Task Order Award.
USCIS Backup Tape Inventory 2011_Master	To be provided after Task Order Award.

Note: Web references that are italicized are only accessible via DHS Network connectivity.

5.0 PERFORMANCE REQUIREMENTS

5.1 RESERVED

5.2 Program Management

During the period of performance of this task order, the Government will require the Contractor to provide program management activities needed to support NATIONS.

The Contractor's program management activities shall include:

- Manage resources and supervise Contractor staff in the performance of all work on this task order;

- Be responsible for the actual accomplishment of the PWS for this task order,
- Organize, direct and coordinate planning and execution of all task order activities,
- Ensure that the schedule, standards, reporting, task order changes, and subcontract management responsibilities are met,
- Maintain task order Acceptable Quality Levels (AQLs) in the Performance and Schedule Standards, Table 3, Section 6.0.
- Actively pursue solutions to correct deficiencies when necessary,
- Be the primary interface with the CO and COR,
- Attend status meetings and ad hoc meetings as required (see Deliverables Schedule).
- Oversee personnel security activities including assignment of properly cleared staff and requests for sensitive accounts access;
- Appoint experienced, knowledgeable and capable points of contact for USCIS task order and task management. These contacts, including key personnel, shall be available for both ad hoc and regularly-scheduled meetings at the Government site;
- Establish systems and internal processes that will provide operational and task order-specific financial information as both scheduled and ad-hoc deliverables;
- Maintain task order Acceptable Quality Levels (AQLs);

The Contractor shall be required to use commercially available automated tools and expertise with applications, processes and metrics that support task order management to achieve NATIONS' objectives. The Government will require access to these automated tools which may be used for quicker access, improved accuracy, and enhanced accessibility for Contractors/Government, real-time monitoring of status/deliverables, tracking the quality of work products and gauging overall customer satisfaction.

5.3 Service Desk Services

The USCIS Service Desk (SD) is the single point of contact for all USCIS authorized users when they need IT services such as service incident, service requests and change requests. The Contractor shall ensure that the SD:

- Operates 24x7x365 as the single point of contact for all IT operations support.
- Provides a single point of communication to the users;
- Provides a point of coordination for all IT groups;
- Provides help desk services, tier 1 and tier 1.5;
- Remains responsible for the ticket (incident and service request) through resolution and serve as the requestors' advocate in tiers 2 and 3;
- Properly assigns incident and service request ticket priority considering impact and urgency;
- Properly assigns incident and service request ticket product categorization classification;
- Complies with metrics such as first-call resolution, speed of answer, abandonment rate and all other stated SD AQLs in the Performance and Schedule Standards, Table 3, Section 6.0;
- Monitors major issues and trends;
- Provides quality control (call intake and ticket);
- Provides physical incident escalation handoff;

- Provides support to work at home (telework) users and pre/post application releases.

Additionally, the Contractor shall be required to comply with the customer satisfaction survey AQL. An automated email will be generated and forwarded to the end user after the Contractor closes their ticket in Remedy. The email message will contain a link to the customer satisfaction survey. Users will have the opportunity to take the survey in Remedy where the results of the survey will be stored. The Contractor shall monitor the survey results for compliance to the AQL.

The Contractor shall provide direct support using Government furnished tools. The Contractor shall use the existing USCIS BMC IT Services Management (ITSM) - Remedy instance in operation at the start of the task order as its SD automation tool. The Contractor shall be able to support all operating systems and device agnostic environments.

5.3.1 Scope of Work

The estimated work load and number of end users and equipment the Contractor shall support includes the following:

- Supported users: ~24,000
- Desktops and laptops: ~ 25,000
- Printers and peripherals: ~25,000
- Servers: ~1,200
- Wireless Devices: ~6,000
- Average monthly in-coming telephone calls: 24,000 to 30,000
- Average monthly in-coming e-mail & fax contacts: 13,000 to 15,000

The following task areas are for the implementation of support services at worldwide USCIS facilities. The current USCIS SD is based on IT Infrastructure Library (ITIL) principles.

- Service Desk Tier 1
- Service Desk Tier 1.5
- Incident Management
- Knowledge Management
- Problem Management
- Service Request management

All Concept of Operations (CONOPS) and Standard Operating Procedures (SOPs) to be developed or updated by the Contractor in this task area are to be provided to the Government within 10 days after NTP.

5.3.2 Service Desk – Tier 1

The Contractor shall provide SD Tier 1 support activities including phone, email and fax. The Contractor shall designate personnel with customer service, phone etiquette, phone system operations, and email (written) communication skills (see comprehension requirements in Tier 1 Personnel section). The Contractor shall understand ticket quality standards. Additionally, the

Contractor shall provide enhanced support for Priority callers and implement the Government Priority policy. The Contractor shall update the policy and forward to the COR and PM for initial review and approval and on a quarterly basis thereafter.

5.3.2.1 Phone Support – Tier 1

The Contractor shall:

- Operate within the SD AQL's, first call resolution, and speed of answer.
- Perform password resets on applicable systems and ensure phone support is staffed with agents who are qualified to serve as Password Issuance and Control System (PICS) officers by the completion of task order transition. PICS is a mainframe system used to manage access to USCIS critical "national" systems. To be eligible to serve as PICS officers, individuals must hold T1 Public Trust "clearances" supported by a Limited Background Investigation (LBI). There is no National Security Information (NSI) security clearance required.
- Collect information from callers and ensure that tickets are promptly and accurately documented in Remedy so that up to date information is available at all times.
- Ensure that other IT requests (application specific and others that cannot be resolved by SD Tier 1, 1.5) are properly routed to the appropriate support organizations.
- Utilize the knowledge base to guide callers through resolution of reported issues.
- Provide a support structure for SD Tier 1 to escalate incident to Tier 1.5 or Critical Incident Response Team (CIRT)
- Provide suggestions on making Tier 1 duties more efficient and better for the customer during weekly and monthly status meetings.

5.3.2.2 Email and Fax Support – Tier 1

The Contractor shall:

- Ensure that all email and fax service requests are processed within the AQL's.
- Ensure that Tier 1 email and fax team also receives Tier 1 phone support training to assist when email and fax incoming volume is low or during spike on the phones.
- Ensure that a response to every contact is acknowledged to requestor, documented accurately and worked as a first contact resolution or assigned appropriately.

5.3.2.3 Tier 1 Personnel

The Contractor shall develop and implement a new staff orientation program to familiarize new SD staff with all SD Tier 1 procedures and processes before they participate in SD support activities, to avoid untrained Contractors from performing new/unfamiliar functions. The Contractor shall accomplish the following:

- Develop and train all new Contractor employees on customer service interaction prior to participating in SD Tier 1 activities.
- Develop and train all new Contractor employees on phone etiquette and phone system operations prior to participating in SD Tier 1 activities.
- Develop and train all new Contractor employees on ticket quality standards prior to participating in SD Tier 1 activities.

- Keep a log or database of all Contractor employees' completed training. Provide Government access to the log at all times.
- Develop and train Tier 1 email and fax team on proper email and written communication etiquette.

5.3.3 Service Desk – Tier 1.5

The Contractor shall ensure that SD Tier 1.5 personnel are trained and understand all of the Tier 1 phone support duties, email and fax team duties and have knowledge of Local Area Network (LAN) Desk (see comprehension requirements in Contractor Personnel section). The Contractor shall perform SD Tier 1.5 functions including:

- Troubleshoot operating system and Commercial off the Shelf (COTS) software related issues.
- Provide knowledge management (KM) articles. After an incident is resolved, the process shall be documented as a KM article for future resolution and reserved in Remedy for future incident reference.
- Support staff working in a remote USCIS office or teleworking.
- Ensure IT services are rendered/ equipment tested on the day telework employees are in the office.
- Be available to support pre/post application release.
- Ensure staff is always in place to take the handoff from Tier 1 support and assist in meeting first call/contact resolution.
- Provide and document policies and procedures for Tier 1.5 team to follow.
- Develop and implement a Tier 1.5 SOP following a similar structure as Tier 1 SOP.

The Contractor shall ensure that Tier 1.5 staff is experienced with LANDesk remote resolution and with using LANDesk to push packages to workstations to complete software installation requests.

5.3.4 Incident Management

The Contractor shall, through successful implementation of incident management processes, restore unexpectedly degraded or disrupted service to users as quickly as possible in order to minimize the impact on the USCIS business. An incident, as it relates to NATIONS, is referred to an unplanned interruption to an IT service or a reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also considered an incident. The Contractor shall:

- Demonstrate expertise in incident management processes. Additionally, the Contractor shall adapt its processes and procedures to those already in place in USCIS after receiving copies of existing incident management documents from the Government.
- The Contractor's incident management team shall use the existing BMC ITSM, which will already be in operation at the start of this task order.
- Follow coordination procedures provided by the Government to ensure an efficient hand-off between the separate Incident Management and Problem Management Contractor and Government staff.

- Ensure that SD remains responsible for the ticket to resolution and is responsible for updating ticket information.
- Implement and update aging tickets in accordance with the SOP escalation procedures.
- Proactively monitor Automated Call Distribution (ACD), Incidents and Service Requests and queues to immediately identify a Critical/High priority incident or identify issues impacting services to USCIS users.
- Ensure the CIRT SOP is updated and maintained and implemented within the Government's response and communication timeline which will be available after award in the form of knowledge management document.
- Ensure that all Critical and High priority Incidents are communicated to appropriate Government points of contact and customers using government provided tools and communication methods and format.
- For critical incidents, ensure communications are distributed timely and hourly updates are completed throughout the lifecycle of the critical incident.
- Ensure proper teamwork is followed while conducting CIRT troubleshooting conference calls.
- Ensure DHS Enterprise Operations Center (EOC) escalations and reporting procedures are implemented and followed. Government will provide DHS EOC guidelines.
- Provide accurate reporting and statistics on all incidents and service requests.
- Perform weekly/monthly trend analysis for reoccurring incidents for escalation to problem management, process improvement, or customer training opportunities.
- Conduct trend analysis to relate Incidents to infrastructure changes, for escalation to problem management.
- Perform monthly trend analysis on tickets to determine performance improvements opportunities (time to resolution), process improvements, staffing improvements, and system enhancements opportunities.
- Perform trend analysis on queues or support organizations with aging tickets and provide tickets to the Government for escalation.
- Ensure participation in Change Advisory Board (CAB) or gate review meetings. Publish release dates and approved maintenance in Remedy or as specified by the Government.
- Provide trend analysis on all AQL's monthly.
- Ensure incident control processes are in place for the analysis of detailed historical data for accurate problem identification.
- Ensure compliance with AQLs for automated registration of incidents with accurate classification and details for successful problem management.
- Develop a Quality Control SOP and implement when approved by the Government.
- Coordinate with other USCIS divisions or supporting groups/contracts to provide a work around or resolve a critical incident.
- Remediation/Reason for Incident is to be communicated to the Problem Management Contractor and Government staff for analysis.

5.3.4.1 Security Incident Support

- In performance of daily functions, if the Contractor identifies weaknesses, vulnerabilities, threats, outages, or degradation of services, the Contractor shall immediately notify the USCIS service desk of these findings.
- When directed by the Security Operations Center (SOC), the Contractor shall act as on-sight incident handlers to perform computer incident response and mitigation/remediation activities required for security incidents.
- When requested, assist USCIS SOC and/or USCIS information system security personnel with technical or data gathering.
- As requested, provide technical assistance to the SOC during a security incident.
- Update security incidents/tasks within Remedy, as required.

5.3.4.2 Regional Alternate Information System Security Officer (AISSO)

The Contractor shall provide collateral duty AISSO support for each of the six OIT support regions to assist the CISNet General Support Systems (GSS) ISSO with the following:

- Provide information necessary to create\maintain regional certification and accreditation (C&A) documentation.
- Assist the ISSO with remediation of identified weakness\vulnerabilities.
- Support development of reports to higher authorities as required.

5.3.5 Knowledge Management

Knowledge management is the process of gathering, analyzing, storing and sharing knowledge and information within an organization. The primary purpose of KM is to improve efficiency by reducing the need to rediscover knowledge. In the context of this task order, KM refers to the operating information, processes and procedures maintained by the SD.

The Contractor shall:

- Ensure that Knowledge base articles are kept up to date and applicable to systems supported by this task order.
- Develop, implement and maintain a detailed knowledge base which will contain reference documentation, and resolution information.
- Participate in application Gate reviews to ensure KM articles are received and in place for USCIS SD and field staff to support the application.
- Conduct monthly trainings for all Tier1 and 1.5 staff on new KM to ensure familiarity and compliance.

5.3.6 Problem Management

Problem Management will be leveraged to identify and resolve structural and process problems within the USCIS IT Infrastructure and support services through a more formal approach to root cause and trend analysis. The Contractor shall:

- Establish an ITIL based Problem Management (PBMGT) capability that provides direct support to the SD and Incident Management as part of the approach to meet these requirements.
- Investigate, diagnose, and document problems with IT services and infrastructure.
- Keep a log of all potential problems in a Remedy problem management database.
- Investigate and diagnose problem root causes.
- Maintain a known error database and document workarounds and permanent solutions as part of a Knowledge Management article.
- Generate known error sub-processes and use KM to facilitate quicker diagnosis and resolution for future incidents or requests.
- Document reviews/analysis of major problems and unplanned service outages. Investigate for root cause and escalate to Government to prevent future major incidents.

5.3.7 Service Request Management

A request is defined as a contact from a user for information, or advice for a standard change or for access to an IT service. Service Requests (SRs) are handled by the SD Tier 1/Tier 1.5 and Field Support, and do not require a Request for Change (RFC) to be submitted. Processes and Service Level Agreements (SLAs) have been defined by the Government for SRs. In USCIS password resets/unlock are classified as Incidents.

- The Contractor shall update SR SOP and related policies to be implemented when Government approval has been granted.
- The Contractor shall implement the SR priority matrix and an escalation matrix provided by the government.
- The Contractor shall attempt to solve the majority of SR's remotely, as a First Call Resolution (FCR) and advise the Government where changes can be implemented to improve and reduce the number of SR's being submitted.
- The Contractor shall document clearly and detail all SR work completed and resolution steps in the SR Remedy ITSM.
- The Contractor shall use the SD Priority List to classify Priority SR's as critical SR's.
- The Contractor shall ensure that SR's are properly escalated and re-prioritized when escalated.
- The Contractor shall ensure proper communication with the SD for KM creation and Incident Management/Problem Management for future incident prevention.

5.3.8 Specialized Support

The Contractor shall provide enhanced support for priority callers. Priority calls shall be routed through the service desk. Priority caller processes are identified in Remedy KM.

The BMC ITSM Remedy is populated with priority user names. A list of priority users will be provided 30 days after award.

The Contractor shall:

- Develop a process to enable priority users to jump in front of the queue (e.g. all priority callers can press 8# on phone for immediate access to service desk staff).
- Determine if caller/end user meets "priority" criteria by comparing their information to the priority user name list.
- Update priority incident tickets every 2 hours when priority caller request is pending resolution and escalated to the next level of support. Resolve the request to meet all appropriate AQLs.
- Monthly review USCIS Leadership Directory and validate priority user name list in Remedy. If inconsistencies are found, the Contractor shall bring it to the Government's attention.
- Assign experienced IT professional(s) with comprehensive knowledge of all service desk activities.
- Oversee 100% of priority requests, incidents and problems from beginning to end. Escalate urgent and complicated issues as appropriate based on the situation and priority person.
- Become knowledgeable of legacy CLAIMS 3 (C3) and CLAIMS 4 (C4) systems by collaborating with application experts to assist with any LAN Desk issues that may arise.
- Develop a mature process whereby maximum number of priority requests are capable of being performed at a Tier 1 level.

The Contractor shall utilize the current USCIS remote support and software deployment. The Contractor shall:

- Utilize the tool for local software deployment and problem resolution;
- Utilize the tool for reporting software/hardware usage and compliance.

Note: the Contractor should assume that the versions and names of some toolsets will change during the term of this task order. Other tools may be adopted within the scope of the Service Desk task area.

5.4 Field Services

The Contractor shall provide a broad range of direct IT support services at USCIS CONUS and OCONUS sites under this section. Site locations are contained in Attachment 1.

5.4.1 Scope of Work

The scope of customers and equipment the Contractors shall support includes the following:

- CONUS and OCONUS Offices: approximately 230 domestic and over 28 overseas sites
- Supported staff: ~ 24,000
- Desktop and laptop systems: ~ 25,000
- Printers and peripherals: ~25,000
- Servers: ~1,200
- Wireless Devices: ~6,000

The following tasks are for the implementation of the USCIS Field Services. These task areas are as follows:

- Deskside Support (CPAF CLIN)
  - Asset Inventory Support (FPAF CLIN)
  - Disposal Preparation Support(CPAF CLIN)
  - Encryption Services (CPAF CLIN)
  - Video Conferencing and A/V O&M (CPAF CLIN)
  - Local On-Site Cabling (CPAF CLIN)
  - OCONUS Site Support (CPAF CLIN)
- Wireless Services (FPAF CLIN)
- Deployment Services (CPAF CLIN)
- Server O&M (CPAF CLIN)
- Training Support (FPAF CLIN)

All Concept of Operations (CONOPs) and Standard Operation Procedures (SOPs) documents referenced that are to be developed or updated by Contractor in this task area shall be provided to the Government within 10 days after NTP.

5.4.2 Deskside Support

The Contractor shall provide comprehensive local IT equipment support for systems and other items generally considered to be IT. The Contractor's end-user support staff shall have overall responsibility, under USCIS OIT management direction, for the organization's entire end-user computing environment throughout USCIS. This includes desktop and laptop computer hardware, software, and peripherals.

- The Contractor shall be available to be called on to provide on-site support for deployment and security remediation functions, some server support and some ad-hoc end-user training.
- The Contractor shall give its local end-user support and staff the flexibility and autonomy to respond to local requests for in-scope support. This flexibility and autonomy will require the Contractor to gather, analyze and report on end-user support trends and developments.
- The Contractor shall provide Deskside support services for all CONUS and OCONUS offices unless the Government requires these services to be performed for a USCIS employee using USCIS GFP while temporarily supporting another agency.
- The Contractor shall provide desktop, application and network application incident resolution support and manage user installation and relocation requests in accordance with Install/Move/Add/Change (IMAC) processes and procedures.
- The Contractor shall perform laptop image and encryption concurrently.
- The Contractor shall re-image workstations and laptops once Contractor or Government employee has turned in their GFP.

The Contractor shall provide end-user support to Federal and Contractor employees that use USCIS Systems. The premise of the NATIONS requirement is to provide deskside support to meet the needs of the task order. The Contractor shall provide a staffing model that delivers the support.

Note: USCIS develops desktop system images under a separate contract. USCIS will supply the Contractor with appropriate workstation and laptop images as they become available.

5.4.2.1 Asset Inventory Support

USCIS asset management is an inherently governmental activity. The Contractor shall assist USCIS OIT management and local site property managers in this task when required. The Contractor shall not assume any collateral duty positions.

To assist in this effort the Contractor shall:

- Assist the Government's property management staff in conducting physical inventories of USCIS IT assets at Government and other USCIS contractor sites containing authorized GFP.
- Conduct scheduled and periodic electronic inventories. Assist property managers with receiving and receipting of property; asset tag functions, and record new property received, conduct annual inventory of property, transfer of property to other organizations where appropriate, and process computer equipment for excess and/or disposition within the parameters of USCIS guidelines
- Report all discrepancies.
- Ensure site support staff Follow USCIS property management procedures.

5.4.2.2 Disposal Preparation Support

The Contractor shall utilize current USCIS methods for disposal preparation. Disposal preparation is defined as wiping/degaussing hard drive prior to equipment removal. The Contractor shall:

- Ensure disposal policies and procedures are followed
- Ensure every device is wiped/degaussed prior to removal from site

5.4.2.3 Encryption Services

The Contractor shall utilize the current USCIS encryption tool or the Governments choice of tool in the future for hardware encryption. The Contractor shall:

- Utilize tool to encrypt laptop computers;
- Administer and manage the encryption tools application server;
- Ensure laptops are properly encrypted;
- Encrypt laptops that are discovered without encryption;
- Provide password recovery for encrypted devices.

5.4.2.4 Video Conference and Audio/Video Operations and Maintenance

5.4.2.4.1 Local Video O&M

The Contractor shall be responsible for general local video operations and maintenance support as part of normal IT site support duties. This task does not include designing, engineering, specifying or acquiring video equipment.

- This support shall include basic troubleshooting of system problems and repairs, when they are identified by enterprise video support staff.
- The Contractor's site support staff shall work with enterprise level voice and video engineers and technicians to conduct more detailed remote troubleshooting and repairs.
- The contractors site support staff shall assist in setting up presentation devices and Video Conference units and provide basic troubleshooting support as needed.
- The Contractor shall set up, ensure functionality, be available during events and shut down video conferences.

5.4.2.4.2 Local Audio O&M

The Contractor shall perform local voice operations and maintenance support related to video teleconferences. This support shall include basic troubleshooting of system problems and repairs when they are indicated by enterprise voice support staff. This task does not include designing, engineering, specifying or acquiring voice communications equipment.

- The Contractor's site support staff shall work with enterprise level voice engineers and technicians in order to conduct more detailed remote troubleshooting and repairs.
- The Contractor shall provide local basic training and assistance to USICS employees as needed.

5.4.2.5 Local On-Site Cabling

The Contractor shall be responsible for small-scale local cabling support. This support shall be limited to replacement and/or the re-patching of patch cables within remote wiring closet or server rooms and running individual cables. In general, larger-scale cabling services will be provided under a separate contract vehicle. The Contractor shall:

- Ensure that technicians have basic cabling skills that shall include the ability to make straight-through and rollover cables from raw cable and RJ-45 connectors and then test and certify them to USCIS cable plant standards that will be provided as Government Furnished Information (GFI).
- Be responsible for restarting wiring closet cabling electronics including switches or other Network devices as Directed by the Government.

- Be responsible for the simple replacement of defective cabling electronics and the simple replacement of components such as switch blades.
- Perform only those local cable services that are required to maintain continuity of service or which are specifically directed by the USCIS OIT. Local demands for cabling activities shall be processed through the service request process

5.4.2.6 OCONUS Site Support

When the Contractor is present on-site at OCONUS locations, they shall provide the same level and type of site support outlined in field services support sections. USCIS OIT will require the Contractor to maintain a staff of support technicians who will travel periodically to USCIS OCONUS sites.

Note: USCIS defines its offices in Hawaii, Guam, Saipan and Puerto Rico as CONUS sites.

There are 28 OCONUS sites, as identified in PWS Attachment 1. Most of these OCONUS sites are located at U.S. Embassies and Consulates and require network services through the State Department. U.S. Embassies and Consulates require contractor personnel cleared NSI TOP SECRET access to gain access. The contractor will provide a sufficient number of personnel with NSI TOP SECRET clearences to perform duties specified.

