ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF PAGES 25

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

1. DATE OF ORDER: 06/01/2017	2. CONTRACT NO. (If any): HSHQDC-14-D-E2051
3. ORDER NO.: HSSCCG-17-J-00045	4. REQUISITION/REFERENCE NO.: TFM170019

5. ISSUING OFFICE (Address correspondence to)
USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

6. SHIP TO:
a. NAME OF CONSIGNEE: Department of Homeland Security
b. STREET ADDRESS: US Citizenship & Immigration Svcs
Office of Information Technology
111 Massachusetts Ave, NW
Suite 5000
c. CITY: Washington | d. STATE: DC | e. ZIP CODE: 20529

7. TO:
a. NAME OF CONTRACTOR: BOOZ ALLEN HAMILTON ENGINEERING SERVICES LLC
b. COMPANY NAME:
c. STREET ADDRESS: 900 ELKRIDGE LANDING RD
d. CITY: LINTHICUM | e. STATE: MD | f. ZIP CODE: 21090

8. TYPE OF ORDER
☐ a. PURCHASE — REFERENCE YOUR: _____
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.

☒ b. DELIVERY
Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA: See Schedule	10. REQUISITIONING OFFICE: USCIS Contracting Office

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
☐ a. SMALL ☒ b. OTHER THAN SMALL ☐ c. DISADVANTAGED ☐ d. WOMEN-OWNED ☐ e. HUBZone
☐ f. SERVICE-DISABLED VETERAN-OWNED ☐ g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM ☐ h. EDWOSB

12. F.O.B. POINT: Destination

13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	16. DISCOUNT TERMS
a. INSPECTION: Destination	b. ACCEPTANCE: Destination			Net 30

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	DUNS Number: 075916762+0000 | Transformation Data Science Services (TDSS) Attachments 1-5 (attached) are incorporated into this task order. Continued ...					

SEE BILLING INSTRUCTIONS ON REVERSE

18. SHIPPING POINT | 19. GROSS SHIPPING WEIGHT | 20. INVOICE NO.

17(h) TOTAL (Cont. pages) ◀ $2,129,457.12

21. MAIL INVOICE TO:
a. NAME: See Invoicing Instructions
b. STREET ADDRESS (or P.O. Box)
c. CITY | d. STATE | e. ZIP CODE

17(i) GRAND TOTAL ◀ $2,129,457.12

22. UNITED STATES OF AMERICA BY (Signature) ▶ Kiley Leahy

23. NAME (Typed): Kiley Leahy
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (Rev. 2/2012)
Prescribed by GSA/FAR 48 CFR 53.213(f)

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
06/01/2017	HSHQDC-14-D-E2051	HSSCCG-17-J-00045

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	The period of performance for this task order is twelve (12) months. Dates will be adjusted based on the issuance of the Notice to Proceed (NTP). No invoicing may occur until after the NTP has been issued. This task order is subject to the Terms and Conditions of the contractor's EAGLE II contract AAP Number: 2017037071 DO/DPAS Rating: NONE Accounting Info: TDSS000 000 EP 20-05-00-000 20-00-0000-00-00-00-00BGE-25-47-00 000000					
0001	TDSS Agile Team	12	MO	177,454.76	2,129,457.12	
	Points of Contact: Larry Simmons, COR Larry.Simmons@uscis.dhs.gov 202-272-9484 Hollie Walsh, CS Hollie.L.Walsh@uscis.dhs.gov 802-872-4649 Kiley Leahy, CO Kiley.M.Leahy@uscis.dhs.gov 802-872-4513 The total amount of award: $2,129,457.12. The obligation for this award is shown in box 17(i).					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) ▷ $2,129,457.12

Transformation Data Science Services (TDSS)
Statement of Work (SOW)

1. OVERVIEW

The Office of Information Technology (OIT) Transformation Delivery Program is seeking to enhance the design of the USCIS Electronic Immigration System (USCIS ELIS). The Transformation Data Science Services (TDSS) contract shall provide services that include statistical modeling, data exploration, data architecture modeling, and other data-related services. TDSS shall support the deployment of a structured lifecycle approach for data collection and analysis, automatic data-driven decision-making, identifying, and analyzing analytics problems of Transformation data.