The Department of State's Diplomatic Telecommunications Service Program Office (DTSPO) provides communications for all OCONUS USCIS sites. An interface between the DTSPO and DHS OneNet is provided. The Contractor shall:

- Designate staff required to provide these services, meet the personnel security requirements and travel to these sites. Staff may be required to travel with less than 24 hours' notice.
- Ensure staff assigned to this area shall have appropriate training certifications, experience and skills to handle the broad array of IT services required at international sites including network installation and troubleshooting, server installation and troubleshooting and desktop installation and troubleshooting.
- Ensure Contractor staff is equipped with the necessary tools, techniques, processes and procedures to fulfill all IT Infrastructure requirements while visiting a site.
- Ensure that encryption and disposal procedures are followed.

5.4.3 Wireless Services

The Contractor shall provide on-site support to meet all service level agreements and manage the daily processing of Mobility Services and device orders as well as the inventory of services and devices for all of USCIS as part of the USCIS Mobility Team. Mobility services and devices is defined in the USCIS Mobility Management Directive as cell phones, smartphones, tablets, satellite phones, both internal and external air cards, hotspot cards, thin client devices, and all related services and functions regarding those devices. The Mobility Team shall provide customer support establishing the integrated process, procedures, effective coordination, and continuity of operations between the DC and Vermont locations. The Mobility Team shall provide fulfillment processing for mobility product requests, technical assistance, supplier

management assistance, and customer service. As of January 2016, the Mobility Team supports approximately 8,000 Mobility devices and 1,000 telework individuals.

5.4.3.1 Order Fulfillment

Initial Order Triage/Validation
Utilize the current USCIS Mobility contract Cellular Wireless Managed Services (CWMS) and USCIS tools and databases to provide oversight of all Mobility requests to ensure that all required information is present before processing an order. Validate order information to ensure that all policies and contractual requirements are adhered to.

Order Submission
The contractor shall submit, modify, or cancel order submissions within the scope of their assigned duties.

Order Follow up and Closeout
Ensure that the customer is updated on the status of their order throughout the entire acquisition process and validate with the Service Provider that the intended service was provisioned and billed correctly before closing out an order. The Contractor shall also perform follow-up actions as needed on lines of service i.e. remove international service when a customer's international service trip has completed.

5.4.3.2 Account Review

Perform account management functions/reviews concerning Mobility devices to include but not limited to the below when required according to the Mobility team SOP.

Follow-up Actions
Complete all follow-up action tasks related to ordering/managing the mobility inventory listed within the Mobility mailbox.

Zero and Minimal Usage
Review all zero and minimal usage lines, suspend per current policies or send out notification emails.

Usage Thresholds
Review current management usage thresholds and send out email notifications to offenders listed.

Suspended Devices
Review all devices suspended over 30 days and cancel service if the line is not listed as an indefinite suspend.

MDM

Review all devices not in compliance with MDM and send notification emails and suspend devices based on current Mobility policies.

Ported Lines
Review all ported lines to ensure lines that are successfully ported from one carrier to another.

Loss Report
Review discrepancies between users who are no longer part of the Account Management listing, but still are assigned a mobility device.

Device Upgrades
Review all inventory, and perform device upgrade projects based on management guidance and free devices on the contract.

Duplicate Services
Review all lines with duplicate service and ensure a proper management approved justification is listed in the portal.

Audits
Perform routine audits of the wireless inventory to ensure proper accountability and assist with the annual audit of all devices.

Wireless Inventory
Manage a local on-hand stock of devices for contingency and break fix requirements.

5.4.3.3 Customer Support

Incident Management
Monitor and respond to Tier 2 break/fix customer requests within an incident management queue. The Contractor shall assess malfunctioning devices to determine if initial triage (re-boot, battery removal, charging) will resolve customer reported issues.

VIP Requests
Provide VIP technical support services and one-on-one instruction if needed.

Training
Provide customer training on requests for the use of devices, services, and the proper ordering procedure through the current wireless ordering system. Assist the customer with their additional features such as international capabilities, plans, dialing instructions.

Customer Satisfaction

Coordinate with the customer to ensure that they have received their new service and/or device and that it is working correctly. Respond to all customer complaints in a timely and professional manner.

Replacements
Coordinate with the USCIS Service Desk, SNOC, CWMS Help Desk, Data Center 2 (DC2) Service Desk, Data Center 1 (DC1) Service Desk, the end user and program office property custodians to identify and suspend service on lost devices; identifying available hardware and assisting with ordering replacement hardware.

Warranty Claims
Process all warranty claims for devices with a warranty issue within the allotted warranty time period.

International Support
Provide guidance and support to USCIS personnel on official travel or stationed overseas ensuring any available and necessary roaming devices and features are ordered and the customer is made familiar with the operation and expectations.

5.4.3.4 Administration

Wireless Support Team Group Mailboxes
Monitor and respond to all incoming requests (i.e. responsibility to manage the content of the mailbox). The group mailboxes will be a distribution point for all wireless services questions and issues related to order provisioning and technical service issues. File all emails if required with pertinent information in the appropriate folders on the shared drive.

Wireless Support Team Group Main Phone Line
Monitor and respond to all incoming requests (i.e. responsibility to answer the main line). The main line will be a distribution point for all wireless services questions and issues related to order provisioning and technical service issues.

Communication
Coordinate with the USCIS Service Desk, CWMS Help Desk, Data Center 2 (DC2) Service Desk, Data Center 1 (DC1) Service Desk, Security and Network Operations Center (SNOC) to ensure the customer is provided a consistent and reliable level of service.

Standard Operating Procedures (SOP)
Document and update all desk procedures and SOPs related to the wireless tasking. Provide informational broadcast messages to the field on the proper use of devices and services. Review and update the Service Desk scripts related to wireless.

Reports

Generate a weekly report on general activities as well as workload statistics and metrics to include numbers or orders processed, users assisted, devices on hand, etc.

5.4.3.5 Required Skills

All Contractor staff providing Mobility support shall have the following minimum qualifications:

- Experience with Microsoft Word – ability to develop and use style sheets, understanding the use of revision marking, and the ability to create and maintain automated tables of contents and tables of figures.
- Experience with Microsoft Excel – ability to generate and maintain cross linked tables, ability to create complex cascading formats and the ability to create pivot tables.
- Experience with iOS, Android, and Windows phone operating systems. Experience with Mobile Device Management solutions and Citrix telework solution.

5.4.4 Deployment Services

Deployment Services requires travel to CONUS and OCONUS sites to perform local on-site cabling, server and/or other IT equipment setups, installations or relocations of new or upgraded software. Desktop deployment services and support is also required by USCIS OIT. Any IT equipment move/refresh greater than 20 systems, conponents or peripherals will be categorized as a deployment.

The Contractor shall:

- Be responsible for implementing deployment plans and overseeing travel arrangements.
- Coordinate large office moves, opening of new facilities, relocations and refresh activities.
- Ensure that servers, minor network equipment, computer workstations and printers are configured, installed on the network and tested as scheduled.
- Ensure deployment staffs attend weekly OIT Facilities calls, Rollout Operations Center (ROC) calls, deployment calls, release management calls and Application Support Center (ASC) calls to ensure IT requirements are provided for these moves, openings and relocations.

The majority of the deployments will be made after working hours, Monday through Friday, and/or on weekends (possibly holidays) to become operational the following Monday morning. During non-deployment, the Deployment personnel will provide local Deskside support services.

Deployment manager and personnel are required to be in close proximity to a major airport for easy and less expensive travel.

5.4.4.1 Pre-Deployment

Pre-deployment requirements include developing a preliminary deployment plan, scheduling and coordinating all infrastructure activities, and preparing a pre-site survey package.

In order to accomplish this, the Contractor shall:

- Contact customers and access/review all available site documents, and identify any current and planned activities that would affect the site and deployment.
- From the information gathered and analysis, develop a preliminary deployment plan and schedule.
- Coordinate all infrastructure activities prior to visiting the site and prepare a pre-site survey package based on the information gathered and analysis.

The Contractor shall provide the following pre-deployment activities at USCIS facilities:

- Perform site surveys of the USCIS facility. This shall include filling out site survey forms, which shall capture all pertinent required information.
- Coordinate with site staff and Products and Technology Branch staff well in advance of a scheduled deployment. All deployment activities shall take place with specific timelines. Answer all questions and/or concerns site staff/Products and Technology Branch staff may have with scheduled deployment activities.
- Inventory IT assets on-site by each location. Identify equipment status to be replaced, upgraded, or left operational. Develop deployment requirements and Bills of Material (BOM) by coordinating with the appropriate OIT management office and managing EUS deployment activities.

5.4.4.2 On-Site Installation

In support of each project, a qualified Contractor team with appropriate management oversight is needed to travel to scheduled upgrade sites and support the upgrade activities.

At a minimum, the following activities are required during on-site installation:

- Power On/ Login
- Testing for Network Connectivity
- Configuration of Peripherals
- User Data Migration
- Personal Bookmarks, Icons, Access Rights, Security Settings
- Configuration of Office Automation Applications
- COTS Software Installation
- Enterprise Application Installation & Configuration
- Emulation Software Installation & Configuration
- Active Directory Location or other updates
- Use of LANDesk or other remote tools for Software deployment

5.4.4.3 Post-Deployment

The Contractor shall be committed to providing customer satisfaction and work diligently through the post-installation period. Once the installation is complete, on-site, post-installation support shall be required following acceptance to ensure all business operations are functional.

As part of post installation support, the Contractor shall:

- Provide technical guidance and assistance to site end users;
- Train site personnel on the components and how to keep the system functioning

- Assist the site personnel to communicate, coordinate, and facilitate any deployment project activities on site;
- Before leaving the site, conduct an exit brief with site end users ;
- Upon returning from the site, finalize a trip report which includes "lessons learned", trip cost analysis and any new or modified migration process as a result; and
- Provide an "As Built" document to the USCIS Task Manager.

The Contractor's activities shall be tightly integrated with OIT to assure service continuity and resiliency during and after deployments.

5.4.4.4 Support for Deployments under the USCIS TITAN

USCIS acquires much of its IT equipment in a streamlined fashion through the USCIS First Source contract vehicles. The Contractor shall provide the following:

- Install workstations and other equipment at HQ and field sites after the First Source Contractor has delivered the pre-imaged system to the subject site. This requirement shall be limited to network connection, peripherals, and data and software migration.

5.4.5 Server Operations and Maintenance

The Contractor shall be able to support all agnostic operating systems within USCIS except those servers managed under other contracts. Supported operating systems include Windows Server 2003 and Windows Server 2008 (Redhat and Linux where applicable).

5.4.5.1 Server and Network Operating System support

The Contractor shall:

- Administer local servers, accounts and those groups operated by USCIS or delegated to it.
- Provide support for local resource server in the field. Resource servers are defined as File and Print Servers.
- Provide Server Hardware and Operating System support for all other sites in the field.
- Install patches and releases
- Perform routine Maintenance
- Server health checks
- Server monitoring and reporting
- Recover and restore data
- Provide after-hours cell phone and on-call support to respond to local network outages.

The Contractor shall provide sufficient DSM support at USCIS facilities during emergency installations of patches and standard releases. The Contractor shall request approval, in writing, in response to emergencies from the local IT Branch Chief or CSL and the COR. If Government staff cannot be reached for approval, the Contractor shall identify the emergency situation in writing to the COR and local Branch Chief/CSL before responding to the crisis.

5.4.5.2 Local Storage and Backup Support

The Contractor shall:

- Be responsible for storage and backup support in the field.
- Coordinate scheduling and pickup of backup media with offsite media storage vendors under separate USCIS contracts.

The Contractor shall perform the following routine tasks:

- Perform daily backups;
- Check and verify the status of previous night's backups;
- Review the backup logs to ensure the backup application is running properly and no problems exist;
- Ensure the virtual backup libraries have an adequate number of virtual tapes available to perform the next night's backup tasks;
- Ensure the tape libraries have an adequate number of tapes available to perform the next night's backup tasks;
- Apply patches to backup applications;
- Work with application owners to add, change, and remove client backups;
- Notify stakeholders on issues in a timely manner;
- Add/Remove backup storage devices;
- Prepare backup tapes for offsite rotation ;
- Local capacity planning of backup infrastructure to meet the future needs;
- Provide recommendations for continuous improvement of the overall data protection within the environment.

5.4.6 Training Support

USCIS Training and Career Development Division (TCDD) has identified a need for dedicated, on site IT Contractor support for the daily O&M of the USCIS Academies located in Williston, VT, Lee's Summit, MO and Dallas, TX, Laguna Niguel, CA as well as support for the Learning Management Systems (i.e. LearningEDGE and Skillport). IT support services to TCDD are needed for USCIS online courses, staff and students (when on site). This support includes the preparation for training classes in areas such as equipment, facility and system planning, re-image of desktop systems to support incoming students, and problem and incident response during scheduled training sessions.

5.4.6.1 USCIS Academy Support

The Contractor shall provide USCIS Academy support as follows:

- Imaging,
- Encryption,
- Outfitting as many as 50 laptops per week to support classes,
- Work with the VPN team to provide remote access,
- Load class materials and set-up students e-mail access,
- Student workstation desktop support.

5.4.6.2 Learning Management Systems IT Support

The Contractor shall provide IT services for Learning Management Systems (LMS), which include Trio and Learning Edge, as follows:

- Local Area Network (LAN) Server Administration.
- Maintain LMS infrastructure hardware resources located in South Burlington, VT.
- Provide assistance in course loading to the LMS and initial functionality/compatibility testing.
- Account creation (LearningEDGE & Skillport).

5.4.6.3 Tier 2 Support

The Contractor shall provide Tier 2 support as follows:

- Customer Service -working directly with the SD and USCIS staff 6:00AM through 6:00PM Monday through Friday on LMS related tickets
- Tracking and reporting of SD issues related to specific courses
- LMS Account Remediation

5.4.6.4 Tier 3 Support

The Contractor shall provide Tier 3 support as follows:

- Microsoft (MS) Windows Server Administration
- MS SQL server administration
- Daily maintenance and backups of servers
- Install operating system patches, upgrades, restores, etc.
- Install application Software patches as needed

5.5 Service Center Services

The Contractor shall provide a broad range of direct IT support services at the following facilities that are critical to the USCIS mission.

- California Service Center (CSC), Laguna Niguel, CA;
- Vermont Service Center (VSC), St. Albans, VT;
- Nebraska Service Center (NSC), Lincoln, NE;
- Texas Service Center (TSC) Dallas, TX.;
- National Benefits Center (NBC), Lee Summit, MO;
- National Records Center (NRC), Lee Summit, MO;
- Potomac Service Center (PSC), Arlington, VA

The CSC, VSC, NSC, TSC and PSC are large processing centers that receive and adjudicate applications and petitions for immigration benefits. The NRC provides records management services relating to physical A-Files and associated materials. The NBC provides screening/clearance for the Direct Mail Program.

5.5.1 Scope of Work

The scope of customers and equipment the Contractors shall support includes the following:

- 24X6 (Monday –Saturday) on-site support for CSC, NSC, TSC, VSC, NBC, and NRC

- 0600 – 1800 (Monday – Friday) for PSC

In addition to field support**,** the service centers will require additional direct IT support:

- Service Center IT Support
- CLAIMS 3 Support (including supporting interfaces)
- CLAIMS 4 Support
- Electronic Immigration System (ELIS) Support
- Treasury Enforcement Communications System (TECS) Support
- Enhanced Server Support

The Field Services AQL also applies to the services rendered at the service centers.

5.5.2 Service Center IT Support

The Contractor shall provide comprehensive local equipment support for IT systems and other items generally considered to be end-user support. The Contractor shall adhere to functions identified under Field Services in providing support to CSC, VSC, NSC, TSC, NBC, NRC and PSC.

The Contractor shall provide the following in addition to adhering to the field services requirement at the service centers:

- Service Centers have a lot of work at home / telework employees hence; the Contractor shall ensure that IT services are rendered/tested on the day telework employee are in the office.
- The Contractor shall provide support to work at home (telework) users utilizing VPN and citrix to complete their work.
- The Contractor shall provide remote support to work at home users using USCIS provided remote support tool.
- The Contractor shall be available to support pre/post application releases.

5.5.2.1 Site Support

USCIS Service Centers shall generally have access only to SBU information but, Service Center contractor support staff shall work with task management and the SOC to remediate classified (NSI SECRET) data spills at each Service Centers. Site leads at each Service Center, Stennis and HQ USCIS shall serve as Tier I support staff in remediating "spills" of NSI classified data specified in DHS 4300B. These "spills" will occur periodically during the course of a year with at least 23 happening in the past year. These incidents are normally caused when a classified document is loaded into an unclassified system such as FIPS, FDNS-DS or is emailed on an unclassified email system to an unauthorized recipient. The following locations had classified spillage incidents over the past 12 months: Boston, Tampa, Denver, Seattle, NY, Arlington Asylum, DC, Frankfurt, NBC/NRC. As such, the Contractor shall staff the CONUS

Service Centers, (currently 6 locations) section 5.5, the Stennis Service Desk and National Capital Region (NCR) with employees cleared to NSI SECRET.

The Contractor shall use its collateral duty Alternate Information Security Systems Officers (AISSOs) designated under section 5.3.4.2 whenever possible to insure the proper handling of classified data or documents in the SBU environment. They should hold SECRET clearances.

The Contractor shall designate certain Site Support staff in advance to handleclassified data spills wherever possible.

5.5.3 CLAIMS 3 (C3) - LAN Support

5.5.3.1 Enhanced C3 Support (for CSC, VSC, NSC, TSC, NBC, NRC, AAO, PSC)

USCIS has a requirement to provide enhanced onsite support for the C3 system. Requirements include support to print forms, backup servers, upload and download data, install various tables, interface releases, CLAIMS releases and various other daily, weekly, and monthly operational tasks that support C3 operations. Support of this system is critical to the USCIS mission. Enhanced C3 Support is required at the Service Centers and NBC, NRC, AAO (Administrative Appeals Office) and Baltimore Field Office.

1. **Daily Support**
   The Contractor shall:
   - Upload/download data to/from CLAIMS Mainframe;
   - Run interfaces: Family Based Adjustment of Status Interface (FBASI), Biometric Retrieval Utility (BRU), Customer Relationship Information System Interface (CRISI), Integrated Card Production System – Print Services (ICPS-PS), Adjustment of Status (AOS) Scheduler, Travel Document Printing System (TDPS) Push, Refugee and Asylee Parole System Employment Authorization Documents (RAPSEAD), Print Server, National File Tracking System Interface(NFTSi), Interim Interagency Border Inspection System (IBIS), and 765 System Qualified Adjudication (SQA) for Temporary Protected Status (TSP).
   - Complete backups and copy to report server of C3 LAN data;
   - Provide print services for C3 notices to include receipts, decisions, transfers, scheduling of biometric appointments and interviews;
   - Download and print E-filing cases;
   - Add/modify/delete User Access Requests;
   - Correct “stuck” cases as needed based on request from business operations.

2. **Periodic Support**
   The Contractor shall:
   - Install monthly zip code table changes;
   - Install ad-hoc security patches;
   - Assist DBAs with server issues, as needed;

- Install quarterly configuration releases;
- Install interface releases as needed;
- Install C3 LAN client server releases;
- Troubleshoot any LAN Desk deployment issues.

3. **National Production System (NPS) Support**
The Contractor shall:
- Install monthly security patches;
- Complete nightly backups and prepare for off-site storage;
- Assist DBAs with restarting/powering down servers, as needed.

5.5.4 CLAIMS 4 (C4) - LAN Support

5.5.4.2.1 Enhanced C4 Support (for CSC, VSC, NSC, TSC, NBC, NRC, AAO, BAL, PSC)

USCIS has a requirement to provide enhanced onsite support for the C4 system. Requirements include support to print forms, backup servers, install CLAIMS 4 releases and various other daily, weekly, and monthly operational tasks that support C4 operations. Support of this system is critical to the USCIS mission. Enhanced C4 Support is required at the Service Centers and NBC.

1. Daily Support
The Contractor shall:
- Complete backups as needed for C4 servers;
- Provide printing services for C4 notices to include receipts, decisions, transfers, scheduling of biometric appointments and interviews; Download and print E-filing cases;
- Add/modify/delete User Access Requests;
- Correct “stuck” cases as needed based on request from business operations.

2. Periodic Support
The Contractor shall:
- Install ad-hoc security patches;
- Assist C4 DBAs with server issues, as needed;
- Install quarterly configuration releases;

5.5.4.2 ELIS Support

5.5.4.2.1 Enhanced ELIS Support (for CSC, VSC, NSC, TSC, NBC, NRC, AAO, BAL, PSC)

USCIS has a requirement to provide enhanced onsite support for the ELIS system. Requirements include support to print forms and various other daily, weekly, and monthly operational tasks that support ELIS operations. Support of this system is critical to the USCIS mission. Enhanced ELIS Support is required at the Service Centers and NBC.

1. Daily Support
The Contractor shall:

- Add/modify/delete User Access Requests;
- Perform equipment maintenance and configuration locally for ELIS access

2. Periodic Support
The Contractor shall:

- Install ad-hoc security patches through GPO application;
- Assist ELIS DBAs with workstation issues, as needed;

5.5.5 After-Hours Support (Service Centers, PSC NBC, NRC, HQ and Bloomington HQ)

The Contractor shall provide after-hours cell phone and on-call support to respond to emergencies (e.g. serious damages to Government equipment/property, cause for loss of productivity), critical security, and network (e.g. devices, circuits, etc.) incidents or outages. The Contractor shall be measured on their response time to incidents according to the AQLs.

The Contractor shall provide sufficient DSM support at Service Centers, NBC, NRC, and HQ during emergency installations of patches and standard releases. The Contractor shall request approval, in writing, in response to emergencies from the appropriate local Government staff and the COR. If Government staff cannot be reached for approval, the Contractor shall identify the emergency situation in writing to the COR and local Government staff before responding to the crisis.

5.6 Account Management

The Government requires the Contractor to support OIT Account Management activities. The Contractor's functions will not include inherently governmental activity of account management. The Contractor shall assist Federal employees by processing requests and performing administrative functions associated with account management activities. Final authority to grant, revoke or change accounts and accesses shall be a Governmental function.

5.6.1 Scope of Work

Contractor support for Account Management shall include the following:

- Provide staff support coverage during the hours of 6:00 am through 10:00 pm Monday through Friday local time;
- Process requests for network account creation, modification and deletion;
- Assist the Government with completion of documentation such as Standard Operating Procedures (SOP) that pertain to areas being managed by Contractors;
- Incident troubleshooting tickets review and resolution.
- Identifying an account administrator lead capable of managing systems access for Active Directory, Exchange, ELIS, PICS, CPMS, FIPS, EDMS, C3-LAN, and CLAIMS 4. Ability to perform CIS1 Account Creation, Deletion, Modification, and role definitions within USCIS CIS1 Active Directory Domain.

- The Contractor shall staff the Service Desk with agents who are qualified to serve as ICE Password Issuance and Control System (PICS) officers by task order cutover. PICS is a mainframe system used to manage access to USCIS critical "national" systems. To be eligible to serve as PICS officers, individuals must hold T1 Public Trust "clearances" supported by a full Background Investigation (BI). There is no NSI security clearance required.

All CONOPS and SOP's referenced to be developed or updated by contractor in this task area are to be provided by contractor within 10 days after NTP. Existing CONOPS and SOPs can be found in Remedy under Knowledge Management. The Contractor shall provide a weekly and monthly report of account management work. The Contractor shall also provide a quarterly report on all accounts that have not been accessed in 90 days for the Government to review.

5.6.2 Account Management Branch

The Account Management Branch shall reside at the Stennis Space Center in Mississippi. The Contractor shall:

- Manage workload through the use of Remedy System.
- Manage tasks, perform queries, complete Work Orders, create, assign and prioritize tasks within the Remedy System.
- Be knowledgeable of the use of scanning hardware and software, as well as the use of Portable Document Format (PDF) files for the creation and management of documents.
- Be knowledgeable with Digital Network Fax Systems used for customer requests sent to the USCIS SD, New Hire queue as well as Account Management.
- Manage electronic documents in performance of all Account Management work.

5.6.3 Account Management Tasks

The Contractor shall support the creation and management of approved accounts under OIT authority, providing staff support at account management section offices at Stennis Space Center, Mississippi. These staffs shall work directly with the EUS section Federal staff members. The Contractor shall:

- Be responsible for creating and managing approved accounts and groups for users and systems according to USCIS IT Security policies and procedures to be supplied after award.
- Be responsible for managing access privileges upon request; according to USCIS IT Security policies and procedures.
- Be responsible for serving as PICS officers to update user clearances, name changes, jurisdiction changes, etc.
- Disable accounts when directed.
- Respond to an average of four ad-hoc information queries and requests per month.
- Actively monitor activity on primary network and application accounts for which it has administrative responsibilities.

- Suspend or disable accounts that have been inactive for 45 days or more, with prior approval, if no termination request/ticket has been placed.
- Report account suspensions to OIT Management daily as they occur and shall inform the EUS account management section offices one week before carrying out 90-day deletions.
- Provide daily and weekly reports to support all tasks and responsibilities as outlined that are conducted through the use of Remedy System.

5.6.4 Specialized Account Management Tasks

The Contractor shall:

- Identify, authenticate, and create initial LAN and email approved accounts after validation of the user's identity and authorization by the Government.
- Have oversight over all USCIS account and access information; to include, but not limited to Active Directory/Exchange, applications, databases, Lightweight Directory Access Protocol (LDAP), Single Sign-On (SSO), and other OIT access management mechanisms.
- Be responsible for Add, Modify, and Delete all approved accounts and groups (user and system) according to USCIS Change Control and IT Security policies and procedures.
- Be responsible for Add, Modify, and Delete all approved account and directory information according to USCIS Change Control policies and procedures
- Be responsible for making requests to USCIS-PICS-TIER2 support to update user clearances, name changes, jurisdiction changes, etc.
- Serve as a central coordination point for all identity management matters for all of USCIS. This includes, but is not limited to, coordination with field administrators, PICS Officers, Office of Security and Integrity (OSI), SD, system owners, and other entities attempting to establish, modify, or request account or identity management services.
- Maintain a USCIS-provided Remedy repository of received access management forms and documentation specified within USCIS policy requirements.
- Establish periodic review and audit of accounts to ensure: (a) accounts are properly authorized, and (b) accounts are authorized in a manner consistent with Personnel Security guidance and database systems.
- Support Incident Response with the termination of account services.
- Support Incident Response with ad-hoc information queries and requests.
- Be responsible for maintaining identity information consistent with Privacy Act record keeping requirements.
- Be responsible for management of Cisco Secure Access Control System.

5.7 Hardware Incident Resolution

The Contractor shall perform this function through a Contractor Hardware Resolution Group (HRG) whose purpose is to process hardware problem tickets and to make arrangements for

resolution. It shall be the responsibility of Contractor CONUS and OCONUS Site Support staff to resolve the problems either directly or by assisting warranty vendor staff.

USCIS has instituted a Comprehensive Refresh Program with the goal of replacing all equipment before the end of its warranty. As such, USCIS intends that hardware problem incidents will be resolved, with parts supplied by the warranty vendor. In many cases, the parts will be installed by the warranty vendor. The NATIONS Contractor shall serve as USCIS' point of contact for warranty parts as part of its larger task of resolving IT incidents.

However, the Comprehensive Refresh is being implemented in phases and some equipment will not be under warranty by the effective date of this task order.

5.7.1 Hardware Incident Resolution Activities

5.7.1.1 Equipment Categories

- Desktop Equipment
    - Workstations
    - Laptops
    - Personal Printers
    - Scanners
- Site-level Networked Equipment

  Hardware Incident Resolution support for servers, network storage devices and other special-purpose equipment is limited to O&M repairs, including PCA parts, of equipment that is out of warranty or service agreement. Upgrades, expansions and major configuration changes are performed by the USCIS OIT Enterprise Infrastructure Division.

  Examples of site-level networked equipment are:

    - Site-level servers
    - Networked scanners
    - Networked printers
- Enterprise Equipment

  In general, enterprise equipment is maintained through support agreements with the manufacturer or other vendors.

  In some cases, equipment remains in service after it is no longer eligible for manufacturer maintenance. In those cases, it is eligible for PCA parts support and best-effort contract support.

  In no case shall the Hardware Incident Resolution task or PCA be used to supply manufacturer or other vendor support out of warranty.

  Examples of Enterprise Equipment are:

- Enterprise servers
- Enterprise storage appliances
- Security appliances and devices
- Network devices including routers, switches, firewalls and VPN appliances.

- Excluded Equipment
  - Personal equipment
  - Contractor-owned equipment
  - Non-USCIS government equipment

5.7.1.2 Hardware Repair

The Contractor shall troubleshoot and resolve hardware incident(s) that involve failure of a permanent, non-consumable part.

5.7.1.3 Hardware Maintenance

The Contractor shall identify and resolve hardware incidents and service requests of a consumable part(s) that have defined service lives and are repaired periodically during the service life of the systems.

Consumable parts

Consumable parts include toner, drums, belts and rollers for printers, main batteries for uninterrupted power supplies and laptops, CMOS batteries for workstations and laptops, CMOS and RAID batteries. During the course of this task order, other classes of parts may be added.

Peripheral parts

Peripheral parts include items such as cables and connectors that become damaged and need to be replaced. These items are neither part of the covered equipment nor consumable items and usually are not covered under warranty.

- The Contractor shall provide replacement parts for specialized peripheral parts that fail.
- The Contractor shall not provide replacements for general-use parts such as standard USB, parallel or monitor cables.

5.7.1.4 Hardware Upgrade

Hardware upgrades are required when a system's hardware configuration does not meet the requirements of software or other hardware. Upgrades include increases in Random Access Memory, increases hard-drive capacity, video or audio cards and processors.

The Contractor shall not process requests for hardware upgrades under this section because they are not repairs. Upgrade parts will be supplied by the Government.

When the Contractor receives an incident or service request for items such as RAM, video that may involve upgrades, the HRG shall:

- Check the working log of the ticket to make sure that the request is to replace a part that actually failed.

- Check the shipping specifications of the hardware system for the base specification of that piece of equipment. The request for repair should match the original specification.

If the checks indicate that the request is an upgrade rather than a repair, the Contractor shall reject them and report it to the OIT official charged with approving PCAs. The HRG is free to escalate questions or protests to the PCA authorizing official.

Note: System configuration varies within model runs. The Contractor should not assume that all instances of a model shipped with the same RAM, hard-drive capacity, etc.

5.7.2 Hardware Resolution

The Contractor HRG shall perform these functions:

- Incident tracking and resolution or cancellation.
- Analyzing and estimating costs for each incident.
- Escalating incidents to OIT management where necessary.
- Arranging for warranty vendors to dispatch technicians or ship parts.
- Acquiring and shipping parts for out-of-warranty incidents that are approved for resolution.
- Coordinating incident resolution with NATIONS CONUS and OCONUS Site Support.
- Arranging billing for shipping and parts acquired under this section

Repair and Maintenance Parts

All repair and replacement parts should meet Original Equipment Manufacturer (OEM) specifications. In some cases, the use of non-OEM consumable parts may void an active warranty.

- The Contractor shall periodically check OIT Equipment Standards and the current catalog for warranty warnings.
- The Government will notify the HRG of additions or deletions of equipment from the catalog.
- The contractor will provide detailed weekly reports on expenditures to the COR and CO.

5.7.3 Warranty and Maintenance Agreement Repairs

The USCIS Service Desk and the HRG shall coordinate repairs under warranties and maintenance agreements for all incidents referred to it.

The Contractor shall maintain and develop contacts with warranty service and parts suppliers and with the vendors of extended maintenance services. If practical, the Contractor shall obtain manufacturer certifications for its technicians to streamline the process of obtaining warranty support.

The Government will provide and update warranties and maintenance agreements for equipment in the USCIS inventory.

5.7.3.1 Warranty Resolution Process

Hardware incident processing should essentially follow the same process for warranty resolutions here and in the PCAs section below. The Contractor shall adhere to the following:

- Incident opened and assigned
- Troubleshooting reveals a hardware failure
- Responsible technician creates a hardware request task within the incident;
    - Some warranty vendors allow certified technicians to obtain parts or on-site support directly. If the Contract chooses to use this provision, the technician shall still create the hardware task, document it completely with the information required for PCAs described in PCA Request Analysis section below.
- HRG analyzes the request and determines that the equipment is covered by warranty or a maintenance agreement.
- The HRG contacts the warranty or maintenance agreement vendor.
- The HRG (or certified technician) schedules delivery of the part or visit by the vendor.
- The HRG (or certified technician) documents resolution and closes the task.

5.7.4 Parts Stores

The Government intends to establish and stock storage lockers at Headquarters and larger field offices. These storage lockers will be stocked with consumable, repair and peripheral parts for equipment in the active inventories of local sites.

The Government will set stocking levels in consultation with the Contractor and the hardware repair and maintenance histories for site-level hardware, as documented in Remedy Incident Management.

Government CSLs will supervise the operation of Hardware Parts Lockers. Access will be strictly limited and parts will be issued only with documentation of accompanying incidents and service requests.

5.7.5 Per-Call Authorization

PCA is the process of obtaining and delivering parts for IT equipment that is out of warranty or no longer under a maintenance support agreement. PCAs are tasks within incidents or service requests and shall be tasked to the Contractor HRG. PCA tasks shall be closed after delivery of parts or disapproval of the request.

Note: For problems whose estimated repair costs exceed 40% of the replacement cost, the HRG shall refer the case to OIT for a PCA decision. For problems whose estimated costs fall below 40% of the replacement cost, the Contractor shall proceed with parts acquisition and shipment.

5.7.5.1 Parts Acquisition and Shipment

The Contractor shall develop reliable sources of repair and maintenance parts from commercial sources. These parts suppliers shall be required to stock some of the most common repair and consumable parts and to ship within 24 hours of receiving an order.

The Contractor may subcontract or utilize other agreements to meet this requirement.

The Contractor shall enter into contracts with courier or shipping services capable of delivery rush orders overnight. The Contractor shall make these shipping contracts available to its parts suppliers to fulfill orders under this section.

.

5.7.5.2 Eligibility for PCA

Only USCIS equipment is eligible for repair or maintenance under PCA. Asset tags, also called Property Control Numbers, "CIS Tags" and "DHS Tags," are mandatory to prove eligibility for repair.

Exceptions

The Contractor shall refer all PCA requests that do not document valid asset tags to the Government for approval and correction.

5.7.5.3 PCA process flow

The Contractor shall establish the process flow PCA requests, which will be approved by the NATIONS COR. In general, the process flow for PCAs should be:

- Incident opened and assigned.
- Troubleshooting reveals a hardware failure.
- Responsible technician creates a PCA request task within the incident.
- HRG analyzes the request and either approves it under the pre-authorization below or refers to the Government for approval.
- After preauthorization or Government approval, order the parts and designate shipment.
- Track shipment and close the task.

PCA Request Analysis

When the Contractor receives a PCA task, the HRG shall:

- Check the information in the task. The task shall document:
    - Asset tag,
    - Manufacturer's serial number or service tag,
    - Manufacturer,
    - Model,
    - Printer page count if available and a statement of whether the printer was using OEM or Non-OEM toner at the time of the incident.
- Check the warranty status of the equipment or confirm it if the site has already checked it.

- Check the equipment lists provided by USCIS to determine the acquisition cost of the system.
- Obtain the cost of parts to repair or maintain the equipment.
- Determine whether the cost of parts exceeds 40% or the acquisition cost. The 40% figure is the Government approval threshold.

Pre-authorization

The Contractor is pre-authorized to acquire and have parts shipped if:

- The equipment is eligible for PCA, see referenced section above.
- The cost of parts required to repair or maintain a system is less that 40% of acquisition cost.
- The equipment is not subject to restrictions issued by the Government.

Government Approval

The Contractor shall refer the task to the Government if:

- The parts cost exceeds the 40% of the replacement cost.
- The equipment is ineligible for PCA because it lacks an asset tag.
- The Government has issued instructions for specific equipment, models or types.

Ordering and Shipping

The Contractor shall acquire and have parts shipped PCA parts promptly on determination of pre-authorization or government approval.

Documentation

Except for invoicing, the Contractor shall document all the steps in the PCA process completely using the IT Service Management System Incident Management or Service Request Management systems. All documentation shall be available to the Government through the system except for Contractual dealings with subcontractors. However, the Government requires detailed invoice information (such as quantity, part number, price, etc.) on PCA parts.

5.7.6 Handling and Shipping of Hard Drives

During Hardware Incident Repair, the Contractor shall be expected to remove and replace damaged hard drives from workstations, servers and laptops. Used hard drives will contain SBU data and may contain Personally Identifiable Information (PII). The drives shall be wiped and degaussed by the onsite Contractor.

The Government will designate one or more collection points for damaged or obsolete hard drives. They should be disk wiped and degaussed before shipment to the collections points.

The Contractor may be required to apply special handling procedures to hard drives or computers if the site involved does not have a degausser or if the Government certifies a reason for shipping drives or computers containing data. This is particularly pertinent to failed hard drives which do not spin up to speed and cannot be subjected to minimal disk wipe procedures.

5.7.6.1 Hard drive handling

Hard drives shall be disk wiped by the Contractor before they are removed from the workstation, laptop or server.

- Wiped hard drives shall be kept in a locked container in a limited access space.
- If the site has a degausser, the Contractor shall degauss drives before shipment.

5.7.7 Government-Supplied Hardware Resolution Information

The Government will supply the following upon award:

- Records of the previous year's PCA activities.
- Current and past standard equipment show manufacturer, model and standard price.
- Current and past prices for parts.

5.8 Other Direct Costs RESERVED

-

6.0 PERFORMANCE AND SCHEDULE AND MEASUREMENTS

Table 3: Acceptable Quality Levels

Functional Area	AQL #	Required Services		Acceptable Quality Level	Monitoring Method
Abandonment Rate	SD1	Number of callers to the SD who abandon the call before a SDA answers it.	No greater than 2% of all calls to the SD will be abandoned by the caller.	98% success rate	Random Monitoring of Auto Call Distribution Stats
First Call Resolution (FCR)	SD2	An incident categorized as low or medium in the KM Articles database received by a SDA must be resolved during first contact. Caller can be transferred from tier 1 to 1.5 agent however; it must be resolved without any call backs.	At a minimum 75% of all tickets must be resolved by the tier 1 and tier 1.5 SDA during the initial call.	75% success rate	ITSM Remedy Report

Functional Area	AQL #	Required Services			Acceptable Quality Level	Monitoring Method
Service Desk - Customer Satisfaction Survey	SD3	Review of Customer Satisfaction Surveys returned by end-users who received services.	On a rating scale of 1 through 5 where 1 is poor and 5 is outstanding, average monthly measurement will not fall below 4.		90% success rate	100% Inspection of Customer Satisfaction Survey
Service Desk Services – Schedule Factor						
Time to Answer	SD4	Calls are answered promptly by Service Desk Analyst (SDA). [Speed of Answer]	Calls have to be answered by SDA within 45 seconds.		98% success rate	Random Monitoring of Auto Call Distribution Stats
SDA Time to Resolve or Transfer	SD5	Time to resolve an incident or escalate to the next level of support or appropriate service provider [Average Time to Transfer / Escalation]. ALL Tickets in SD queue	USER	VIP User: 15 min Standard: 30 min	95% success rate	ITSM Remedy Report
SDA Time to Resolve or Transfer	SD6	Time to resolve an incident or escalate to the next level of support or appropriate service provider [Average Time to Transfer / Escalation]. ALL Tickets in SD queue	SYSTEM	VIP User: 15 min Standard: 30 min	95% success rate	ITSM Remedy Report
Service Desk - Responsiveness to Emails	SD7	Response time for email requests to be received and tickets entered with completed information by the SDA.	Emails have to be acknowledged and recorded by SDA within 60 minutes of receipt.		95% success rate	ITSM Remedy Report
Service Desk - Responsiveness to Faxes	SD8	Response time for faxed requests to be received and tickets entered with completed information by the SDA.	Faxes have to be acknowledged and recorded by SDA within 60 minutes of receipt.		95% success rate	ITSM Remedy Report

Functional Area	AQL #	Required Services			Acceptable Quality Level	Monitoring Method
Service Desk Services, Incident Management – Performance Factor						
First Level Resolution (FLR) Rate	IM1	Percentage of FLR tickets settled.	At a minimum, 95% of FLR tickets shall be assigned correctly and resolved at the level identified. 95% success rate		ITSM Remedy Report	ITSM Remedy Report
Percentage of Incidents Solved Remotely	IM2	Percentage of non-FCR SDA incident and SRM tickets resolved by Remote Field Support Team.	At a minimum, 50% of non-FCR SDA incident and SRM tickets shall be resolved remotely. 90% success rate		ITSM Remedy Report	ITSM Remedy Report
Incidents/Request Solved and QA Standard Met	IM3	Percentage of tickets (incidents/requests) solved and met USCIS ticket standards.	At a minimum, 98% of tickets shall be solved using knowledge management articles and meet the USCIS ticket standards.		98% success rate	Random Monitoring, ~10% Sample
Service Desk Services, Incident Management – Schedule Factor						
Mean Time to Incident Resolution (MTR)	IM4	Mean time to achieve incident resolution for end users.	USER	-VIP User MTR: 4 hrs	95% success rate	ITSM Remedy Report
MTR – Incident Resolution	IM5	Mean time to achieve incident resolution for systems.	PRIORITY	- High MTR (Security Remediation): 1 business day -Medium: 2 business days -Low: 3 business days	95% success rate	ITSM Remedy Report
Service Request Management – Schedule Factor						
SDA Time to Resolve or Transfer SRM Tickets	SRM 1	SDA's time to resolve a request/work order/task or escalate to the next level of support or appropriate service provider.	VIP User: 15min Standard User: 30min		98% success rate	ITSM Remedy Report

Functional Area	AQL #	Required Services		Acceptable Quality Level	Monitoring Method
Mean Time to Achieve SRM Resolution	SRM 2	Mean time to attain request/work order/task resolution.	High: 1 business days Medium: 3 business days Low: 4 business days	95% success rate	ITSM Remedy Report
Field Services					
Deployment Services – Performance Factor					
Upgrade Activity Support	DS1	A qualified contractor team will travel to scheduled upgrade/new sites and support the upgrade/ activities.	Qualified IT staff will be on location of each upgrade/move NLT 1 hour before move/deployment activities are scheduled to begin.	98% success rate	100% Inspection by CSLs at deployment site
Test Equipment	DS2	Equipment will be tested following installation by the Contractor.	The Contractor deployment team will test 100% of equipment immediately following installation.	100% success rate	100% Inspection by CSLs at deployment site
Account Management – Schedule Factor					
Validation and Account Addition	AM1	Identify, authenticate, and create initial LAN and email approved accounts after validation of the user's identity and authorization by the Government and receipt of completed documentation.	The Contractor shall complete identification, authentication, and creation of initial LAN and email approved accounts within 1 day of receipt of Government authorization.	98% success rate	ITSM Remedy Report
Account Disabling	AM2	Support Incident Response with the disabling of account services	The Contractor shall disable an account within 4 hours of receiving a ticket requesting termination.	100% success rate	ITSM Remedy Report
Account Removal	AM3	Response time to support Remedy requests with removal of account services.	The Contractor shall remove an account within 5 hours of receiving a ticket requesting termination.	100% success rate	ITSM Remedy Report

Functional Area	AQL #	Required Services		Acceptable Quality Level	Monitoring Method
Incident Troubleshooting	AM4	Respond time to Incident troubleshooting tickets.	The Contractor will review and resolve an Incident request within 1 working day.	98% success rate	ITSM Remedy Report
Hardware Incident Resolution – Performance Factor					
Hardware Maintenance – Resolution of Personal Use System Problems	HW1	Time taken for return to service for warranty repair for all Personal Use Systems.	Personal Use Systems returned to service in two (2) business days. For systems requiring Per-Call Authorization (PCA), this AQL shall apply after PCA is granted.	85% Success Rate	ITSM Remedy Report
Hardware Maintenance – Resolution of Network System Problems	HW2	Time taken for return to service for warranty repair for all Network Systems.	Network Systems returned to service by next business day. For systems requiring PCA, this AQL shall apply two (2) days after PCA is granted.	95% Success Rate	ITSM Remedy Report
Hardware Incident Resolution – Schedule Factor					
Hardware Maintenance - Response for Personal Use and Network Systems	HW4	Time from receipt of hardware ticket at the Technical Assistance Center to parts identification and order placement for all Personal Use and Network Systems. Includes warranty service only.	Parts will be ordered within 4 hours from receipt of ticket by the Hardware Resolution Group (HRG) for Personal Use Systems. Parts will be ordered within 2 hours from receipt of ticket by the HRG for all Network Systems.	90% Success Rate	ITSM Remedy Report

7.0 DELIVERABLES

The Contractor shall submit the deliverables that are indicated in Table 4 – Task Order Deliverables (below) to the CO and COR. Unclassified soft copies are acceptable via Email if approved in writing by the CO or COR in advance of delivery.

The Government will provide a preferred format for all deliverables upon award, if not identified in Table 4. The Contractor will be notified in writing by the CO and/or the COR upon final

acceptance of all deliverables. In addition to the deliverable requirements indicated in the table, each deliverable requirement shall be associated with the respective PWS Section.