2. SCOPE

OIT will acquire services to leverage and provide data science services to deploy a structured lifecycle approach for data collection and analysis, automatic data-driven decision-making, identifying, and analyzing analytics problems of Transformation data. The team will apply appropriate analytic techniques and tools to analyze USCIS data, deploy a structured lifecycle approach to statistical modeling, data exploration, data modeling, qualitative and quantitative techniques, and processes to collect and analyze data for data driven decision-making.

The scope of this requirement includes the following:

1. Provide a ten person agile team.
2. Identify key technologies, patterns, and relationships within a dynamic USCIS ELIS technology landscape and be able quickly identify data patterns, trends, and relationships as they emerge and develop.
3. Establish big data reporting and enterprise analytics platform that will enable USCIS to analyze increasingly larger and more complex data sets collected by the USCIS ELIS system.
4. Identify and correct data quality issues and establish a data governance framework to enforce data standards and improve accuracy using integrated internal and external disparate data sources.
5. Develop highly optimized, scalable, automatic case matching logic on microservice/container technology that includes developing machine-learning algorithms to improve how USCIS collects, predicts, and processes information to meet USCIS mission needs.
6. Adopt evolving USCIS design and coding standards in the course of analyzing, modeling and collecting ELIS data.
7. Provide technical methods, techniques, and concepts that are innovative, practical, cost-effective and conducive to agile application development.
8. Collaborate with internal stakeholders.

2.1. **Technical Landscape**

The USCIS technical landscape is shifting from a proprietary commercial-off-the-shelf-based framework to open source. One of USCIS's goals is to use platforms and tools that are familiar to a broad range of developers; this has influenced the selection of open source products and frameworks. All USCIS source code and tests are stored in the agency's Enterprise Github repository, and code is shared between different projects where appropriate. USCIS is also moving towards containerized micro-service architecture.

Team members will be expected to gain a basic understanding of the technical landscape so they can effectively advocate for technology solutons that benefit users.

In addition, ELIS data utilizes an Oracle database. All TDSS agile team members shall work within ELIS's Oracle database to conduct analytics, reporting, and develop DHS Section 508 compliant dashboards.

3. AGILE TEAM REQUIREMENTS

The contractor shall provide one agile team consisting of ten members. One of the team members shall be the Technical Lead and must be a senior data scientist professional (see additional qualifications in Section 5, Key Personnel). Additionally, at least one person on the team must be a certified Scrum Master. The team should include following expertise:

a. Data scientist who works with USCIS ELIS software engineers to collect data needed to form decisions;
b. Modeling specialists who use their machine learning expertise to build predictive models;
c. Platform builders who create data platforms, balancing both engineering and data analysis concerns (current USCIS ELIS data platform is Amazon Web Services (AWS));
d. Polymaths who do all data science activities;
e. User interface designer to produce government approved analytics DHS Section 508 compliant dashboards from the results of Task 2.0 and as reflected in the Final Report (see Task 2.0 below);
f. Technical team leader who leads the team of data scientists and promotes best practices.

4. TASKS

The tasks identified in this section describe the work that will comprise this task order.

Task 1 – Exploratory Statistical Data Analysis

Utilizing ELIS's Oracle database and other required data sources, the contractor shall conduct an exploratory statistical analysis on the data sets for a period of time that is agreed upon by USCIS and the contractor after task order award. The contractor shall use appropriate statistical methods, including but not limited to, building a system for collecting data from multiple sources, inserting instrumentation code to gather statistical data, USCIS consumer habits, and indentifying data issues and bottlenecks.

- Deliverable 1: Exploratory Statistical Data Analysis and Report

Task 2 – Final Statistical Data Analytics

The contractor shall conduct a focused statistical analysis based on the results of Task 1 and input from USCIS ELIS stakeholders. This analysis shall be conducted from the conclusion of Task 1 through the completion of this task order, accumulating in a final report. The requirements under this task include:

- Data merging and cleaning
- Sampling: selecting a subset set of behavior and weigh profiles to approximate normal behavior
- Data shaping, including selecting and creating features: transforming data into a new format and creating new attributes in a feature vector
- Defining sensible metrics: defining metrics that are sensible to USCIS data consumers
- Building predictive models: by applying machine learning, data mining, and statistics
- Defining ground truths: defining class labels and scenarios of anomalies

- Hypothesis testing: setting a null hypothesis and an alternative hypothesis and estimating the confidence level of rejecting the null hypothesis using various statistical methods
- Operationalizing predictive models: integrating predictive models into software products
- Defining actions and triggers: defining automated actions and triggers for different labels of predictions
- Translating insights and models to business values
- Report format shall be DHS Section 508 compliant

    - Deliverable 2: DHS Section 508 compliant Final Statistical Analysis and Report

4.1. Administrative Activities

The contractor shall conduct the following activities:

- The contractor shall collaborate with stakeholders, support contractors and third party vendors.
- The contractor shall manage all contractor resources and supervise all contractor staff in the performance of work on this task order.
- The contractor shall organize, direct and coordinate planning and execution of all task order activities.
- Vehicles for transparency, such as the agency Agile Application Lifecycle Management (ALM) tool, shall be maintained with data so that reports and charts can be generated as needed, and so that tasks and status are available to stakeholders.

5. KEY PERSONNEL

The contractor shall identify one key personnel to be the **technical lead** for this task order. The key personnel will be one of the ten people on the agile team. The proposed key personnel must be employed by the prime contractor, and shall possess the required qualifications, skills and experience, which should be reflected by a Statement of Qualifications provided by the contractor within 5 days after contract award.

Role	EAGLE II Level	Skills / Experience
Technical Lead	II or higher	Must have a minmum of 5 years of experience managing data scientists, data mining, and data analytics teams. Must have familiarity with the Agile process and environments. Must be PMP certified.

6. TRANSITION SUPPORT

Upon completion of performance of this task order, the contractor shall fully support the transition of the work that is turned over to another entity, either government or a successor. The contractor shall assist with transition planning and shall comply with the transition milestones and schedule. To ensure the necessary continuity of services and to maintain the required level of support, USCIS may retain services of the incumbent contractor for some or all of the transition period, as required.

The contractor shall be responsible for the transition of all design activities. As part of the transition, the contractor shall be responsible for:

- Inventory and orderly transfer of all Government Furnished Property (GFP), to include hardware, software, and licenses, Contractor Acquired Government Property.
- Transfer of documentation currently in process
- Transfer of all software code in process
- Exchange of accounts to access software and hosted infrastructure components
- Participation in knowledge transfer activities

Transition planning generally begins 120 days before the transition deadline. If the government provides a transition plan template, the contractor shall complete it as assigned; otherwise, the contractor shall submit a transition plan at the direction of the government. The transition plan shall:

- Document the strategic approach
- Identify equipment, hardware, software, documents and other artifacts that are included in the transition
- Establish milestones and schedules
- Establish activities
- Identify transition risks and risk mitigation
- Define roles and responsibilities
- Define transition approval authorities and lines of communication
- Define appropriate labor mix to perform CI/CD activities
- Define a knowledge transfer approach
- Define a property inventory and transition approach
- Create bi-party or tri-party agreements
- Provide checklists

7. DELIVERABLES

Deliverable Number	Deliverable	PWS Reference	Due
1	Key Personnel Statement of Qualifications	Section 5	Within 5 days after task order award, and any time a replacement is proposed.
2	Post Award Kickoff Meeting – Presentation by contractor, including overview of company, introduction of key personnel, company points of contact for security and project management, an overview of the technical proposal, invoicing and an opportunity for introductions and questions.	N/A	Within 10 business days after task order award
3	Exploratory Statistical Data Analysis	Secton 4,	A date agreed upon by

	and Report	Task 1	Government and contractor at the post award kickoff meeting
4	DHS Section 508 compliant Final Statistical Analysis and Report	Section 4, Task 2	A date agreed upon by Government and contractor at the post award kickoff meeting
5	DHS Section 508 compliant Government approved analytics dashboards from the results of Task 2.0 and as reflected in the Final Report	Section 3	A date agreed upon by Government and contractor at the post award kickoff meeting
6	Transition-Out Plan	Section 6	120 days before task order end date *if requested by the government*

7.1. **Task Order Management Artifacts**

The contractor shall provide status briefings that support task order management, as described below:

As required by the COR, the contractor shall attend meetings with the COR and/or other USCIS stakeholders in order to review work accomplished, work in progress, plans for future work, transition plans and status, and issues pertinent to the performance of work tasks that require USCIS attention.