The Contractor shall include, as part of each Monthly Status Report, the Monthly Status Meeting; Monthly Status Briefing; Weekly Status Briefing and all Ad Hoc Reporting (those specific deliverable requirements that are based on the indicated deliverables).

Administrative deliverables consist of revised and/or updated task order Plans, Progress Reports, Financial Reports, and Performance Reports.

- Progress reports shall be prepared and distributed in accordance with the contract;

The Contractor shall submit a soft copy, in a mutually agreeable file format, of the progress and financial reports.

Submission of deliverables shall begin 30 calendar days after award or as requested by the COR.

Table 4 Task Order Deliverables

PWS Section	Deliverables	Description/Format	Due Dates
General Deliverables			
7.1.1	Post Award Conference	In-person meeting	CO will determine the place and time of kick off meeting after award.
7.1.2	Staffing Plan	Staffing plan identifying personnel qualifications & certifications meeting PWS.	**NLT 10 calendar days after ATP.** An electronic copy of the report shall be submitted to CO and COR, and approved by the CO before beginning activity.
7.1.3	Staffing Report	Contractor's staff on board and their status by location.	**Weekly - NLT Monday of each week.** Data to include status through Friday of prior week. An electronic copy of the report shall be submitted to the CO and COR.
7.1.4, 5.3.1, 5.4.1, 5.6.1	Operating Procedures/Concepts	CONOPS, SOP, etc. Task areas at Service Desk Services, Field services, and Account Management Branch.	**NLT 10 calendar days after ATP** or **as specified in section 7.1**. An electronic copy of the report shall be submitted to the CO and COR.
7.1.5.1	Weekly and Monthly Status Reports	Consolidated report outlining accomplishments, plans and issues for each functional area.	**Weekly - NLT 1600 EST** on **1st working day** after the end of the **previous week** and **Monthly** on **8th working day** after the end of the **previous month after NTP issuance.** An electronic copy of the

			report shall be submitted to the CO and COR.
7.1.5.2	Quarterly Status Report	Issues and future planned activities	**Quarterly - NLT 1600 EST** on the **3rd working day** after the **end of the quarter.** Post Implementation Review (PIR) to occur within 90 calendar days of task order award and subsequently on a quarterly basis. An electronic copy of the report shall be submitted to the CO and COR.
7.1.6	Weekly Status Meeting	Accompanying weekly status report.	**30 calendar days after task order award** and **weekly** thereafter on a scheduled to be agreed upon.
7.1.7	Project Plan and Schedule	Resources, activities, milestones	**NLT 30 calendar daysNTP** and thereafter for each change/ modification. An electronic copy of the report shall be submitted to the CO and COR.
7.1.8	GFP Inventory List	Inventory list	Upon request to the COR.
7.1.9	Program Review	In person informal executive summary	**90 calendar days after NTP** and **quarterly** thereafter on a scheduled to be agreed upon or as needed.
7.1.10	Ad Hoc Reports	e.g. trending, ticket type analysis. Covers task areas at Service Desk Services, Field Services, Service Center Services, Account Management Group, and Hardware Incident Resolution.	**As requested** by the COR**.** An electronic copy of the report shall be submitted to the CO and COR.
7.1.11	After Action Report	Performance evaluation and improvement.	Include with Weekly and Monthly Reports within 24 hours of incident closure. An electronic copy of the report shall be submitted to the CO and COR.
7.4.1	Performance/Quality Control Plan	Inspection and monitoring contractor actions.	**NLT 30 calendar days after award** and **quarterly** thereafter on a scheduled to be agreed upon or as needed.
3.4	COOP/Devolution Plan	Plan for each site.	**As requested** by the COR**.** An electronic copy of the plan shall be submitted to the CO and COR.
Service Desk Services			
7.2.1	Daily ACD Summary Report	Each day's ACD metrics	**Daily - NLT 0600 EST.** An electronic copy of the report shall be submitted to the CO and COR.
7.2.2	Daily Enterprise Aging Queue Report	Incidents/Request aging by queue assignment	**Daily - NLT 0600 EST.** An electronic copy of the report shall be submitted to the CO and COR.
7.2.3	Weekly/Monthly Overall Service Desk Report	ACD and high/abnormal statistics	**NLT 1600 EST** on the **1st working day** of that **week** and of the **month.** An electronic copy of the report shall be submitted to the CO and COR.

7.2.4	Monthly Percentage Report	Incidents/Requests solved within 5 business days and AQL stats	**NLT 0600 EST** on **1st working day** of the **month**. An electronic copy of the report shall be submitted to the CO and COR.
7.2.5	Monthly Ticket Quality Assurance Report	Ticket quality SOP	**NLT 1600 EST** on the **3rd working day** after the **end of the previous month.** An electronic copy of the report shall be submitted to the CO and COR.
Service Center Service			
7.3.1	After Hour Duty Roster	After hour escalation by service centers, NBC, NRC and HQ.	**Weekly – NLT 1600 EST** on **1st working day** after the end of the **previous week.** An electronic copy of the report shall be submitted to the CO and COR.
Account Management			
5.6.1	Quarterly Account Deletion Report	90 day disable list	**NLT 1600 EST** on the **3rd business day** after **the end of the quarter**. An electronic copy of the report shall be submitted to the CO and COR.

7.1 General Deliverables

7.1.1 Post Award Conference

The CO will schedule a post award conference after task order award. The meeting will be either in-person at OIT HQ and/or by teleconference. The participants will discuss primary points of contact, task order scope and tasks, and Government Furnished Property.

7.1.2 Staffing Plan

The Contractor shall provide a staffing plan that identifies the certification type, certification date, and percentage of dedicated staff by task area that possess certifications relevant to meeting task order requirements.

7.1.3 Staffing Report

The Contractor shall submit a staffing report on Monday of each week and the data shall show a status through Friday of prior week. The report shall include, at a minimum, the following:

- Contractor Employee name
- Identify as Prime or Sub Contractor
- Enter on Duty (EOD) status
- Date EOD approved
- Actual EOD date
- Start date on task order
- Labor category

- Supporting location (by USCIS district/region/field office/service centers and address)
- Supported task areas
- Identify personnel certifications by type, certification date, and percentage of dedicated staff by task area that possess certifications relevant to meeting task order requirements.
- Summary of number of Contractor Employees on board, open positions, and total positions by location.

7.1.4 Operating Procedures

All CONOPS and SOP's referenced to be developed or updated by Contractor are to be provided by Contractor within 10 days after Notice to Proceed (NTP) issuance.

7.1.5 Status Reports

7.1.5.1 Weekly and Monthly Status Report

The Contractor shall submit an electronic copy of a weekly and monthly status/progress report to the CO and COR, as specified in the deliverables table, for review, processing, and acceptance. The weekly/monthly report shall contain, but is not limited to, the following:

- Description of work planned and accomplished; Analysis of the difference between planned and accomplished.
- Minutes/Notes from the Monthly Status Meeting and all Ad Hoc Reporting (those specific deliverable requirements that are based on the indicated deliverables). These reports should be tailored, as appropriate, to the applicable provisions of USCIS OIT.
- Task schedule in the weekly and monthly report prepared in Microsoft (MS) Project softcopy format to facilitate the coordination of functional areas with other Government and Contractor activities and for dissemination of schedule information to USCIS field offices.
- The management summary includes documenting any major problems/issues, current expenditures by work hours, and any significant progress or events;
- Narrative includes a description of work performed on tasks(s) during the reporting period and expected to be performed during the next month, including discussions of any problems/issues and recommendations for correction by the 15th business day following the end of each month.
- Account management work including how many accounts have been created, deleted and the productivity.

7.1.5.2 Quarterly Status Report

The Contractor shall prepare a quarterly status report for the CO and the COR. These reports should include accomplishments, any deviations from planned activities, field related issues, other issues, and planned activities for the next period. The Contractor shall provide status and activity report of Post Implementation Review (PIR) for SELC releases and infrastructure changes. The reports are for the CO and COR, and may be delivered in hardcopy or via electronic (e-mail). Additionally, the CO and/or the COR may request impromptu meetings to discuss status or issues.

7.1.6 Weekly Status Meeting

A weekly status report of all activities performed by the Contractor shall be produced and presented to the USCIS CO, COR and Government PM during weekly status meetings. Generally, these reports include status and progress on all pending releases and other O&M related tasks, field related issues, and minutes of previous week's meeting, etc.

Inspection and acceptance of deliverables will use the following procedures:

a) The Government will provide written acceptance, comments, and/or change requests, if any, within fifteen (15) business days of receipt of all required task order deliverables.

b) Upon receipt of the Government comments, the Contractor shall within fifteen (15) business days rectify the situation and re-submit the task order deliverable(s) if it is not a "draft" deliverable. If it is a "draft" deliverable, the Contractor shall rectify the situation before the next scheduled submission of this deliverable.

7.1.7 Project Plan and Schedule

The Contractor shall develop a Project Plan, outlining resources, activities, and milestones necessary to accomplish work specified in the respective task areas. Technical activities in the schedule shall be at a level of detail sufficient for the Contractor to manage the task. The Contractor shall revise the existing project plan and schedule whenever there is a modification to the task order. The Contractor shall provide the initial plan within ten (10) days of NTP approval and when any changes are made to plan including modifications to the task order.

7.1.8 GFP Inventory Listing

The Contractor shall maintain and provide the COR, upon request, ann inventory listing of all GFP in possession by the NATIONS Contractors. The listing shall include but is not limited to identifying the NATIONS task area/CLINs that the GFP supports, location of the GFP and Contractor name in possession of GFP.

7.1.9 Program Review

The Contractor shall participate in quarterly Program Reviews with the CO and Government Program Manager to review selected tasks. The purpose of this meeting is to verify the state of operations and that all application software efforts are coordinated, consistent, and not duplicative. Budgets, schedules and other program related issues shall also be addressed when required. The program review is intended to be an informal executive summary of these events, and should require only minimal presentation time.

7.1.10 Ad Hoc Reports

The Contractor shall develop, provide, update, store, and distribute ad-hoc reports as requested by the Government including but not limited to ad hoc trending, ticket type analysis.

7.1.11 After Action Report

The Contractor shall provide an After Action Report (AAR) on a monthly basis. An AAR shall provide a detailed analysis of outages or maintenance for follow-up purpose. See Attachment 3

for a template of the AAR. The format of the template may be improved however; all content of the template must be captured. The AAR shall:

- Identify incidents or violations,
- Make recommendation for correcting incidents and violations ,
- Focusing on improving activities/preventive maintenance.

7.2 Service Desk Reports

7.2.1 Daily Automatic Call Distribution Summary Report

The Contractor shall provide daily ACD reports. The daily report will cover each day's ACD metrics including, average time to answer, customer hold times, queue hold times, number of calls abandoned, number of call broken down, skillset menu options, total number of calls received, shift 1 agent performance, and total number of priority incidents/request. The Government will provide a template upon award.

7.2.2 Daily Enterprise Aging Queue Report

The Contractor shall provide Daily Enterprise Aging queue reports. The Daily reports will contain a total number of incidents and request aging by queue assignment.

7.2.3 Weekly/Monthly Overall Service Desk Report

The Contractor shall provide a weekly and monthly report of ACD statistics and reasons for high/abnormal stats. The report shall include:

- Total number of incidents, request received and closed per week/month and current backlog;
- Analysis of previous week's critical/high incidents and RFI;
- Top 10 incidents/request trend analysis;
- Survey report summary, as described in AQL SD6;
- Current trends and remediation report;
- Total number of new, reviewed, retired knowledge management articles;
- Total number of new potential problems, status of problem analysis, number of new known errors and KM's implemented.
- Complete SD dashboard metrics.

7.2.4 Monthly Percentage Report

The Contractor shall provide monthly percentage of incidents/request solved within 5 business days, and SD Services AQL statistics.

7.2.5 Monthly Ticket Quality Assurance Report

The Contractor shall provide a monthly Ticket Quality Assurance (QA) reports based on the ticket quality SOP. The QA reports shall evaluate a statistically significant number of closed tickets monthly to makes sure documentation was correctly completed, tickets were

assigned/escalated correctly, knowledge management was used, etc. Approximately 5% of monthly tickets shall be included in the QA reports.

7.3 Service Center Services Report

7.3.1 After-Hour Duty Roster

The Contractor shall provide an after-hour duty roster on a weekly basis. Data contained in the roster shall include a list of primary and secondary on-call DSMs by service centers, regions and districts with their phone numbers. The report shall also include DSM's site code, onsite or remote status, 24/7 support or not, and their primary regional/site supervisor's name and phone number.

7.4 Performance Plan

The NATIONS Performance Plan (RFP, Attachment 2) has been developed to provide an effective surveillance method of monitoring the Contractor's performance. The Performance Plan provides a systematic method to evaluate the services the Contractor is required to furnish.

7.4.1 Performance Plan

The Contractor, and not the Government, is responsible for management and quality control actions to meet the performance objectives of the task order. The role of the Government is surveillance to ensure task order standards are achieved. In this task order the performance program is the driver for quality service. The Contractor is required to develop a comprehensive program of inspections and monitoring actions that aligns with the performance objectives (AQLs). The first major step to ensuring a "self-correcting" task order is to ensure that the performance program approved at the beginning of the task order provides the measures needed to lead the Contractor to success. Once the performance program is approved, careful application of the process and standards presented in the remainder of this document will ensure a robust performance program.

The Contractor shall maintain quality control and adhere to performance measurement methods.

- The Contractor shall analyze trends and identify cost-saving approaches and productivity improvements to maintain IT performance while operating within budget and task constraints.
- The Contractor shall develop, maintain, and manage all NATIONS performance program activities.
- The Contractor shall gather and present service performance information.
- The Contractor shall analyze performance trends.
- The Contractor shall perform quality audits of processes and documentation.
- The Contractor shall monitor performance program activities.
- The Contractor shall archive discrepant performance events so that root cause analyses can be performed.
- The Contractor shall manage continuous process improvement.

8.0 CONTRACTOR PERSONNEL

8.1 Key Personnel

The Contractor shall provide the following key personnel to meet the requirements of this task order. Before removing or replacing any of the specified individuals, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this task order. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change. All key personnel, except Service Desk Manager, shall be located in the National Capital Area. Service Desk Manager shall be located at Stennis Space Center, Mississippi.

Table 5 –Key Personnel Qualifications and Knowledge/Skill Level

Key Personnel	Qualifications	GSA Alliant Knowledge/Skill Level
Program Manager	Bachelor's Degree or higher; Minimum of 10+ years of IT program (project) management experience; Project Management Professional (PMP) or equivalent; ITIL certification.	**Level:** Master **Knowledge/Skill**: Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.
Deputy Program Manager	Bachelor's Degree or higher; Minimum of 4+ years of IT program (project) management experience; PMP or equivalent; ITIL certification.	**Level:** Master **Knowledge/Skill**: Similar to Program Manager
Service Desk Manager	Bachelor's Degree or higher; 3-5 year's experience in IT service desk environment; Help Desk Institute (HDI) or Service Desk Institute (SDI) certification; ITIL certification.	**Level:** Senior **Knowledge/Skill**: Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.
Deployment Manager	Bachelor's Degree or higher; 3-5 years	**Level:** Senior

Key Personnel	Qualifications	GSA Alliant Knowledge/Skill Level
	deployment experience; PMP or equivalent; ITIL certification; Infrastructure background; Knowledgeable of IT service desk environment.	**Knowledge/Skill**: Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

8.1.1 Program Management

Program Manager

The Contractor PM shall have overall authority for this task order and for management of all services and personnel. The primary responsibility of the Contractor PM shall be to act as liaison between the Contractor support team and the Government (CO, COR, PM) in the conduct of all services performed under this task order.

The Contractor PM shall:

- Have sufficient organizational, technical and contractual level of authority within the Contractor organization to ensure full access to corporate personnel, the commitment of resources that may be necessary in the performance of this task order, and in the technical and contractual resolution of all issues that pertain to that performance.
- Develop and maintain business management policies and procedures for all task areas. Coordinate program activities including, but not limited to, cost estimating and reporting; financial oversight; subcontractor management; deliverable schedule and reports; and expenditure reports.
- Appoint management leads with a manager to employee ratio that can sufficiently present oversight and direction for activities in support of the Government.
- Ensure attainment and maintenance of task order AQLs;
- Monitor compliance with small business participation of 30%;
- Manage and review task invoicing functions; resolve discrepant areas prior to submission to customer for payment; and
- Annually refresh the technical skills of all staff in task areas of Service Desk Services, Field Services, Service Center Services, Account Management Group, and Hardware Incident Resolution at its own expense as the USCIS architecture and technical reference model evolve. Training and associated travel costs shall not be directly charged to the Government.

Deputy Program Manager

The Contractor Deputy PM shall also work collaboratively with the USCIS Government PM, COR and Contracting Office. Under the guidance of the Contractor PM, the Contractor Deputy PM shall assist in the overall management of this task order and insure that the technical solutions and schedules in the task order are implemented in a timely manner.

8.1.2 Service Desk Manager

The SD Manager shall possess the technical and leadership skills requirements set forth under the labor categories in the GSA Alliant GWAC. In addition to those skills, it is desired that the SD Manager possess the skills/qualifications identified in the following table:

Service Desk Manager

The SD Manager shall manage the performance of Level 1/1.5 services and support to customers to ensure that service levels are achieved. The SD Manager is responsible for ensuring that customer expectations are met or exceeded. They are also responsible for ensuring the Contractor staff is meeting and exceeding performance expectations, defined metrics/benchmarks, and that standards and processes are followed to provide effective customer service and deliverables.

The Service Desk Manager shall:

- Oversee 100% of the requests, incidents and problems;
- Manage and coordinate urgent and complicated support issues;
- Act as escalation point for all requests and incidents;
- Develop and mature phone/ticket escalation processes to ensure free flowing escalation and information within the organization;
- Determine root cause of issues and communicate appropriately to internal and external customers;
- Train and coach service desk specialists (Level 1 – 1.5) before being assigned to their duties. Oversee staff activities;
- Identify team leads for three sections including Tier 1.5, Incident Management and Problem Management.
- Verify sufficient employee coverage and provide backup support;
- Communicate status/issues with customers;
- Develop strategies for improvement;
- Monitor and manage phone queue (participating in escalated calls as needed);
- Oversee Knowledge Management repository and ensure top quality solutions are available to the staff;
- Develop an effective and workable framework for managing and improving customer IT support in the organization;
- Advise management on situations that may require additional client support or escalation; and
- Review customer satisfaction survey feedback from end users to improve services, tools and support experience;

The SD Manager will disseminate policy, prepare and distribute schedules, monitor Contractor activities, advise Government personnel of the status of projects, and prepare deliverables. The SD Manager or designated representative shall be responsible for the delivery and coordination of all deliverables required of the Service Desk task areas of this PWS.

8.1.3 Field Services

The Government has determined that the Deployment Manager is a key personnel for this scope of work.

Deployment Manager

The Contractor Deployment Manager shall work with the Government Deployment Manager during coordination of large office moves, opening of new facilities, relocations and refresh activities. The Deployment Manager shall be willing to travel and have strong project management and supervisory skills. The Deployment Manager shall manage the Contractor deployment IT staff and review/evaluate their work. He/She shall serve as the primary point of contact (POC) for deployment activities and be responsible for implementing deployment plans. In addition, he/she shall ensure task order deployment staff attend weekly OIT Facilities calls, ROC calls, deployment calls, release management calls and ASC calls to ensure IT requirements are provided for these moves, openings and relocations.

8.2 Contractor Workforce

8.2.1.1 Tier 1.5 Certifications

Tier 1.5 and DSM staff shall have the following professional IT certifications. The Contractor shall have six months, following Enter on Duty (EOD) date, to complete the required training. Existing knowledge base of Tier 1.5 functions may be applied as equivalent to these certifications without jeopardizing task order support requirements.

- Ensure Tier 1.5 staff are certified with Help Desk Institute (HDI) Certification or Service Desk Institute (SDI) Certification, Comptia A+, and IT Infrastructure Library (ITIL) version 3 (v3) Foundation

8.3 Mandatory Contractor Training

The Contractor shall be subject to certain mandatory training requirements to be offered via LearningEDGE. The Contractor shall complete mandated training required of all DHS or USCIS Contractors, and the Contractor shall provide proof of training to the CO and COR. The training shall include but is not limited to:

- A Culture of Privacy Awareness (DHS) training within the first 30 days of Entry on Duty (EOD) and annually thereafter.
- Records Management Awareness (USCIS) training within the first 30 days of EOD and annually thereafter.
- Private Key Infrastructure (PKI) training within 30 days of EOD.
- Contractors using the DHS Network must successfully complete Computer Security Awareness Training (CSAT) training within 24 hours of first accessing a USCIS system.
- Annual refresh training

The Contractor shall annually refresh the technical skills of all staff in task areas of Service Desk Services, Field Services, Service Center Services, Account Management Group, and Hardware Incident Resolution at its own expense as the USCIS architecture and technical reference model evolve. Training and associated travel costs shall not be directly charged to the Government.

9.0 TRAVEL

Travel outside of the local area may be required. In the event travel is required, travel shall not be performed in connection with this task order without prior approval in writing (Email for the request and approval is acceptable) to the CO and COR.

9.1 Government Vehicle Authorization

Contractor employees may use Government motor vehicles when authorized in accordance with the Federal Acquisition Regulation (FAR), GSA Fleet procedures, and the following conditions:

(a) Government motor vehicles are used for official purposes only and solely in the performance of the contract;
(b) Government motor vehicles cannot be used for transportation between residence and place of employment, unless authorized in accordance with 31 U.S.C. 1344;
(c) Contractor must:
(1) Establish and enforce suitable penalties against employees who use, or authorize the use of, Government motor vehicles for unofficial purposes or for other than in the performance of the contract; and
(2) Pay any expenses or cost, without Government reimbursement, for using Government motor vehicles other than in the performance of the contract.

10.0 PLACE OF PERFORMANCE

The principal place of performance shall be at Government provided work sites. Telework is not authorized under this task order. Government sites are identified in the following table and on Attachment 1.

Functional Task Area	Place of Performance
Program Management	Contractor Site in the National Capital Area
Service Desk Service	Stennis Space Center, Mississippi
Field Services	Attachment 1 and 2
Service Center Services	Attachment 1
Account Management	Stennis Space Center, Mississippi
Hardware Incident Resolution	Stennis Space Center, Mississippi

DHS EOC, used as the central coordination point for incident management, will be co-located at Stennis Space Center, Mississippi with the USCIS Service Desk.

10.1 Hours of Operation

Normal service hours shall be between 6:00 a.m. to 6:00 p.m. local time Monday through Friday, excluding Government Holidays, at all supported sites unless otherwise stated. These hours may vary marginally due to site support or facility access requirements.

- USCIS CSC, NSC, TSC, VSC, NBC and NRC are unique and operate on three shifts around the clock six days per week. The Contractor shall provide on-site support on the same schedule. USCIS AAO and BAL shall operate during business days and hours, Monday through Friday 8:00am to 5:00pm local time.
- The SD shall operate 24 hours per day, seven days per week(24X7).
- The Account Management Branch shall perform functions from 6:00 am to 10:00 pm, Monday through Friday local time.

11.0 GOVERNMENT EQUIPMENT, PROPERTY, AND INFORMATION

For the NATIONS task order, only the terms Government Provided Equipment (GPE), Government Furnished Property (GFP) and Government Furnished Information (GFI) shall have effective meaning.

11.1 Government Provided Equipment

USCIS will provide the necessary workspace and office equipment to the Contractor staff required to perform their work under this task order in Government facilities. This will include all essentials, including computer equipment, software, furniture, and office supplies necessary to perform the tasks required under this task order. USCIS will provide maintenance and repair or replacement as necessary for all GPE. However, the Contractor must exercise reasonable care in the use of the equipment provided. See Section 4.0, Table 1, Applicable Documents, which identifies references to properly handling GPE.

11.2 Government Furnished Property

GFP will include laptops and multiple Blackberry devices to enable Contractors to maintain contact when traveling or performing work at sites experiencing outages. The COR will verify the need for and approve each request for GFP.

Anticipated GFP includes, but is not limited to, the following:

- Blackberry devices (secure and non-secure)
- Smart mobile devices
- Desktops
- Laptops
- Storage devices
- Virtual Private Network (VPN) tokens
- Computer peripherals (i.e. printers, scanners)

11.3 Government Furnished Information

The Government will provide the Contractor with all applicable policies, procedures, guidelines, pre-deployment information and data applicable to and in use by the incumbent Contractors only after final award of this task order.

12.0 WORK PRODUCT

All documents, data or other information produced by the Contractor staff as work product under the task order shall be the property of the Government. The Contractor may designate documents as proprietary only as they relate to internal business practices and strategies, pricing, staffing or Human Relations.

All final reports and data held in Government servers, workstations and databases are Government property. Maintenance of personal or corporate documents on GFP equipment may be subject to sanctions under DHS MD 4600.1 PERSONAL USE OF GOVERNMENT OFFICE EQUIPMENT.

13.0 ENCRYPTION

All encryption under this task order shall be FIPS 140-2 and FIPS 197 compliant.

14.0 SECURITY OVERSIGHT

14.1 Supported Systems

The Contractor shall support USCIS equipment used by USCIS Federal and Contractor employees or Federal or Contractor employees authorized by USCIS to access its systems. Personal or contractor-owned equipment shall not be supported.

14.1.1 System Classification

The Contractor shall perform IT support services under NATIONS on SBU networks and equipment. All support requiring access to classified systems and networks will be performed by the Government.

14.1.2 System Access

The favorable enter on duty (EOD) decision may allow the NATIONS employees to commence work temporarily prior to the completion of the full investigation. Full background investigation is mandatory for positions that will require access to systems administration, database administration, or where administrative access will allow the modification of the system.

15.0 SECTION 508 COMPLIANCE

All tasks referenced in this document and described in the respective attachments must comply with the appropriate Information Technology Accessibility for Persons with Disabilities standards outlined below.

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.

15.1 Section 508 Applicable EIT Accessibility Standards

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 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 technical support shall have the ability to transmit and receive messages using TTY.

15.2 Section 508 Applicable Exceptions

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 COR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

36 CFR 1194.3(b) Incidental to the task order, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

36 CFR 1194.3(f) – Back Office, applies to any EIT item that will be located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment. This exception does not include remote user interfaces that are accessible outside the enclosed "space".

15.3 Section 508 Compliance Requirements

36 CFR 1194.2(b) – (COTS 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 on Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@dhs.gov.

16.0 SECURITY REQUIREMENTS

Security requirements are included in Section H.1.

PART II – CONTRACT CLAUSES

This task order is subject to the terms and conditions of the GSA Alliant 2 Unrestricted Contract.

Federal Acquisition Regulation (FAR) Clauses Incorporated by Reference

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 these addresses: http://www.acquisition.gov/far.

(End of clause)

52.204-18 Commercial and Government Entity Code Maintenance (Jul 2016)
52.204-19 Incorporation by Reference of Representations and Certifications (Dec 2014)
52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019)
52.245-1 Government Property (Jan 2017)
52.212-4 Contract Terms and Conditions -- Commercial Items (Oct 2018)
52.237-3 Continuity of Services (Jan 1991)

Federal Acquisition Regulation (FAR) Clauses Incorporated in Full Text

52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders -- Commercial Items (JAN 2020)
(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:
(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).
(2) 52.204-23, Prohibition on Contracting for Hardware,68
Software, and Services Developed or Provided by Kaspersky Lab and
Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).
(3) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)
(4) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).
(5) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77, 108-78 (19 U.S.C. 3805 note)).
(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the contracting officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

__X_ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

__X_ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).
__X_ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub L. 111-5) (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009).
__X_ (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Oct 2018) (Pub. L. 109-282) (31 U.S.C. 6101 note).
___ (5) [Reserved]
__X_ (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).
___ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).
__X_ (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Oct 2015) (31 U.S.C. 6101 note).
__X_ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).
___ (10) [Reserved]
___ (11) (i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011) (15 U.S.C. 657a).
___ (ii) Alternate I (Nov 2011) of 52.219-3.
__X_ (12) (i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).
___ (ii) Alternate I (Jan 2011) of 52.219-4.
___ (13) [Reserved]
___ (14) (i) 52.219-6, Notice of Total Small Business Aside (Nov 2011) (15 U.S.C. 644).
___ (ii) Alternate I (Nov 2011).
___ (iii) Alternate II (Nov 2011).
___ (15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).
___ (ii) Alternate I (Oct 1995) of 52.219-7.
___ (iii) Alternate II (Mar 2004) of 52.219-7.
__X_ (16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).
___ (17) (i) 52.219-9, Small Business Subcontracting Plan (Aug 2018) (15 U.S.C. 637 (d)(4)).
___ (ii) Alternate I (Nov 2016) of 52.219-9.
_ _ (iii) Alternate II (Nov 2016) of 52.219-9.
___ (iv) Alternate III (Nov 2016) of 52.219-9.
___ (v) Alternate IV (Aug 2018) of 52.219-9.
___ (18) 52.219-13, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).
___ (19) 52.219-14, Limitations on Subcontracting (Jan 2017) (15 U.S.C. 637(a)(14)).
___ (20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).
___ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011) (15 U.S.C. 657f).
___ (22) 52.219-28, Post Award Small Business Program Representation (Jul 2013) (15 U.S.C. 632(a)(2)).

___ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Dec 2015) (15 U.S.C. 637(m)).
___ (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Dec 2015) (15 U.S.C. 637(m)).
__X_ (25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).
__X_ (26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Jan 2020) (E.O. 13126).
__X_ (27) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
__X_ (28) (i) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).
___ (ii) Alternate I (Feb 1999) of 52.222-26.
__X_ (29) (i) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).
___ (ii) Alternate I (July 2014) of 52.222-35.
__X_ (30) (i) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).
___ (ii) Alternate I (July 2014) of 52.222-36.
__X_ (31) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).
__X_ (32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
__X_ (33) (i) 52.222-50, Combating Trafficking in Persons (JAN 2019) (22 U.S.C. chapter 78 and E.O. 13627).
___ (ii) Alternate I (Mar 2015) of 52.222-50, (22 U.S.C. chapter 78 and E.O. 13627).
__X_ (34) 52.222-54, Employment Eligibility Verification (Oct 2015). (E. O. 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)
___ (35) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
___ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
___ (36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O.13693).
___ (37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).
___ (38) (i) 52.223-13, Acquisition of EPEAT® -Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514
___ (ii) Alternate I (Oct 2015) of 52.223-13.
___ (39) (i) 52.223-14, Acquisition of EPEAT® -Registered Television (Jun 2014) (E.O.s 13423 and 13514).
___ (ii) Alternate I (Jun 2014) of 52.223-14.
___ (40) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).
___ (41) (i) 52.223-16, Acquisition of EPEAT® -Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).
___ (ii) Alternate I (Jun 2014) of 52.223-16.

__X_ (42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (Aug 2011) (E.O. 13513).
___ (43) 52.223-20, Aerosols (Jun 2016) (E.O. 13693).
___ (44) 52.223-21, Foams (Jun 2016) (E.O. 13696).
__X_ (45) (i) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).
__X_ (ii) Alternate I (Jan 2017) of 52.224-3.
___ (46) 52.225-1, Buy American--Supplies (May 2014) (41 U.S.C. chapter 83).
___ (47) (i) 52.225-3, Buy American--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).
___ (ii) Alternate I (May 2014) of 52.225-3.
___ (iii) Alternate II (May 2014) of 52.225-3.
___ (iv) Alternate III (May 2014) of 52.225-3.
___ (48) 52.225-5, Trade Agreements (Aug 2018) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).
__X_ (49) 52.225-13, Restrictions on Certain Foreign Purchases (June 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
___ (50) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
___ (51) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).
___ (52) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).
___ (53) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505), 10 U.S.C. 2307(f)).
___ (54) 52.232-30, Installment Payments for Commercial Items (Jan 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).
__X_ (55) 52.232-33, Payment by Electronic Funds Transfer--System for Award Management (Oct 2018) (31 U.S.C. 3332).
___ (56) 52.232-34, Payment by Electronic Funds Transfer—Other Than System for Award Management (Jul 2013) (31 U.S.C. 3332).
___ (57) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).
__X_ (58) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).
__X_ (59) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(13)).
___ (60) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).
___ (ii) Alternate I (Apr 2003) of 52.247-64.
___ (iii) Alternate II (Feb 2006) of 52.247-64.
(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or executive orders applicable to acquisitions of commercial items:

_X__ (1) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495)
___ (2) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67.).
_____ (3) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).
___ (X4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C.206 and 41 U.S.C. chapter 67).
___ (5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).
___ (6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67).
_X__ (7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).
__X_ (8) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015) (E.O. 13658).
__X_ (9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).
___ (10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792).
(d) Comptroller General Examination of Record The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.
(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.
(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.
(e)
(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—
(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Jan 2019) (41 U.S.C. 3509).
(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further

Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).
(iii) 52.204-23, Prohibition on Contracting for Hardware,
Software, and Services Developed or Provided by Kaspersky Lab and
Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).
(iv) 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).
(iv) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $700,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.
(v) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (1) of FAR clause 52.222-17.
(vi) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
(vii) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).
(viii) 52.222-35, Equal Opportunity for Veterans (Oct 2019) (38 U.S.C. 4212).
(ix) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).
(x) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).
(xi) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.
(xii) 52.222-41, Service Contract Labor Standards (Aug 2018), (41 U.S.C. chapter 67).
(xiii) (A) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O. 13627).
(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).
(xiv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67.)
(xv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67)
(xvi) 52.222-54, Employment Eligibility Verification (Oct 2015) (E. O. 12989).
(xvii) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).
(xviii) 52.222-62, Paid sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).
(xix) (A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).
(B) Alternate I (Jan 2017) of 52.224-3.
(xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
(xxi) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.
(xxii) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.
(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(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 **10 days** before the contract expires; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **20 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 **8 months.**

(End of clause)

52.224-3 Privacy Training (Jan 2017)
(a) Definition. As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A–130, Managing Federal Information as a Strategic Resource).
(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—
(1) Have access to a system of records;
(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or
(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).
(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing Privacy at DHS: Protecting Personal Information accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.
(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.
(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.
(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—
(1) Have access to a system of records;
(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or
(3) Design, develop, maintain, or operate a system of records.

(End of clause)

52.252-4 Alterations in Contract (Apr 1984)
Portions of this contract are altered as follows:
Use of the word "contract" is understood to mean "task order" wherever such application is appropriate. Use of the word "solicitation" is understood to mean "fair opportunity notice" wherever such application is appropriate.(End of clause)

Homeland Security Acquisition Regulation (HSAR) Clauses Incorporated by Reference

The full text of HSAR clauses may be accessed electronically at the following address:
http://www.acquisition.gov/far

3052.205-70 Advertisements, Publicizing Awards, and Releases (SEP 2012)
3052.222-70 Strikes or Picketing Affecting Timely Completion of the Contract Work (Dec 2003)
3052.222-71 Strikes or Picketing Affecting Access to a DHS Facility (Dec 2003)

Homeland Security Acquisition Regulation (HSAR) Clauses Incorporated in Full Text

3052.209-73 Limitation of future contracting (Jun 2006)
a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5--Organizational Conflicts of Interest.
(b) The nature of this conflict is that the contractor will be required to work directly with vendors/OEMs to perform market research and develop requirements for the procurement of relevant hardware, software and professional services. This will include developing requirements documents to ensure all technical requirements will be met for the Government. The contractor will be required to work with other agency contract resources or external contract vendors that provide services such as solution development, project management and infrastructure deployment, to include improvements and fixes.
(c) The restrictions upon future contracting are as follows:
(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.
(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or

confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

(End of clause)

3052.212-70 Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items (Sep 2012)

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference:

[The Contracting Officer should either check the provisions and clauses that apply or delete the provisions and clauses that do not apply from the list. The Contracting Officer may add the date of the provision or clause if desired for clarity.]

(a) Provisions.

__X_3052.209-72 Organizational Conflicts of Interest.

____3052.216-70 Evaluation of Offers Subject to An Economic Price Adjustment Clause.

___3052.219-72 Evaluation of Prime Contractor Participation in the DHS Mentor Protégé Program.

(b) Clauses.

__X__3052.203-70 Instructions for Contractor Disclosure of Violations.

____3052.204-70 Security Requirements for Unclassified Information Technology Resources.

__X__3052.204-71 Contractor Employee Access.

__X__Alternate I

__X__3052.205-70 Advertisement, Publicizing Awards, and Releases.

____3052.209-73 Limitation on Future Contracting.

____3052.215-70 Key Personnel or Facilities.

____3052.216-71 Determination of Award Fee.

____3052.216-72 Performance Evaluation Plan.

____3052.216-73 Distribution of Award Fee.

____3052.217-91 Performance. (USCG)

____3052.217-92 Inspection and Manner of Doing Work. (USCG)

____3052.217-93 Subcontracts. (USCG)

____3052.217-94 Lay Days. (USCG)

____3052.217-95 Liability and Insurance. (USCG)

____3052.217-96 Title. (USCG)

____3052.217-97 Discharge of Liens. (USCG)

____3052.217-98 Delays. (USCG)

____3052.217-99 Department of Labor Safety and Health Regulations for Ship Repair. (USCG)

____3052.217-100 Guarantee. (USCG)

____3052.219-70 Small Business Subcontracting Plan Reporting.

____3052.219-71 DHS Mentor Protégé Program.

__X__3052.228-70 Insurance.

____3052.228-90 Notification of Miller Act Payment Bond Protection. (USCG)

____3052.228-91 Loss of or Damage to Leased Aircraft. (USCG)

____3052.228-92 Fair Market Value of Aircraft. (USCG)
____3052.228-93 Risk and Indemnities. (USCG)
____3052.236-70 Special Provisions for Work at Operating Airports.
__X__3052.242-72 Contracting Officer's Technical Representative.
____3052.247-70 F.o.B. Origin Information.
____Alternate I
____Alternate II
____3052.247-71 F.o.B. Origin Only.
____3052.247-72 F.o.B. Destination Only.

(End of clause)

3052.215-70 Key Personnel or Facilities (Dec 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel or Facilities under this Task Order:

Program Manager
Deputy Program Manager
Service Desk Manager
Deployment Manager

(End of clause)

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)
(HSAR Class Deviation 15-01)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions*. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable

information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, 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.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive

as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only)*

Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on

the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation,

databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, 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 Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To

transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:
(i) Inspections,

(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements*.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of clause)

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)
(HSAR Class Deviation 15-01)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail

notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

Other Task Order Requirements

1. ADDITIONAL INVOICING INSTRUCTIONS

(a) In accordance with FAR 52.212-4(g), all invoices submitted to USCIS for payment shall include the following:
(1) Name and address of the Contractor;
(2) Invoice date and number;
(3) Contract number, line item number and, if applicable, the order number;
(4) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(5) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;
(6) Terms of any discount for prompt payment offered;
(7) Name and address of official to whom payment is to be sent;
(8) Name, title, and phone number of person to notify in event of defective invoice; and
(9) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.
(10) Electronic funds transfer (EFT) banking information.

(b) Invoices not meeting these requirements will be rejected and not paid until a corrected invoice meeting the requirements is received.

(c) USCIS' preferred method for invoice submission is electronically. Invoices shall be submitted in Adobe pdf format with each pdf file containing only one invoice. The pdf files shall be submitted electronically using the "To" line in the e-mail address to USCISInvoice.Consolidation@ice.dhs.gov with each email conforming to a size limit of 500 KB.

(d) If a paper invoice is submitted, mail the invoice to:
USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495

DIRECT PAYMENT INQUIRIES TO ICE FINANCIAL OPERATIONS, (877) 491-6521

2. POSTING OF TASK ORDER IN FOIA READING ROOM

(a) The Government intends to post the task order resulting from this solicitation to a public FOIA reading room.
(b) Within 30 days of award, the Contractor shall submit a redacted copy of the executed contract (or order) (including all attachments) suitable for public posting under the provisions of the Freedom of Information Act (FOIA). The Contractor shall submit the documents to the USCIS FOIA Office by email at foiaerr.nrc@uscis.dhs.gov with a courtesy copy to the contracting officer.
(c) The USCIS FOIA Office will notify the contractor of any disagreements with the Contractor's redactions before public posting of the contract or order in a public FOIA reading room.

3. PERFORMANCE REPORTING

The government intends to record and maintain contractor performance information for this task order in accordance with FAR Subpart 42.15. The contractor will need to enroll at www.cpars.gov, so it can participate in this process.

4. FINAL PAYMENT

As a condition precedent to final payment, a release discharging the government, its officers, agents and employees of and from all liabilities, obligations, and claims arising out of or under this order shall be completed. A release of claims will be forwarded to the contractor at the end of each performance period for contractor completion, as soon thereafter as practicable.

5. GOVERNMENT FURNISHED PROPERTY (GFP)

(a) The Government will provide contractor personnel with the GFP specified in PWS Section 11.2.
(b) The contractor shall notify personnel that there shall be no expectation of privacy on any USCIS Systems.
(c) The contractor shall operate Government provided property in accordance with USCIS procedures and manufacturer's specifications.
(d) The contractor shall initiate and track maintenance calls and/or service requests for government provided IT equipment to the DHS Helpdesk. The contractor shall notify the COR and/or Program Manager (PM) of any repair needs and/or problems with maintenance/service contractor activities within four (4) hours of each occurrence.
(e) The Government provides computer laptops and software in various hardware configurations, and reserves the right to upgrade, add, delete, or replace equipment and software.

PART III – DOCUMENT, EXHIBITS, OR ATTACHMENTS

Attachment	Title/Description	Pages
1	Places of performance	17
2	Field Service Physical Place of Performance	5
3	After Action Report	1
4	Sites Requiring On-site Staff	4
5	Acronyms	2

ATTACHMENT 1 – PLACE OF PERFORMANCE

Below is a list of CONUS and OCONUS Government facilities requiring Contractor support for NEON.

CONUS

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
*CIS HEADQUARTERS - CONSOLIDATING 12/31/2020	1 Town Center, Capital Gateway Drive	Camp Springs	MD	20746	HQ	3,700

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
*CIS HEADQUARTERS (UNION LABOR/UNION/LIFE) - CONSOLIDATING 12/31/2020	111 MASSACHUSETTS AVE NW	WASHINGTON	DC	20529	HQ	
*CIS HEADQUARTERS (CASMIR PULASKI) CONSOLIDATING 12/31/2020	20 MASSACHUSETTS AVE NW	WASHINGTON	DC	20529	HQ	
*CIS HEADQUARTERS (JUDICIARY SQUARE) - CONSOLIDATING 12/31/2020	633 3RD STREET	WASHINGTON	DC	20529	HQ	
CIS HEADQUARTERS VERIFICATION DIVISION (NoMA Station)	131 M St NE	WASHINGTON	DC	20529	HQ	255
NORTH CAPITAL STREET	999 N CAPITAL ST	WASHINGTON	DC	20529	HQ	200
NORTHEAST REGION OFFICE	70 KIMBALL AVENUE	SOUTH BURLINGTON	VT	05403	RO	164
EASTERN FORM CENTER	124 LEROY ROAD	WILLISTON	VT	05495	FC	46
CIS HQ Contracting Office	300 INTERSTATE CORPORATE CENTER	WILLISTON	VT	05495	HQ	15
FIELD SUPPORT CENTER	100 INTERSTATE CORPORATE CENTER	WILLISTON	VT	05495	HQ	175
BURLINGTON TTC	237 HARVEST LANE	WILLISTON	VT	05495	HQ	125
BURLINGTON PSO	65 BOWDOIN STREET	SOUTH BURLINGTON	VT	05403	HQ	124
BOSTON DISTRICT OFFICE	JFK FEDERAL BUILDING, GOVERNMENT CENTER ROOM E-160, 15 NEW SUDBURY STREET	BOSTON	MA	02203	DO	152

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
BOSTON FIELD OFFICE	JFK FEDERAL BUILDING, GOVERNMENT CENTER ROOM E-160, 15 NEW SUDBURY STREET	BOSTON	MA	02203	FO	20
BOSTON ASYLUM OFFICE	5 POST OFFICE SQUARE	BOSTON	MA	02109	ASY	66
PORTLAND FIELD OFFICE & ASC	TBD		ME	04106	FO/ASC	18
PROVIDENCE FIELD OFFICE	1543 ATWOOD AVENUE	JOHNSTON	RI	02919	FO	42
LAWRENCE FIELD OFFICE	2 Mill Street	LAWRENCE	MA	01840	FO/ASC	96
MANCHESTER FIELD OFFICE & ASC	9 Ridgewood Road	MANCHESTER	NH	03110	FO/ASC	19
BOSTON ASC	170 PORTLAND STREET	BOSTON	MA	02114	ASC	6
PROVIDENCE ASC	CROSSROADS OFFICE PARK, 105 SOCKANOSSET CROSS ROAD, SUITE 210	CRANSTON	RI	02920	ASC	5
BUFFALO DISTRICT OFFICE, FIELD OFFICE & ASC	138 DELAWARE AVENUE	BUFFALO	NY	14202	DO/ASC	58
BUFFALO VERIFICATION OFFICE	10 Fountain Plaza	BUFFALO	NY	14202	HQ	180
SYRACUSE FIELD SUPPORT OFFICE & ASC	401-403 S. SALINA STREET/412 S. Warren St	SYRACUSE	NY	13202	FSO/ASC	73
ALBANY FIELD OFFICE & ASC	1086 TROY-SCHENECTADY ROAD	LATHAM	NY	12110	FO/ASC	26