In the event the government requires additional information related to technical performance, schedule, risks, resources, or any contract-related data, the contractor shall provide this report information in the format requested by the government. Requests for reporting may vary in scope and complexity and may require the contractor to attend OIT meetings to obtain required information, review and research applicable documentation, and extract applicable database information required to assemble the report.

8. TASK ORDER ADMINISTRATION DATA

8.1. Place of Performance

The principal place of performance shall be at the USCIS facilities at 111 Massachusetts Ave. NW, Washington D.C. and 20 Massachusetts Avenue, N.W. The contractor may propose the use of its own facilities for specific, short-term activities. Occasional travel to USCIS offices outside of the Washington, D.C. area may be contemplated.

8.2. Hours of Operation

Normal duty hours for the Government are from 8am to 5pm, Monday through Friday, excluding Federal Government holidays. The contractor shall be available during this time period.

8.3. Government Furnished Property (GFP)

GFP laptops will be issued and used in performing work on this contract. No personal or company owned storage devices, (thumb drives, DVDs, or CDs) will be used with the GFP. A webinar account, such as AT&T Connect, will be provided to the contractor to facilitate virtual demos and other meetings with stakeholders at various physical locations. Mobile devices may be provided as identified by the COR or Government Project Manager.

Equipment / Government Property	Date / Event Indicate when the GFP will be furnished	Date / Event Indicate when the GFP will be returned	Unit	Unit Acquisition Cost	Quantity	Manufacture & Model Number
Laptop	After EOD	Upon Departure	EA	$2,758	10	Standard USCIS approved manufacturer
Smartphone	After EOD	Upon Departure	EA	TBD	TBD	Standard USCIS approved manufacturer

The contractor is responsible for all costs related to making the property available for use, such as payment of all transportation, installation or rehabilitation costs. The Contractor will be responsible for receipt, stewardship, and custody of the listed GFP until formally relieved of responsibility in accordance with FAR 52.245-1 Government Property and FAR 52.245-9 Use and Charges. The property may not be used for any non-task order purpose. The Contractor bears full responsibility for any and all loss of this property, whether accidental or purposeful, at full replacement value.

9. PERFORMANCE CRITERIA

The team will be evaluated on a monthly basis, or as required by the government, and the evaluation will be discussed with the contractor. The purpose of the discussions is to enhance performance. In addition, in the aggregate, the discussions will be used partially as a basis for past performance reporting.

It is anticipated that the contractor will be evaluated based on the team's ability to:

- Provide clear, concise analysis,
- Present delivreables with substance,
- Implement automatic data-driven decision-making vehicles quickly,
- Identify and analyze analytics problems of Transformation data.

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 sensitive but unclassified information, and that the Contractor will adhere to the following.

SUITABILITY DETERMINATION

USCIS shall have and exercise full control over granting, denying, withholding or terminating access 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 suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by USCIS, at any time during the term of the contract. No Contractor employee shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability 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 shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the Position Designation Determination (PDD) for Contractor Personnel. 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.

To the extent the Position Designation Determination form reveals that the Contractor will not require access to sensitive but unclassified information or access to USCIS IT systems, OSI PSD may determine that preliminary security screening and or a complete background investigation is not required for performance on this contract.

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

2. FD Form 258, "Fingerprint Card" **(2 copies)**

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

4. Position Designation Determination for Contract Personnel Form

5. Foreign National Relatives or Associates Statement

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

7. ER-856, "Contract Employee Code Sheet"

EMPLOYMENT ELIGIBILITY

Be advised that unless an applicant requiring access to sensitive but unclassified 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.