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
HARTFORD FIELD OFFICE	450 MAIN STREET, FIRST FLOOR	HARTFORD	CT	06103	FO	99
ST ALBANS FIELD OFFICE & ASC	64 GRICE BROOK ROAD	ST ALBANS	VT	05478	FO/ASC	14
HARTFORD ASC	467 SILVER LANE	EAST HARTFORD	CT	06118	ASC	8
NEW YORK DISTRICT OFFICE	JACOB JAVITS FEDERAL BUILDING, 26 FEDERAL PLAZA,	NEW YORK	NY	10278	DO	624
NEW YORK ASYLUM OFFICE	1065 STEWART AVE	BETHPAGE	NY	11714	ASY	77
EASTERN ICS & MANHATTAN ASC	201 VARICK STREET	NEW YORK	NY	10014	ICS/ASC	192
LONG ISLAND FIELD OFFICE AND ASC	30 BARRETTS AVENUE	HOLTSVILLE	NY	11742	FO/ASC	101
QUEENS FIELD OFFICE	TBD 11/2020	NEW YORK	NY	TBD	FO	171
NEW ROCHELLE ASC	40 South Main Street	PORT CHESTER	NY	10573	ASC	7
BROOKLYN ASC	1260-1278 60TH STREET	BROOKLYN	NY	11219	ASC	19
BRONX ASC	1827 WESTCHESTER AVE	BRONX	NY	10472	ASC	10
QUEENS/ JAMAICA ASC	153-01 JAMAICA AVE	JAMAICA	NY	11432	ASC	15
HEMPSTEAD ASC	87 BETHPAGE ROAD	HICKSVILLE	NY	11801	ASC	7
JACKSON HEIGHTS ASC	27-35 JACKSON AVE	LONG ISLAND CITY	NY	11101	ASC	6
NEWARK ASYLUM OFFICE	1200 WALL STREET WEST, FOURTH FLOOR	LYNDHURST	NJ	07071	ASY	146
MT LAUREL FIELD OFFICE	530 FELLOWSHIP RD	MOUNT LAUREL	NJ	08054	FO	85

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
NEWARK DISTRICT OFFICE	PETER RODINO FEDERAL BUILDING, 970 BROAD STREET	NEWARK	NJ	07102	DO	375
NEWARK ASC	285-299 NORTH BROAD STREET	ELIZABETH CITY	NJ	07208	ASC	20
HACKENSACK ASC	116 KANSAS STREET, MAIN FLOOR	HACKENSACK	NJ	07601	ASC	5
PHILADELPHIA DISTRICT OFFICE & FIELD OFFICE	30 NORTH 41ST STREET	PHILADELPHIA	PA	19104	DO/FO	144
CHARLESTON ASC	210 KANAWHA BOULEVARD WEST	CHARLESTON	WV	25302	ASC	5
PITTSBURGH FIELD OFFICE	3000 SIDNEY STREET, Suite 200	PITTSBURGH	PA	15203	FO	36
DOVER ASC	250 Gateway South Blvd Suite: 260	DOVER	DE	19901	ASC	4
PHILADELPHIA ASC	10300 DRUMMOND RD., SUITE 100	PHILADELPHIA	PA	19154	ASC	12
PITTSBURGH ASC	800 PENN AVENUE, SUITE 101	PITTSBURGH	PA	15222	ASC	4
YORK ASC	3400 CONCORD ROAD	YORK	PA	17402	ASC	3
SALISBURY ASC	2040 SHIPLEY DRIVE, SUITE 2C	SALISBURY	MD	21801	ASC	4
BALTIMORE DISTRICT OFFICE & FIELD OFFICE	3701 KLOPPERS STREET	BALTIMORE	MD	21227	DO/FO	260
BALTIMORE ASC	100 S CHARLES ST, SUITE 201	BALTIMORE	MD	21201	ASC	12
GLENMONT ASC	12331 GEORGIA AVENUE, Suite C	WHEATON	MD	20906	ASC	10
NORFOLK FIELD OFFICE	5280 HENNEMAN DRIVE	NORFOLK	VA	23513	FO	47
WASHINGTON DISTRICT OFFICE & FIELD OFFICE	2675 PROSPERITY AVENUE	FAIRFAX	VA	22031	DO	90

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
ARLINGTON ASYLUM OFFICE	1525 WILSON BOULEVARD, SUITE 300	ARLINGTON	VA	22209	ASY	70

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
NORFOLK ASC	2501 ALMEDA AVENUE Suite 114	NORFOLK	VA	23513	ASC	16
ALEXANDRIA ASC	8850 RICHMOND HIGHWAY, Suite 100	ALEXANDRIA	VA	22309	ASC	12
AAO OFFICE	2221 S. CLARK STREET	CRYSTAL CITY	VA	22202	AAO	145
HARRISONBURG FILE STORAGE FACILITY/COOP	1344 PLEASANTS DRIVE	HARRISONBURG	VA	22801	FSF/WARE	36
SOUTHEAST REGION OFFICE	390 NORTH ORANGE AVENUE, #220	ORLANDO	FL	32801	RO	67
ATLANTA DISTRICT OFFICE	2150 PARKLAKE DRIVE	ATLANTA	GA	30345	DO/FO	181
CHARLESTON FIELD OFFICE & ASC	1 POSTON ROAD, Suite 130	CHARLESTON	SC	29407	FO/ASC	20
GREER FIELD SUPPORT OFFICE & ASC	501 Pennsylvania Ave	Greer	SC	29650	FSO/ASC	13
CHARLESTON TRAINING ACADEMY (FLETC)	2222 S HOBSON AVE	NORTH CHARLESTON	SC	29405	TRAINING	36
CHARLOTTE FIELD OFFICE	201 REGENCY EXECUTIVE PARK DRIVE	CHARLOTTE	NC	28217	FO	59
RALEIGH-DURHAM FIELD OFFICE & ASC	301 ROYCROFT DRIVE	DURHAM	NC	27703	FO/ASC	43
FT. JACKSON FIELD SUPPORT OFICE	4204 Sumter Ave	Fort Jackson	SC	29207	FSO	6
BIRMINGHAM FIELD SUPPORT OFFICE & ASC	529 BEACON PARKWAY W, SUITE 106	BIRMINGHAM	AL	35209	FSO/ASC	4

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
MONTOGOMERY FIELD OFICE (Opening summer 2017)	3381 Atlanta Highway	Montgomery	AL	36109	FO	27
ATLANTA ASC	1255 COLLIER ROAD NW, SUITE 100	ATLANTA	GA	30318	ASC	19
ATLANTA ASYLUM OFFICE AND FDNS VETTING CENTER	401 W PEACHTREE ST NW,	ATLANTA	GA	30308	ASY	200
CHARLOTTE ASC	4801 CHASTAIN AVENUE, Building 10 Suite 175	CHARLOTTE	NC	28217	ASC	10
MIAMI DISTRICT OFFICE	8801 N.W. 7th AVENUE	MIAMI	FL	33150	DO/FO/ASC	160
MIAMI ASYLUM	99 SE 5TH STREET, 3RD FLOOR	MIAMI	FL	33131	ASY	69
MIAMI OSI INVESTIGATIONS	909 SE 1ST AVE, 7TH FLOOR	MIAMI	FL	33131	OSI	9
KENDALL FIELD OFFICE	14675 S.W. 120th STREET	MIAMI	FL	33186	FO/ASC	97
HIALEAH FIELD OFFICE	5880 N.W. 183rd STREET	HIALEAH	FL	33015	FO/ASC	95
OAKLAND PARK FIELD OFFICE	4451 N.W. 31st AVENUE	OAKLAND PARK	FL	33309	FO/ASC	88
CHRISTIANSTED FIELD SUPPORT OFFICE & ASC	Sunny Isle Shopping Center, CENTER LINE & S HIGHWAY, Suite 5A-8A	CHRISTIANSTED, St. Croix	VI	823	FSO/ASC	5
SAN JUAN FIELD OFFICE	Metro Office Park, 2nd Street	GUAYNABO	PR	968	FO	20
CHARLOTTE AMALIE FIELD OFFICE & ASC	6783 ESTATE SMITH BAY	ST THOMAS	VI	802	FO/ASC	23
SAN JUAN ASC	TLD BUILDNG LOT NO. 1 VALENCIA OFFICE PARK	GUAYNABO	PR	968	ASC	3

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
TAMPA DISTRICT OFFICE	5629 Hoover Boulevard	TAMPA	FL	33634	DO/FO/ASC	105
JACKSONVILLE FIELD OFFICE & ASC	4121 SOUTHPOINT BOULEVARD	JACKSONVILLE	FL	32216	FO/ASC	45
ORLANDO FIELD OFFICE	6680 Corporate Centre Boulevard	ORLANDO	FL	32822	FO	82
WEST PALM BEACH FIELD OFFICE	9300 BELVEDERE ROAD	WEST PALM BEACH	FL	33411	FO	89
WEST PALM BEACH ASC	1661-B SOUTH CONGRESS AVE	WEST PALM BEACH	FL	33406	ASC	6
ORLANDO ASC	6200 Lee Vista Blvd	ORLANDO	FL	32822	ASC	11
FORT MYERS ASC	3850 COLONIAL BOULEVARD	FORT MYERS	FL	33966	ASC	6
FORT MYERS FIELD OFFICE	4220 EXECUTIVE CIRCLE SUITE 1	FORT MYERS	FL	33916	FO	41
MEMPHIS FIELD OFFICE	80 MONROE AVENUE SUITE 700	MEMPHIS	TN	38122	FO	37
MEMPHIS ASC	7174 STAGE ROAD	MEMPHIS	TN	38122	ASC	6
NASHVILLE FIELD OFFICE	340 PLUS PARK BLVD	NASHVILLE	TN	37217	FO	32
NEW ORLEANS DISTRICT OFFICE & ASC	1250 POYDRAS STREET	NEW ORLEANS	LA	70113	DO/FO/ASC	45
NEW ORLEANS ASYLUM OFFICE	2424 EDENBORN AVENUE 3RD FLOOR	METAIRIE	LA	70001	ASY	36
NATIONAL CUSTOMER SUPPORT CENTER	301 BENTON ROAD	BOSSIER CITY	LA	71111	CC	160
JACKSON FIELD SUPPORT OFFICE & ASC	DR. A.H. MCCOY FEDERAL BUILDING, 100 W CAPITOL ST, SUITE 727	JACKSON	MS	39269	FSO/ASC	6
FORT SMITH FIELD OFFICE & ASC	4624 KELLEY HIGHWAY	FORT SMITH	AR	72903	FO/ASC	14

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
NASHVILLE ASC	1400 DONELSON PIKE, AIRPARK CENTER, Suite B-13	NASHVILLE	TN	37217	ASC	8
CENTRAL REGION OFFICE & DALLAS TRAINING ACADEMY	4500 FULLER DRIVE	IRVING	TX	75063	RO	122
DETROIT, FIELD OFFICE & ASC	11411 E. JEFFERSON AVENUE	DETROIT	MI	48214	DO/ASC	109
GRAND RAPIDS ASC	4484 BRETON ROAD SE	KENTWOOD	MI	49508	ASC	5
CINCINNATI FIELD OFFICE & ASC	550 MAIN STREET	CINCINNATI	OH	45202	FO/ASC	26
CLEVELAND DISTRICT OFFICE FIELD OFFICE & ASC	1240 E NINTH STREET	CLEVELAND	OH	44199	DO/ASC	47
CLEVELAND ASYLUM OFFICE	201 SUPERIOR AVENUE EAST	CLEVELAND	OH	44114	AO	4
INDIANAPOLIS FIELD OFFICE & ASC	1099 N. MERIDIAN STREET, 10th FLOOR LANDMARK CENTER	INDIANAPOLIS	IN	46204	FO/ASC	35
COLUMBUS FIELD OFFICE & ASC	5466 WESTERVILLE ROAD	WESTERVILLE	OH	43081	FO	30
LOUISVILLE FIELD OFFICE & ASC	601 WEST BROADWAY ROOM 390	LOUISVILLE	KY	40202	FO/ASC	24
INTEGRATED CARD PRODUCTION CENTER	203 ALLISON BOULEVARD	CORBIN	KY	40701	CARD	62
CUSTOMER CONTACT CENTER	207 HOSPITAL DRIVE	Barbourville	KY	40906	CC	337
KENTUCKY CONSULAR CENTER	3505 N HIGHWAY 25W	WILLIAMSBURG	KY	40769	FDNS	4
MILWAUKEE FIELD OFFICE & ASC	310 E. KNAPP STREET, Room 154	MILWAUKEE	WI	53202	FO/ASC	33

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
CHICAGO DISTRICT OFFICE & FIELD OFFICE	101 WEST IDA B. WELLS DRIVE	CHICAGO	IL	60605	DO/FO	241
CHICAGO LOCKBOX	131 S. DEARBORN ST.	CHICAGO	IL	60608	LB	10
CHICAGO ASYLUM OFFICE	181 W. MADISON ST.	CHICAGO	IL	60602	AO	69
NORRIDGE ASC	4701 NORTH CUMBERLAND AVENUE, Suites B-D	NORRIDGE	IL	60706	ASC	9
NAPERVILLE ASC	888 SOUTH ROUTE 59, Suite 124	NAPERVILLE	IL	60540	ASC	6
WAUKEGAN ASC	25 SOUTH GREENBAY ROAD	WAUKEGAN	IL	60085	ASC	5
AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATION	350 EAST CERMAK RD 5TH FLOOR	CHICAGO	IL	60616	Commercial site	0
CHICAGO SOUTH ASC	8004 B SOUTH CICERO AVENUE	CHICAGO	IL	60459	ASC	7
MICHIGAN CITY ASC	284 DUNES PLAZA	MICHIGAN CITY	IN	46360	ASC	9
ST LOUIS FIELD OFFICE & ASC	1222 SPRUCE STREET	SAINT LOUIS	MO	63103	FO/ASC	26
KANSAS CITY DISTRICT OFFICE, FIELD OFFICE & ASC	10320 NW PRAIRIE VIEW RD	KANSAS CITY	MO	64153	DO/ASC	52
KANSAS CITY OSI OFFICE	8930 WARD PARKWAY SUITE 2079	KANSAS CITY	MO	64114	OSI	8
WICHITA FIELD OFFICE & ASC	550 WEST DOUGLAS AVENUE	WICHITA	KS	67203	FO/ASC	12
DES MOINES FIELD OFFICE & ASC	210 WALNUT STREET	DES MOINES	IA	50309	FO/ASC	18
OMAHA FIELD OFFICE & ASC	1717 AVENUE H	OMAHA	NE	68110	FO/ASC	17
OMAHA ASYLUM OFFICE	111 SOUTH 18TH STREET	OMAHA	NE	68111	AO	4

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
RAPID CITY ASC	2255 HAINES AVENUE, SUITE 214	RAPID CITY	SD	57701	ASC	3
ST. PAUL FIELD OFFICE & EEO OFFICE	2901 METRO DRIVE	BLOOMINGTON	MN	55425	FO	76
SIOUX FALLS SUPPORT OFFICE & ASC	300 EAST 8TH STREET	SIOUX FALLS	SD	57103	ASC	13
DULUTH ASC	515 W. 1ST STREET, SUITE 208	DULUTH	MN	55802	ASC	4
FARGO ASC	657 2ND AVENUE N., SUITE 248	FARGO	ND	58102	ASC	3
ST. PAUL ASC	1360 UNIVERSITY AVENUE, SUITE 103	SAINT PAUL	MN	55104	ASC	5
DALLAS DISTRICT OFFICE & FIELD OFFICE	6500 CAMPUS CIRCLE DRIVE EAST	IRVING	TX	75063	DO	154
OKLAHOMA CITY FIELD OFFICE & ASC	7100 SOUTH I35 SERVICE ROAD	OKLAHOMA CITY	OK	73149	FO/ASC	38
LEWISVILLE LOCKBOX	2501 S. STATE HIGHWAY 121	LEWISVILLE	TX	75067	LB	12
DALLAS NORTH ASC	10051 WHITEHURST DRIVE, SUITE 200	DALLAS	TX	75243	ASC	7
FORT WORTH ASC	5932 Quebec Street, Suite 160	FORT WORTH	TX	76135	ASC	6
LUBBOCK ASC	3502 SLIDE ROAD, Suite A-24	LUBBOCK	TX	79414	ASC	7
DALLAS SOUTH ASC	7334 SOUTH WESTMORELAND ROAD	DALLAS	TX	75237	ASC	7
HOUSTON DISTRICT OFFICE & FIELD OFFICE	810 GEARS RD	HOUSTON	TX	77067	DO	259
HOUSTON - SOUTHEAST ASC	8505 GULF FRWY, Suite D	HOUSTON	TX	77017	ASC	8
HOUSTON - SOUTHWEST ASC	11777 STATE HIGHWAY 6 SOUTH	SUGARLAND	TX	77498	ASC	16
HOUSTON - NORTHWEST ASC	10555 NORTHWEST FREEWAY, Suite 150	HOUSTON	TX	77092	ASC	13

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
HOUSTON ASYLUM OFFICE	16630 IMPERIAL VALLEY, SUITE 200	HOUSTON	TX	77060	ASY	229
SAN ANTONIO DISTRICT OFFICE, FIELD OFFICE & ASC	8940 FOUR WINDS DRIVE	WINDCREST	TX	78239	DO	122
HARLINGEN FIELD OFFICE & ASC	1717 ZOY STREET	HARLINGEN	TX	78552	FO/ASC	56
EL PASO FIELD OFFICE	1545 HAWKINS BOULEVARD	EL PASO	TX	79925	FO	55
ALBUQUERQUE FIELD OFFICE	1720 RANDOLPH ROAD SE	ALBUQUERQUE	NM	87106	FO	20
ALBUQUERQUE ASC	1605 ISLETA BOULEVARD, S.W., Suite C	ALBUQUERQUE	NM	87105	ASC	7
EL PASO ASC	10500 MONTWOOD DRIVE, Suite 167	EL PASO	TX	79935	ASC	6
MCALLEN ASC	220 SOUTH BICENTENNIAL BOULEVARD, Suite C	MCALLEN	TX	78501	ASC	6
NCSC – CEC TIER 1	2901 N. 23RD ST	MCALLEN	TX	78501	CC	201
LAREDO ASC	707 EAST CALTON ROAD, Suite 301	LAREDO	TX	78041	ASC	6
AUSTIN ASC	11301 LAKELINE BOULEVARD, Suite 150	AUSTIN	TX	78717	ASC	5
SAN ANTONIO ASC	5121 CRESTWAY DRIVE, Suite 112	SAN ANTONIO	TX	78239	ASC	7
KARNES CITY DETENTION CENTER	409 FN 1144	KARNES CITY	TX	78118	ASYLUM	17
PEARSALL DETENTION CENTER	566 VETERANS DRIVE	PEARSALL	TX	78061	ASYLUM	11
CIBOLO DETENTION CENTER	2000 CIBOLA LOOP	CIBOLO	NM	87021	ASYLUM	8
DILLEY RESIDENCE CENTER	300 EL RANCO WAY	DILLEY	TX	78017	ASYLUM	39

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
DENVER DISTRICT OFFICE & FIELD OFFICE	12484 E. WEAVER PLACE	CENTENNIAL	CO	80111	DO	88
SALT LAKE CITY FIELD OFFICE & ASC	TBD	SALT LAKE CITY	UT	84123	FO/ASC	57
HELENA FIELD OFFICE & ASC	754 RIVER ROCK DRIVE	HELENA	MT	59602	FO/ASC	14
BOISE FIELD OFFICE & ASC	1185 S. VINNELL WAY	BOISE	ID	83709	FO/ASC	21
IDAHO FALLS ASC	2265 WEST BROADWAY, SUITE A	IDAHO FALLS	ID	83402	ASC	3
CASPER ASC	150 E B STREET ROOM 1014	CASPER	WY	82601	ASC	2
DENVER ASC	15037 EAST COLFAX AVENUE, Unit G	AURORA	CO	80011	ASC	8
GRAND JUNCTION ASC	2454 HIGHWAY 6 & 50, Suite 115	GRAND JUNCTION	CO	81505	ASC	4
WESTERN REGION OFFICE	24000 AVILA ROAD	LAGUNA NIGUEL	CA	92677	RO	93
WESTERN FORM CENTER	5160 RICHTON STREET	MONTCLAIR	CA	91763	FC	9
SEATTLE DISTRICT OFFICE, FIELD OFFICE & ASC	12500 TUKWILA INTERNATIONAL BOULEVARD	SEATTLE	WA	98168	DO/ASC	127
SPOKANE FIELD OFFICE & ASC	920 WEST RIVERSIDE AVENUE, ROOM 691	SPOKANE	WA	99201	FO/ASC	14
YAKIMA FIELD OFFICE & ASC	415 NORTH THIRD STREET	YAKIMA	WA	98901	FO/ASC	21
ANCHORAGE FIELD OFFICE & ASC	620 E. 10TH AVENUE, SUITE 102	ANCHORAGE	AK	99501	FO/ASC	17
PORTLAND FIELD OFFICE & ASC	1455 NW Overton	PORTLAND	OR	97209	FO/ASC	52
SAN FRANCISCO DISTRICT OFFICE & FIELD OFFICE	630 SANSOME STREET	SAN FRANCISCO	CA	94111	DO	184

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
SAN FRANCISCO ASYLUM OFFICE	95 HAWTHORNE STREET, #303S	SAN FRANCISCO	CA	94105	ASY	149
SAN JOSE FIELD OFFICE	1450 COLEMAN AVENUE	SANTA CLARA	CA	94107	FO	92
OAKLAND ASC	2040 TELEGRAPH AVENUE	OAKLAND	CA	94612	ASC	10
SANTA ROSA ASC	1401 GUERNEVILLE ROAD, Suite 100	SANTAS ROSA	CA	95403	ASC	6
SALINAS ASC	1954 NORTH MAIN STREET	SALINAS	CA	93906	ASC	5
SAN FRANCISCO ASC	250 BROADWAY STREET	SAN FRANCISCO	CA	94111	ASC	9
SAN JOSE ASC	1450 COLEMAN AVENUE	SANTA CLARA	CA	94107	ASC	8
SACRAMENTO DISTRICT OFFICE & FIELD OFFICE	650 CAPITOL MALL	SACRAMENTO	CA	95814	DO/FO	100
FRESNO FIELD OFFICE	1177 FULTON MALL	FRESNO	CA	93721	FO	64
SACRAMENTO ASC	825 RIVERSIDE PARKWAY, SUITE 100	SACRAMENTO	CA	95605	ASC	8
MODESTO ASC	901 NORTH CARPENTER ROAD, Suite 14	MODESTO	CA	95351	ASC	7
FRESNO ASC	4893 EAST KINGS CANYON ROAD	FRESNO	CA	93727	ASC	7
BAKERSFIELD ASC	4701 PLANZ ROAD, Suite A12	BAKERSFIELD	CA	93309	ASC	8
SAN BERNARDINO FIELD OFFICE	655 WEST RIALTO AVENUE	SAN BERNARDINO	CA	92410	FO	71
SAN BERNARDINO ANNEX	290 N. D Street	SAN BERNARDINO	CA	92401	FO	58
LOS ANGELES DISTRICT OFFICE, FIELD OFFICE, LOS ANGELES COUNTY	300 NORTH LOS ANGELES STREET, ROOM 1001	LOS ANGELES	CA	90012	DO/ICS	450

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
FIELD OFFICE & WESTERN ICS						
LOS ANGELES ASYLUM OFFICE	1585 SOUTH MANCHESTER AVENUE	ANAHEIM	CA	92802	ASY	201
SAN FERNANDO FIELD OFFICE & ASC	19809 PRAIRIE STREET	CHATSWORTH	CA	91311	FO	92
CHATSWORTH ASC	19809 PRAIRIE STREET	CHATSWORTH	CA	91311	ASC	10
SANTA ANA FIELD OFFICE	34 CIVIC CENTER PLAZA	SANTA ANA	CA	92701	FO	110
POMONA ASC	435 WEST MISSION BOULEVARD, Suite 110	POMONA	CA	91766	ASC	6
EL MONTE ASC	9251 GARVEY AVENUE, Suite Q	SOUTH EL MONTE	CA	91733	ASC	11
GARDENA ASC	15715 CRENSHAW BOULEVARD, Room B-112	GARDENA	CA	90249	ASC	5
BELLFLOWER ASC	17610 BELLFLOWER BOULEVARD, Suite A-110	BELLFLOWER	CA	90706	ASC	5
FAIRFAX/LA BREA ASC	5949 WEST PICO BOULEVARD	LOS ANGELES	CA	90035	ASC	3
SANTA ANA ASC	1666 NORTH MAIN STREET, Suite 100-A	SANTA ANA	CA	92701	ASC	6
BUENA PARK ASC	8381 LA PALMA AVENUE, Suite A	BUENA PARK	CA	90620	ASC	6
RIVERSIDE ASC	10082 MAGNOLIA AVENUE	RIVERSIDE	CA	92503	ASC	9
OXNARD ASC	2000 OUTLET CENTER DRIVE, SUITE 200	OXNARD	CA	93036	ASC	5
WILSHIRE ASC	1015 WILSHIRE BOULEVARD	LOS ANGELES	CA	93017	ASC	11

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
TUSTIN ASC	14541 RED HILL AVENUE	TUSTIN	CA	92780	ASC	10
SAN DIEGO DISTRICT OFFICE & FIELD OFFICE	880 FRONT STREET, SUITE 1234	SAN DIEGO	CA	92101	DO/FO	127
SAN DIEGO ASC	16555 BROADWAY	CHULA VISTA	CA	91911	ASC	7
SAN DIEGO DETENTION FACILITY (CCA)	7488CALZADA DE LA FUENTE	SAN DIEGO	CA	92158	ICE	4
SAN MARCOS ASC	727 WEST SAN MARCOS BOULEVARD, SUITES 101-103	SAN MARCOS	CA	92078	ASC	6
IMPERIAL FIELD SUPPORT OFFICE & ASC	509 INDUSTRY WAY	IMPERIAL	CA	92251	FSO/ASC	15
PASADENA HISTORICAL FINGERPRINT ENROLLMENT	75 NORHT FAIR OAKS, FLOOR 03	PASADENA	CA	91103	HFE	69
ADELANTO DETENTION FACILITY	10400 RANCHO ROAD	ADELANTO	CA	92301	ICE	TBD
IMPERIAL REGIONAL DETENTION CENTER	1572 GATEWAY RD	CALEXICO	CA	92231	ICE	TBD
PHOENIX DISTRICT OFFICE, FIELD OFFICE & ASC	1300 SOUTH 16TH STREET	PHOENIX	AZ	85034	DO/FO/ASC	120
ELOY DETENTION FACILITY	1705 EAST HANNA RD	ELOY	AZ	85231	ICE	9
FLORENCE DETENTION FACILITY	3250 NORTH PINAL PKWY	FLORENCE	AZ	85232	ICE	4
RENO FIELD OFFICE & ASC	790 SANDHILL RD	RENO	NV	83502	FO/ASC	21
LAS VEGAS FIELD OFFICE & ASC	5650 WEST BADURA AVE	LAS VEGAS	NV	89118	FO/ASC	102

Location Name	Street Address	City	State	Zip Code	Office Types	End Users
LAS VEGAS DETENTION FACILITY	3373 PEPPER LANE	LAS VEGAS	NV	89120	ICE	5
LAS VEGAS EOIR COURT	3365 PEPPER LANE	LAS VEGAS	NV	89120	ICE	5
TUCSON FIELD OFFICE & ASC	4475 S COACH DRIVE	TUCSON	AZ	85714	FO/ASICEC	46
PHOENIX LOCKBOX	1820 E SKY HARBOR CIRCLE SOUTH, 1st Floor	PHOENIX	AZ	85034	LB	13
YUMA ASC	3250 SOUTH 4TH AVENUE, Suite E	YUMA	AZ	85365	ASC	7
AGANA FIELD OFFICE & ASC	108 HERNAN CORTEZ, SUITE 100	AGANA	GU	96910	FO/ASC	24
GUAM DETENTION FACILITY	108 HERNAN CORTEZ AVE.	Hagatna	GU	96910	ICE	5
HONOLULU DISTRICT OFFICE, FIELD OFFICE & ASC	500 ALA MOANA BLVD	HONOLULU	HI	96813	DO/ASC	50
HAWAII DETENTION AND REMOVAL OPERATION	595 ALA MOANA BLVD	HONOLULU	HI	96813	ICE	5
SAIPAN ASC	TSL PLAZA BUILDING BEACH ROAD	GARAPAN	MP	96951	ASC	6

USCIS Centers						
Location Name	**Street Address**	**City**	**State**	**Zip Code**	**Office Types**	**End Users**
NATIONAL BENEFITS CENTER – LEE'S SUMMIT	850 NW CHIPMAN ROAD	LEES SUMMIT	MO	64063	NBC	1,950
NATIONAL BENEFITS CENTER – OVERLAND PARK	7600 W. 119th STREET	OVERLAND PARK	KS	66213	NBC	750

USCIS Centers						
Location Name	**Street Address**	**City**	**State**	**Zip Code**	**Office Types**	**End Users**
LEE'S SUMMIT PROCESSING FACILITY	777 NW BLUE PARKWAY	LEES SUMMIT	MO	64086	CARD	25
NATIONAL RECORDS CENTER	150 NW SPACE CENTER LOOP	LEES SUMMIT	MO	64064	NRC	806
NATIONAL RECORDS CENTER – Extension Site 1	LOOP	LEES SUMMIT	MO	64064	NRC	25
TEXAS SERVICE CENTER - MESQUITE	4141 N SAINT AUGUSTINE ROAD	DALLAS	TX	75227	SC	449
TEXAS SERVICE CENTER - DALLAS	7701 N STEMMONS FREEWAY	DALLAS	TX	75247	SC	382
TEXAS SERVICE CENTER - DALLAS	8001 N STEMMONS FREEWAY	DALLAS	TX	75247	SC	474
NEBRASKA SERVICE CENTER – HIGHLANDS BUILDING	1301 WEST HIGHLAND BOULEVARD	LINCOLN	NE	68521	SC	500
NEBRASKA SERVICE CENTER – STAR BUILDING	850 S STREET	LINCOLN	NE	68508	SC	750
NEBRASKA SERVICE CENTER DACA – FEDERAL BUILDING	100 Centennial Mall North	LINCOLN	NE	68508	SC	80
VERMONT SERVICE CENTER - TABOR BUILDING	COOTE FIELD INDUSTRIAL PARK	SAINT ALBANS	VT	05479	SC	1,213
VERMONT SERVICE CENTER - ESSEX IBM CAMPUS #1	30 RIVER ROAD	ESSEX	VT	05452	SC	570
Location Name	**Street Address**	**City**	**State**	**Zip Code**	**Office Types**	**End Users**
VERMONT SERVICE CENTER - ESSEX IBM CAMPUS #2	38 RIVER ROAD	ESSEX	VT	05452	SC	280

USCIS Centers						
Location Name	**Street Address**	**City**	**State**	**Zip Code**	**Office Types**	**End Users**
LAGUNA NIGUEL REGIONAL OFFICE & CALIFORNIA SERVICE CENTER	24000 AVILA ROAD	LAGUNA NIGUEL	CA	92677	SC	1,549
POTOMAC SERVICE CENTER	2200 CRYSTAL DRIVE	ARLINGTON	VA	22202	SC	904
TWIN CITIES MANAGEMENT OFFICE	9360 ENSIGN AVENUE	BLOOMINGTON	MN	55438	TCMO	250
ENTERPRISE OPERATIONS CENTER	1 Stennis Space Center - NASA	STENNIS	MS	39529	SD/NOC/SOC	100
USCIS MANAGEMENT HEADQUARTERS (ETD 2021)	TBD	RALEIGH	NC	TBD	HQ/MGMT	150
EQUINIX ASHBURN DATA CENTER	21691 FILIGREE COURT BLDG DC4	ASHBURN	VA	20147	DC	0
EQUINIX CHICAGO DATA CENTER	1905 LUNT AVENUE BLDG CH3	CHICAGO	IL	60007	DC	0
EQUINIX DALLAS DATA CENTER	1950 NORTH STEMMONS FREEWAY BLDG 6	DALLAS	TX	75207	DC	0
EQUINIX SAN JOSE DATA CENTER	9 GREAT OAKS BLVD BLDG 5	SAN JOSE	CA	95119	DC	0
TOTAL						27,309

OCONUS

* Total should include Refugee Officer Corps (69 end users) with a total of 166 OCONUS end users.

Location Code	Location Name	Street Address	City	Country	End Users
RIT	ROME DISTRICT OFFICE	VIA VITTORIO VENETO 119A Closing February 2020	ROME	ITALY	16
ACG	ACCRA SUB OFFICE (U.S. EMBASSY ANNEX BUILDING #10)	11 LANE EMBASSY ROAD Closing January 2020	ACCRA	GHANA	5

Location Code	Location Name	Street Address	City	Country	End Users
JHS	JOHANNESBURG SUB OFFICE	1 RIVER ST Closing January 2020	JOHANNESBURG	SOUTH AFRICA	2
ATH	ATHENS SUB OFFICE	91 VASSILISSIS SOFIAS AVENUE Closing January 2020	ATHENS	GREECE	6
FKG	FRANKFURT SUB OFFICE	GIESSENER STRASSE 30 Closing January 2020	FRANKFURT	GERMANY	8
AMM	AMMAN SUB OFFICE	AMERICAN EMBASSY Closing January 2020	AMMAN	JORDAN	3
LDN	LONDON SUB OFFICE	5 UPPER GROSVENOR STREET Closing January 2020	LONDON	ENGLAND	4
NBO	NAIROBI SUB OFFICE	UNITED NATIONS AVENUE, GIGIRI	NAIROBI	KENYA	5
MEX	MEXICO DISTRICT OFFICE	PASEO de la REFORMA # 305	MEXICO DF	MEXICO	17
GMT	GUATEMALA CITY SUB OFFICE	AVENIDA de la REFORMA 7-01ZONA 10	GUATEMALA CITY	GUATEMALA	7
LMA	LIMA SUB OFFICE	AVENIDA ENCALADA, CUADRA 17 Closing January 2020	LIMA	PERU	5
SAN	SAN SALVADOR SUB OFFICE	FINAL BOULEVARD SANTA ELENA	SAN SALVADOR	EL SALVADOR	3
SDM	SANTO DOMINGO SUB OFFICE	CALLE CESAR NICOLAS PENZON Closing March 2020	SANTO DOMINGO	DOMINICAN REPUBLIC	3
BEI	BEIJING SUB OFFICE	XIU SHUI BEI JIE 3	BEIJING	CHINA	8
GZH	GUANGZHOU SUB OFFICE	1 SHAMIAN SOUTH ST.	GUANGZHOU	CHINA	8
NDI	NEW DELHI SUB OFFICE	SHANTI PATH, CHANAKYAPURI	NEW DELHI	INDIA	12
TOTAL					112
1.1.1.1.1.	****USCIS HQ Plans to move December 2020 more details will be provided after award when available***				

ATTACHMENT 2 – FIELD SERVICES: PHYSICAL PLACE OF PERFORMANCE

City	State	Field Office
Washington	DC	HQU - 111 Mass. Ave.
Washington	DC	HQR - 1200 First St.
Washington	DC	HQP - 20 Mass Ave.
Washington	DC	HQM - 131 M. St.
Washington	DC	CJD - 633 Judiciary Sq.
Camp Springs	MD	OTC – One Town Center
Fairfax	Virginia	Washington DO/FO
Arlington	Virginia	Arlington Asylum
Norfolk	Virginia	Norfolk FO/ASC
Baltimore	Maryland	Baltimore DO/FO
Arlington	Virginia	AAO - 2121 Crystal Drive
Washington	DC	MRY – Maryland Avenue
Arlington	VA	Potomac Service Center
Glenmont	MD	Glenmont ASC
Salisbury	MD	Salisbury ASC
Washington	DC	999 North Capital St.
Harrisonburg	VA	COOP site
Alexandria	VA	Alexandria ASC
Arlington	VA	JETS Contractor site
Lincoln	Nebraska	NSC
Lee's Summit	Missouri	Lee’s Summit, MO/Overland Park, KS NBC
Lee's Summit	Missouri	OSI Office Site/Kansas City, KS NBC
Lee's Summit	Missouri	Lee’s Summit, MO NRC
Lee's Summit	Missouri	Lee’s Summit, MO LPF
Detroit	Michigan	Detroit DO/ASC
Grand Rapids	Michigan	Grand Rapids ASC
Cleveland	Ohio	Cleveland DO/FO/ASC

City	State	Field Office
Cleveland	Ohio	Cleveland Asylum Office
Cincinnati	Ohio	Cincinnati FO/ASC
Columbus	Ohio	Columbus FO/ASC
Indianapolis	Indiana	Indianapolis FO/ASC
Barbourville	Kentucky	Barbourville Customer Contact Center
Louisville	Kentucky	Louisville FO/ASC
Corbin	Kentucky	Corbin ICPF
Williamsburg	Kentucky	Kentucky Consular Center
Chicago	Illinois	Chicago DO/FO/ASC/AO/Lockbox
Chicago	Illinois	Naperville ASC
Chicago	Illinois	Norridge ASC
Chicago	Illinois	Pulaski ASC
Chicago	Illinois	Broadway ASC
Waukegan	Illinois	Waukegan ASC
Michigan City	Michigan	Michigan City ASC
Milwaukee	Wisconsin	Milwaukee FO/ASC
Kansas City	Missouri	Kansas City DO/FO/ASC
Duluth	Minnesota	Duluth ASC
Fargo	North Dakota	Fargo ASC
Rapid City	South Dakota	Rapid City ASC
Sioux Falls	South Dakota	Sioux Falls ASC
St. Paul	Minnesota	St. Paul FO/ASC
Bloomington	Minnesota	Twin Cities Management Office
Omaha	Nebraska	Omaha FO/ASC
Omaha	Nebraska	Omaha Asylum
Des Moines	Iowa	Des Moines FO/ASC
St. Louis	Missouri	St Louis FO/ASC
Wichita	Kansas	Wichita FO/ASC
Denver	Colorado	Denver DO/FO/ASC
Grand Junction	Colorado	Grand Junction ASC

City	State	Field Office
Casper	Wyoming	Casper ASC
Idaho Falls	Idaho	Idaho Falls ASC
Boise	Idaho	Boise FO/ASC
Helena	Montana	Helena FO/ASC
Salt Lake City	Utah	Salt Lake City FO/ASC
Dallas	Texas	TSC
Irving	Texas	Central Region Office
Irving	Texas	Dallas Training Academy
Dallas	Texas	Dallas DO/FO
Houston	Texas	Houston DO/FO
San Antonio	Texas	San Antonio DO/FO/ASC
Harlingen	Texas	Harlingen FO/ASC
El Paso	Texas	El Paso FO/ASC
Dallas	Texas	ASC - North
Dallas	Texas	ASC - South
Lewisville	Texas	Lockbox
Ft. Worth	Texas	Fort Worth ASC
Lubbock	Texas	Lubbock ASC
Oklahoma City	Oklahoma	Oklahoma City FO/ASC
Houston	Texas	Asylum Office
Houston	Texas	ASC - Southeast
Houston	Texas	ASC - Southwest
Houston	Texas	ASC - Northwest
Albuquerque	New Mexico	FO/ASC
Laredo	Texas	ASC
Austin	Texas	ASC
McAllen	Texas	McAllen Customer Contact Center
Ft. Worth	Texas	Ft. Worth Customer Contact Center
Karnes City	Texas	Detention Center

City	State	Field Office
Pearsall	Texas	Detention Center
Cibolo	New Mexico	Detention Center
Gallup	New Mexico	Detention Center
Dilley	Texas	Residence Center
Fort Sill	Texas	ASC
St. Albans	Vermont	VSC - Tabor Bldg.
Boston	Massachusetts	Boston DO/FO/ASC
Latham	New York	Albany FO
Philadelphia	Pennsylvania	Philadelphia FO/ASC
Portland	Maine	Portland FO/ASC
Buffalo	New York	Buffalo Verification Office
Buffalo	New York	Buffalo FO
Essex	Vermont	VSC - Essex
S. Burlington	Vermont	S. Burlington Regional Office
S. Burlington	Vermont	OSI/PSD
Williston	Vermont	Technology and Training Center
Essex Junction	Vermont	Essex Junction FO
Newark	New Jersey	Newark DO/FO
Newark	New Jersey	Newark Asylum
Pittsburgh	Pennsylvania	Pittsburgh FO
New York	New York	New York DO/FO/ASC
S. Burlington	Vermont	S. Burlington Regional Office
New York	New York	Eastern Telephone Center (ETC)
Hartford	Connecticut	Hartford FO/ASC
Lawrence	Massachusetts	Lawrence FO/ASC
Clarksburg	West Virginia	Clarksburg FO
Charleston	West Virginia	ASC
Dover	Delaware	ASC
York	Pennsylvania	ASC
Bethpage	New York	New York Asylum

City	State	Field Office
Hackensack	New Jersey	ASC
Providence	Rhode Island	FO/ASC
New Rochelle	New York	ASC
Brooklyn	New York	ASC
Bronx	New York	ASC
Atlanta	Georgia	Atlanta DO/FO
Atlanta	Georgia	Atlanta Asylum Office
Atlanta	Georgia	Atlanta ASC
Tampa	Florida	Tampa DO/FO/ASC
Charlotte	North Carolina	Charlotte FO/ASC
Greer	South Carolina	Greer FO/ASC
Columbia	South Carolina	Fort Jackson Military Support Office
Miami	Florida	Hileah Field Office
Miami	Florida	Kendall FO
Miami	Florida	Miami DO/FO/ASC
Miami	Florida	Miami Asylum Office
Orlando	Florida	Orlando SERO
Orlando	Florida	Orlando FO
Nashville	Tennessee	Nashville FO
Memphis	Tennessee	Memphis FO/ASC
Charleston	South Carolina	Charleston FO
Charleston	South Carolina	Charleston Training Academy (FLETC)
Fort Smith	Arkansas	Fort Smith FO
Fort Myers	Florida	Fort Myers FO/ASC
West Palm Beach	Florida	West Palm Beach FO/ASC
Jackson	Mississippi	Jackson Field Support Office/ASC
New Orleans	Louisiana	New Orleans DO/FO/ASC
New Orleans	Louisiana	New Orleans Asylum Office
Bossier City	Louisiana	Bossier City Customer Contact Center
San Juan	Puerto Rico	San Juan FO
Jacksonville	Florida	Jacksonville FO/ASC

City	State	Field Office
Oakland Park	Florida	Oakland Park FO
Raleigh	North Carolina	Raleigh FO
Birmingham	Alabama	Birmingham ASC
Montgomery	Alabama	Montgomery FO
Saint Croix	U.S. Virgin Islands	Saint Croix Sub-Office/ASC
Saint Thomas	U.S. Virgin Islands	Saint Thomas FO/ASC
Laguna Niguel	California	CSC/RO
Seattle	Washington	Seattle DO/FO/ASC
Tucson	Arizona	Tucson FO
Yuma	Arizona	Yuma ASC
Fresno	California	Fresno FO/ASC
Los Angeles	California	Los Angeles DO/FO
Anchorage	Alaska	Anchorage FO
San Francisco	California	San Francisco Asylum
San Bernardino	California	San Bernardino FO
Phoenix	Arizona	Phoenix DO/FO
San Diego	California	San Diego DO/FO
Reno	Nevada	Reno FO
Las Vegas	Nevada	Las Vegas FO
Agana	Guam	Guam FO
Honolulu	Hawaii	Honolulu DO/FO/ASC
Portland	Oregon	Portland OR FO/ASC
Yakima	Washington	Yakima FO/ASC
Santa Ana	California	Santa Ana DO
San Jose	California	San Jose FO/ASC
Chatsworth	California	San Fernando FO/ASC
Los Angeles	California	Western Telephone Center (WTC)
Tustin	California	Tustin ASC
Adelanto	California	Adelanto Detention Facility
Calexico	California	Imperial Regional Detention Center
Santa Ana	California	Santa Ana Sub-Office

City	State	Field Office
Eloy	Arizona	Eloy Detention Facility
Florence	Arizona	Florence Detention Facility
Las Vegas	Nevada	Las Vegas Detention Facility
Las Vegas	Nevada	Las Vegas EOIR Court
Anaheim	California	Los Angeles Asylum
Hagatna	Guam	Guam Detention Facility
Garapan	Mariana Islands	Saipan ASC
Honolulu	Hawaii	Hawaii Detention and Removal Operation
Sacramento	California	Sacramento DO/FO/ASC
Seattle	Washington	Seattle DO/FO/ASC
San Francisco	California	San Francisco DO/FO
Pasadena	California	Historical Fingerprint Enrollment
Calexico	California	Imperial Regional Detention Center
Dallas	Texas	Equinix Dallas Data Center
Ashburn	Virginia	Equinix Ashburn Data Center
San Jose	California	Equinix San Jose Data Center
Elk Grove Village	Illinois	Equinix Chicago Data Center

ATTACHMENT 3 – AFTER ACTION REPORT TEMPLATE

The purpose of the After Action Report is to provide a detailed analysis of the outage or maintenance for follow-up purposes.