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

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, 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 Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **USCIS Office Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)

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.

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 Corporate 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.

The Contractor shall be responsible for all damage or injuries resulting from the acts or omissions of their employees and/or any subcontractor(s) and their employees to include financial responsibility.

SECURITY PROGRAM BACKGROUND

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

- Public Law 107-296, Homeland Security Act of 2002.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Executive Order 12829, *National Industrial Security Program*, January 6, 1993.
- Executive Order 12958, *Classified National Security Information*, as amended.
- Executive Order 12968, *Access to Classified Information*, August 2, 1995.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001
- National Industrial Security Program Operating Manual (NISPOM), February 2001.
- DHS *Sensitive Systems Policy Publication 4300A* v2.1, July 26, 2004

- DHS *National Security Systems Policy Publication 4300B* v2.1, July 26, 2004
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal*
- *Information Resources*.
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (U), July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security*
- *Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.
- Title 36 Code of Federal Regulations 1236, Management of Vital Records, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

GENERAL

Due to the sensitive nature of USCIS information, the contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The contractor's security program shall adhere to the requirements set forth in the DHS Management Directive 4300 IT Systems Security Pub Volume 1 Part A and DHS Management Directive 4300 IT Systems Security Pub Volume I Part B. This shall include conformance with the DHS Sensitive Systems Handbook, DHS Management Directive 11042 Safeguarding Sensitive but Unclassified (For Official Use Only) Information and other DHS or USCIS guidelines and directives regarding information security requirements. The contractor shall establish a working relationship with the USCIS IT Security Office, headed by the Information Systems Security Program Manager (ISSM).

IT SYSTEMS SECURITY

In accordance with DHS Management Directive 4300.1 "Information Technology Systems Security", USCIS Contractors shall ensure that all employees with access to USCIS IT Systems are in compliance with the requirement of this Management Directive. Specifically, all contractor

employees with access to USCIS IT Systems meet the requirement for successfully completing the annual "Computer Security Awareness Training (CSAT)." All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter.
CSAT can be accessed at the following: http://otcd.uscis.dhs.gov/EDvantage.Default.asp or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

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

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

and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation). As appropriate the Contractor shall be granted access to the USCIS TAF and Risk Management System (RMS) tools to support C&A and its annual assessment requirements. Annual assessment activities shall include completion of the NIST 800-26 Self-Assessment in TAF, annual review of user accounts, and annual review of the FIPS categorization. C&A status shall be reviewed for each incremental system update and a new full C&A process completed when a major system revision is anticipated.