Title	Description
AAR Number	
Description of Incident/Violation	
Ticket #	
Prepared By	
Date Incident/Process Violation Occurred	
Time Incident / Process Violation Occurred	
Duration	
Systems/Network /Process Affected	
Customers/Site Affected	
Troubleshooting Steps/Analysis, if applicable	
Resolution/Corrective Action	
Root Cause, if identifiable	
Preventive Action	
Knowledge Base Update, if applicable	
Lessons Learned	
Supervisor Name and Review Date	

Service Manager Name and Review Date	

Attachment 4 – Sites Requiring Onsite Staff

USCIS Staffed Locations

Current	Location	Site Code	Onsite/Remote
District 01	Boston, MA District Office	BOS	Onsite
	Hartford, CT Field Office	HAR	Onsite
	Lawrence Field Office	LAW	Onsite
	Manchester, NH Field Office	MNH	Onsite
District 02	Albany, NY Field Office	ANY	Onsite
	Buffalo, NY District Office	BUF	Onsite
	Buffalo, NY Verification Office	BEV	Onsite
	Northeast Regional Office	NER	Onsite
District 03	Queens, NY Field Office	QNS	Onsite
	Long island Field Office	LNY	Onsite
	New York City Asylum Office	ZNY	Onsite
	New York City District Office	NYC	Onsite
	Eastern Telephone Center	ETC	Onsite
	NYC - Holtsville ASC	XNQ	Onsite
District 04	Mt Laurel Field Office	MTL	Onsite
	Newark, NJ Asylum	ZNK	Onsite
	Newark, NJ District Office	NEW	Onsite
District 05	Philadelphia, PA District Office	PHI	Onsite
	Pittsburgh, PA Field Office	PIT	Onsite
Vermont Service Center (VSC)		VSC/VES	Onsite
Washington, DC	111 Mass Ave, NW	HQU	Onsite
	20 Mass Ave, NW	HQP	Onsite
	131 M Street	HQM	Onsite
	1200 1st Street	HQR	Onsite
	633 3rd Street	CJD	Onsite
	Crystal City	CCV	Onsite

	Camp Springs (2020)	COW	Onsite
District 06	Baltimore, MD District Office	BAL	Onsite
	Arlington, VA Asylum Office	ZAR	Onsite
District 07	Norfolk, VA Field Office	NOR	Onsite
	Washington, DC District Office	WAS	Onsite
	Administrative Appeals Office	AAO	Onsite
Potomac Service Center		PSC	Onsite
District 08	Atlanta DO/FO, GA	ACS	Onsite
	Atlanta Asylum/Vetting		Onsite
	Charleston FO/ASC, SC	CHO/XAE	Onsite
	Charleston Training Academy		Onsite
	Charlotte FO, NC	CLT	Onsite
	Greer FSO, SC	GRR	Onsite
	Raleigh FO/ASC, NC	RAL/XAF	Onsite
	Montgomery FO, AL		Onsite
District 09	Hialeah FO/ASC, FL	HIA/XMA	Onsite
	Kendall FO/ASC, FL	KND/XMC	Onsite
	Miami Asylum Office, FL	ZMI/MIH	Onsite
	Miami DO/FO/ASC, FL	MIA/XMB	Onsite
	Oakland Park FO/ASC, FL	OKL/XMD	Onsite
	San Juan FO, PR	SAJ/XPM	Onsite
	St. Thomas FO, PR	CHA	Onsite
District 10	Ft. Myers FO, FL	XMJ	Onsite
	Jacksonville FO/ASC, FL	JAC/	Onsite
	Orlando FO, FL	ORL	Onsite
	Southeast RO, FL	SER	Onsite
	Tampa DO/FO, FL	TMP/XMF	Onsite
	West Palm Beach FO/ASC, FL	WPB/XMH	Onsite
District 11	Bossier City Call Center, LA	BSR	Onsite
	New Orleans DO/FO/ASC, LA	NOL/XNA	Onsite
	Fort Smith FO/ASC, AR	FSA/XNB	Onsite

	Memphis FO/ASC, TN	MEM/XND	Onsite
	Nashville FO, TN	NSV	Onsite
	Stennis	ENO	Onsite
District 12	Detroit DO & FO	DMI	Onsite
District 13	Barbourville Call Center, KY	BVK	Onsite
	Corbin Card Production Facility	CBN	Onsite
	Cleveland DO & FO	CLE	Onsite
	Cincinnati FO	CIN	Onsite
	Louisville FO	LOU	Onsite
District 14	Chicago DO & FO	CHI	Onsite
	Chicago Asylum	ZCH	Onsite
District 15	Kansas City DO/FO, MO	KMO	Onsite
	Omaha FO, NE	OMA	Onsite
	St. Louis FO, MO	SMO	Onsite
	St. Paul FO and EEO, MN	SPM	Onsite
District 19	Denver DO & FO	DEN	Onsite
	Boise FO	BOI	Onsite
	Helena FO	HEL	Onsite
	Salt Lake City FO	SLT	Onsite
National Benefits Center/National Records Center		MSC/NBC/NRC	Onsite
Nebraska Service Center		NSC/NSS	Onsite
Twin Cities Management Office		MDP	Onsite
District 16	Dallas District Office	DAL	Onsite
	Dallas Field Office		Onsite
	Irving Training Academy	DAT	Onsite
	Irving Central Region Headquarters	CRO	Onsite
District 17	Houston District Office	HOU	Onsite
	Houston Field Office	HLA	Onsite
	Houston Asylum Office	ZHN	Onsite
District 18	San Antonio District Office	SNA	Onsite

	San Antonio Field Office	SNA	
	Harlingen Field Office	HLG	Onsite
	McAllen Call Center	MAT	Onsite
	El Paso Field Office	ELP	Onsite
Texas Service Center		TSC	Onsite
District 20	Western Regional Office	WRO	Onsite
	Anchorage Field Office	ANC	Onsite
	Anchorage ASC	XAA	On site (co-located with ANC)
	Portland Field Office	PRT	Onsite
	Portland-OR ASC	XPL	On site (co-located with PRT)
	Seattle District Office	SEA	Onsite
	Seattle ASC	XSE	On site (co-located with SEA)
	Seattle Asylum		Extension of ZSF
	Spokane ASC	XSF	On site (co-located with SPO)
	Yakima ASC	XSH	On site (co-located with YBO)
	Yakima Field Office	YBO	Onsite
District 21	San Francisco District Office	SFR	Onsite
	San Jose Field Office	SNJ	Onsite
	San Jose ASC	XTE	On site (co-located with SNJ)
	San Francisco Asylum	ZSF	Onsite
District 22	Fresno Field Office	FRM	Onsite
	Sacramento District Office	SAC	Onsite

District 23	Los Angeles District Office	LOS	Onsite
	Los Angeles - WTC	LOS	Onsite
	Santa Ana Field Office	SAA	Onsite
	San Bernardino Field Office	SBD	Onsite
	San Fernando Field Office	SFN	Onsite
	Pasadena HFE	CPA	Onsite
	Los Angeles Asylum Office	ZLA	Onsite
District 24	San Diego District Office	SND	Onsite
	San Diego ASC	XSB	On site (co-located with CVS)
District 25	Las Vegas Field Office	LNV	Onsite
	Phoenix Field Office	PNX	Onsite
	Reno Field Office	RNO	Onsite
	Tucson Field Office	TUC	Onsite
	Las Vegas ASC	XPF	On site (co-located with LVG)
	Tucson ASC	XPG	On site (co-located with TUC)
	Reno Field ASC	XPH	On site (co-located with RNO)
	Phoenix ASC	XPQ	On site (co-located with PNX)
District 26	Agana Field Office (Guam)	AGA	Onsite
	Agana ASC	XHG	On site (co-located with AGA)
	Honolulu District Office	HHI	Onsite
	Honolulu ASC	XHF	On site (co-located with HHI)
California Service Center (CSC)		CSC	Onsite

ATTACHMENT 5 – ACRONYMS

ACD	Automated Call Distribution
AQL	Acceptable Quality Level
AISSO	Alternate Information System Security Officer
A/V	Audio/Video
BOM	Bills of Materials
C&A	Certification and Accreditation
CAB	Change Advisory Board
CIRT	Critical Incident Response Team
CISNET	Citizenship and Immigration Service Network
CLIN	Contract Line Item Number
CO	Contracting Officer
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations
COR	Contracting Officer's Representative
COTS	Commercial Off the Shelf
CSIRT	Computer Security Incident Response Team
CSL	Customer Service Liaison-EUS Employee
DHS	Department of Homeland Security
DTSPO	Diplomatic Telecommunications Service Program Office
FSE	Field Support Engineer
EIT	Electronic Information and Technology
EOC	Enterprise Operations Center
FC	Functional Category
FCR	First Call Resolution
FLR	First Level Resolution
GFI	Government Furnished Information
GFP	Government Furnished Property

GSA	General Services Administration
GSS	General Support Systems
GWAC	Government Wide Acquisition Contracts
HRG	Hardware Resolution Group
HQ	Headquarter
HW	Hardware
IDS	Industry Detention Systems
IPS	Intrusion Prevention Systems
ISD	Information Security Division
ISS	Internet Security Systems
IT	Information Technology
ITFS	Information Technology Field Services
ITIL	Information Technology Infrastructure Library
ITLM	Information Technology Lifecycle Technology
ITOM	Information Technology Operations and Maintenance
ITSM	Information Technology Services Management
IMAC	Install/Move/Add/Change
KM	Knowledge Management
LAN	Local Area Network
LBI	Limited Background Investigation
LCMS	Learning Content Management System
LDAP	Lightweight Directory Access Protocol
LMS	Learning Management Systems
MCD	Mobile Communications Devices
MD	Management Directive
MDO	Master Delivery Order
MS	Microsoft
MTR	Mean Time Resolution
NEON	Technology Operations Support
NC	National Capital
NSI	National Security Information
OCONUS	Outside of the Continental United States

OIT	Office of Information Technology
O&M	Operations and Maintenance
OSI	Office of Security and Integrity
PBMGT	Problem Management
PCA	Per-Call Authorization
PICS	Password Issuance and Control System
PIR	Post Implementation Review
PM	Program Manager
PWS	Performance Work Statement
QA	Quality Analysis
SBU	Sensitive but Unclassified
SD	Service Desk
SDA	Service Desk Analyst
SLA	Service Level Agreement
SLIN	Sub-Contract Line Item Number
SOC	Security Operation Center
SOP	Standard Operating Procedures
SQL	Structured Query Language
SR	Service Request
SRM	Service Request Management
SSO	Single Sign-On
SW	Software
TCDD	Training and Career Development Division
USCIS	United States Citizenship and Immigration Services
VPN	Virtual Private Network
WSUS	Windows Server Update Services
WTR	Wireless Technology Research

U.S. Citizenship and Immigration Services
Office of Security and Integrity – Personnel Security Division

SECURITY REQUIREMENTS

GENERAL

U.S. Citizenship and 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 classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 13526, Classified National Security Information, and supplementing directives.

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the National Industrial Security Program Operating Manual (NISPOM) for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service.

Any firm or business under contract with the Department of Homeland Security (DHS), which requires access to classified information, will require a Facility Security Clearance (FCL) commensurate with the level of access required. Firms that do not possess a FCL, or the requisite level FCL, will be sponsored by DHS to obtain one.

FITNESS DETERMINATION

USCIS shall have and exercise full control over granting, denying, withholding or terminating access of unescorted Contractor employees 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 Fitness authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment Fitness 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 Contractor employee shall be allowed unescorted access to a Government facility without a favorable EOD decision or Fitness determination by the Office of Security & Integrity Personnel Security Division (OSI PSD).

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information and/or classified information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the DHS Form 11000-25, Contractor Fitness/Security Screening Request Form and the USCIS Continuation Page to the DHS Form 11000-25. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI PSD.

Completed packages must be submitted to OSI PSD for prospective Contractor employees no less than 30 days before the starting date of the contract or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor. The Contractor shall follow guidelines for package submission as set forth by OSI PSD. A complete package will include the following forms, in conjunction with security questionnaire submission of the SF-85P, Security Questionnaire for Public Trust Positions via e-QIP:

1. Additional Questions for Public Trust Positions – Branching

2. DHS Form 11000-6, Conditional Access to Sensitive But Unclassified Information Non- Disclosure Agreement

3. FD Form 258, Fingerprint Card **(2 cards)**

4. DHS Form 11000-9, Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act

5. DHS Form 11000-25, Contractor Fitness/Security Screening Request Form

6. USCIS Continuation Page to DHS Form 11000-25

7. OF 306, Declaration for Federal Employment (approved use for Federal Contract Employment)

8. Foreign National Relatives or Associates Statement

EMPLOYMENT ELIGIBILITY

Be advised that unless an applicant requiring access to sensitive but unclassified information and/or classified information has resided in the U.S. for three of the past five years, OSI PSD 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.

Only U.S. citizens are eligible for employment on contracts requiring access to Department of Homeland Security (DHS) Information Technology (IT) systems or involvement in the development, operation, management, or maintenance of DHS IT systems, unless a waiver has been granted by the Director of USCIS, or designee, with the concurrence of both the DHS Chief Security Officer and the Chief Information Officer or their designees. In instances where non-IT requirements contained in the contract can be met by using Legal Permanent Residents, those requirements shall be clearly described.

VISIT AUTHORIZATION LETTER (VAL)

The Contractor is required to submit a VAL for those individuals who require access to classified information during performance on this contract and who have an active Personnel Security Clearance (PCL). The letter will be valid for a period not to exceed one year. If the requirement to access classified information no longer exists, or if access eligibility changes, OSI PSD will be notified immediately. The VAL must be submitted to OSI PSD in accordance with, and contain information as required by, Chapter 6 of the NISPOM.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the Contracting Officer's Representative (COR) will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract. In accordance with USCIS policy, contractors are required to undergo a periodic reinvestigation every five years.

Security documents will be submitted to OSI PSD within ten business days following notification of a contractor's reinvestigation requirement.

In support of the overall USCIS mission, Contractor employees are required to complete one-time or annual DHS/USCIS mandatory trainings. The Contractor shall certify annually, but no later than December 31st each year, or prior to any accelerated deadlines designated by USCIS, that required trainings have been completed. The certification of the completion of the trainings by all contractors shall be provided to both the COR and Contracting Officer.

- **USCIS Security Awareness Training** (required within 30 days of entry on duty for new contractors, and annually thereafter)
- **USCIS Integrity Training** (annually)
- **DHS Insider Threat Training** (annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **Unauthorized Disclosure Training** (one time training for contractors who require access to USCIS information regardless if performance occurs within USCIS facilities or at a company owned and operated facility)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)
- **USCIS PKI Initiative Training** (if supervisor determines the need for a PKI certificate)
- **Computer Security Awareness Training** (if contractor requires access to USCIS IT systems, training must be completed within 60 days of entry on duty for new contractors, and annually thereafter)

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 or whom USCIS determines to present a risk of compromising sensitive but unclassified information and/or classified information.

Contract employees will report any adverse information concerning their personal conduct to OSI PSD. The report shall include the contractor's name along with the adverse information being reported. Required reportable adverse information includes, but is not limited to, criminal charges and or arrests, negative change in financial circumstances, and any additional information that requires admission on the SF-85P security questionnaire or on any security form listed above.

In accordance with Homeland Security Presidential Directive-12 (HSPD-12) http://www.dhs.gov/homeland-security-presidential-directive-12 contractor employees who require access to United States Citizenship and Immigration Services (USCIS) facilities

and/or utilize USCIS Information Technology (IT) systems, must be issued and maintain a Personal Identity Verification (PIV) card throughout the period of performance on their contract.

Government-owned contractor- operated facilities are considered USCIS facilities.

After the Office of Security & Integrity, Personnel Security Division has notified the Contracting Officer's Representative that a favorable entry on duty (EOD) determination has been rendered, contractor employees will need to obtain a PIV card.

For new EODs, contractor employees have [*10 business days unless a different number is inserted*] from their EOD date to comply with HSPD-12. For existing EODs, contractor employees have [*10 business days unless a different number of days is inserted*] from the date this clause is incorporated into the contract to comply with HSPD-12.

Contractor employees who do not have a PIV card must schedule an appointment to have one issued. To schedule an appointment:
http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/PIV/default.aspx

Contractors who are unable to access the hyperlink above shall contact the Contracting Officer's Representative (COR) for assistance.

Contractor employees who do not have a PIV card will need to be escorted at all times by a government employee while at a USCIS facility and will not be allowed access to USCIS IT systems.

A contractor employee required to have a PIV card shall:

- Properly display the PIV card above the waist and below the neck with the photo facing out so that it is visible at all times while in a USCIS facility
- Keep their PIV card current
- Properly store the PIV card while not in use to prevent against loss or theft
  http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/SIR/default.aspx

OSI PSD must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and HSPD-12 card, or those of terminated employees to the COR. If an identification card or HSPD-12 card is not available to be returned, a report must be submitted to the COR, referencing the card number, name of individual to whom issued, the last known location and disposition of the card.

SECURITY MANAGEMENT

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

The COR 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 COR determine that the Contractor is not complying with the security requirements of this contract 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.

In the event classified information is inadvertently received by a contractor who does not hold an active security clearance at the Secret level, a Government employee or Contractor with the appropriate security clearance equal to or higher than the classified information received, will take possession of the material and shall safeguard and store the information in accordance with standards set forth in the NISPOM. The inadvertent disclosure will be immediately reported to their supervisor and then to the designated OSI Local Security Officer or OSI Field Security Manager for action as appropriate.

Subpart 4.4—Safeguarding Classified Information Within Industry
4.402 General.
(a) Executive Order 12829, January 6, 1993 (58 FR 3479, January 8, 1993), entitled "National Industrial Security Program" (NISP), establishes a program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. Executive Order 12829 amends Executive Order 10865, February 20, 1960
(25 FR 1583, February 25, 1960), entitled "Safeguarding Classified Information Within Industry," as amended by Executive Order 10909, January 17, 1961 (26 FR 508, January 20, 1961).
(b) The National Industrial Security Program Operating Manual (NISPOM) incorporates the requirements of these Executive orders. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission, and the Director of Central Intelligence, is responsible for issuance and maintenance of this Manual. The following DoD publications implement the program:
(1) National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M).
(2) Industrial Security Regulation (ISR) (DoD 5220.22-R).
(c) Procedures for the protection of information relating to foreign classified contracts awarded to U.S. industry, and instructions for the protection of U.S. information relating to classified contracts awarded to foreign firms, are prescribed in Chapter 10 of the NISPOM.
(d) Part 27—Patents, Data, and Copyrights, contains policy and procedures for safeguarding classified information in patent applications and patents.

4.403 Responsibilities of Contracting Officers.
(a) *Presolicitation phase*. Contracting officers shall review all proposed solicitations to determine whether access to classified information may be required by offerors, or by a contractor during contract performance.
(1) If access to classified information of another agency may be required, the contracting officer shall—
(i) Determine if the agency is covered by the NISP; and
(ii) Follow that agency's procedures for determining the security clearances of firms to be solicited.
(2) If the classified information required is from the contracting officer's agency, the contracting officer shall follow agency procedures.

(b) *Solicitation phase*. Contracting officers shall—
(1) Ensure that the classified acquisition is conducted as required by the NISP or agency procedures, as appropriate; and
(2) Include—
(i) An appropriate Security Requirements clause in the solicitation (see 4.404); and
(ii) As appropriate, in solicitations and contracts when the contract may require access to classified information, a requirement for security safeguards in addition to those provided in the clause (52.204-2, Security Requirements).

(c) *Award phase*. Contracting officers shall inform contractors and subcontractors of the security classifications and requirements assigned to the various documents, materials, tasks, subcontracts, and components of the classified contract as follows:
(1) Agencies covered by the NISP shall use the Contract Security Classification Specification, DD Form 254. The contracting officer, or authorized representative, is the approving official for the form and shall ensure that it is prepared and distributed in accordance with the ISR.
(2) Contracting officers in agencies not covered by the NISP shall follow agency procedures.

4.404 Contract clause.
(a) The contracting officer shall insert the clause at 52.204-2, Security Requirements, in solicitations and contracts when the contract may require access to classified information, unless the conditions specified in paragraph (d) of this section apply.
(b) If a cost contract (see 16.302) for research and development with an educational institution is contemplated, the contracting officer shall use the clause with its Alternate I.
(c) If a construction or architect-engineer contract where employee identification is required for security reasons is contemplated, the contracting officer shall use the clause with its Alternate II. (d) If the contracting agency is not covered by the NISP and has prescribed a clause and alternates that are substantially the same as those at 52.204-2, the contracting officer shall use the agency- prescribed clause as required by agency procedures.

52.204-2 Security Clause Requirements.
As prescribed in 4.404(a), insert the following clause:
Security Requirements (Aug 1996)
(a) This clause applies to the extent that this contract involves access to information classified "Top Secret."
(b) The Contractor shall comply with—
(1) The Security Agreement (DD Form 441), including the *National Industrial Security Program Operating Manual* (DOD 5220.22-M); and
(2) Any revisions to that manual, notice of which has been furnished to the Contractor.
(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.
(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.
(End of clause)

Alternate I (Apr 1984). If a cost contract for research and development with an educational institution is contemplated, add the following paragraphs (e), (f), and (g) to

the basic clause:
(e) If a change in security requirements, as provided in paragraphs (b) and (c), results (1) in a change in the security classification of this contract or any of its elements from an unclassified status or a lower classification to a higher classification, or (2) in more restrictive area controls than previously required, the Contractor shall exert every reasonable effort compatible with the Contractor's established policies to continue the performance of work under the contract in compliance with the change in security classification or requirements. If, despite reasonable efforts, the Contractor determines that the continuation of work under this contract is not practicable because of the change in security classification or requirements, the Contractor shall notify the Contracting Officer in writing. Until resolution of the problem is made by the Contracting Officer, the Contractor shall continue safeguarding all classified material as required by this contract.
(f) After receiving the written notification, the Contracting Officer shall explore the circumstances surrounding the proposed change in security classification or requirements, and shall endeavor to work out a mutually satisfactory method whereby the Contractor can continue performance of the work under this contract.
(g) If, 15 days after receipt by the Contracting Officer of the notification of the Contractor's stated inability to proceed, (1) the application to this contract of the change in security classification or requirements has not been withdrawn, or (2) a mutually satisfactory method for continuing performance of work under this contract has not been agreed upon, the Contractor may request the Contracting Officer to terminate the contract in whole or in part. The Contracting Officer shall terminate the contract in whole or in part, as may be appropriate, and the termination shall be deemed a termination under the terms of the Termination for the Convenience of the Government clause.
Alternate II (Apr 1984). If employee identification is required for security or other reasons in a construction contract or architect-engineer contract, add the following paragraph (e) to the basic clause:
(e) The Contractor shall be responsible for furnishing to each employee and for requiring each employee engaged on the work to display such identification as may be approved and directed by the Contracting Officer. All prescribed identification shall immediately be delivered to the Contracting Officer, for cancellation upon the release of any employee. When required by the Contracting Officer, the Contractor shall obtain and submit fingerprints of all persons employed or to be employed on the project.