SECURITY ASSURANCES

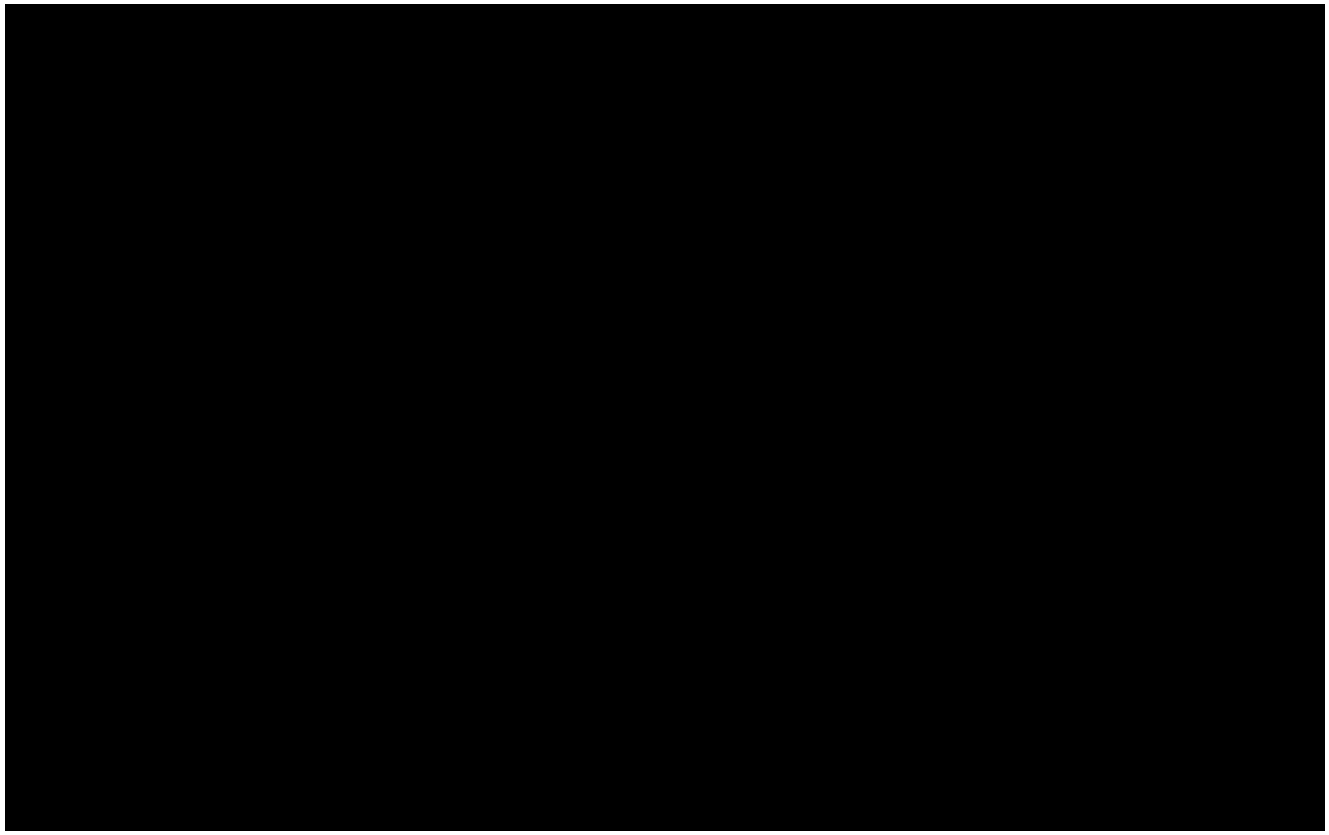
DHS Management Directives 4300 requires compliance with standards set forth by NIST, for evaluating computer systems used for processing SBU information. The Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are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

- *User Identification and Authentication (I&A)* – I&A is the process of telling a system the identity of a subject (for example, a user) (*I*) and providing that the subject is who it claims to be (*A*). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All USCIS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the USCIS standard system in use at the time of a systems development.
- *Discretionary Access Control (DAC)* – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- *Object Reuse* – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- *Audit* – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the USCIS IT Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.
- *Banner Pages* – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

DATA SECURITY

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

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



[redacted]

[redacted]

Department of Homeland Security
DHS Office of Accessible Systems and Technology (OAST)

Accessibility Requirements (Section 508)

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 (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

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

Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.25 Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this work statement.

36 CFR 1194.26 Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

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 COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

Section C—Task Order Clauses

Federal Acquisition Regulation (FAR) clauses incorporated by reference

52.209-10	**Prohibition on Contracting With Inverted Domestic Corporations**	(Nov 2015)
52.227-17	**Rights in Data—Special Works**	(DEC 2007)
52.217-8	**Option to Extend Services** fill-in: **30 days before the task order expires**	(Nov 1999)
52.232-39	**Unenforceability of Unauthorized Obligations**	(Jun 2013)
52.237-3	**Continuity of Services**	(Jan 1991)

Federal Acquisition Regulation (FAR) clauses incorporated in full text

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.

52.203-99 **Prohibition On Contracting With Entities That Require Certain Internal Confidentiality Agreements (DEVIATION)** (Jul 2016)

(a) The contractor shall not require its employees or subcontractors seeking to report fraud, waste, or abuse to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the execution of a government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

(b) The contractor shall notify current employees and subcontractors that prohibitions and restrictions of any internal confidentiality agreements covered by this clause, to the extent that such prohibitions and restrictions are inconsistent with the prohibitions of this clause, are no longer in effect.

(c) The prohibition in paragraph (a) of this clause does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(d) In accordance with Section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015, (Pub. L. 113-235) use of funds appropriated (or otherwise made available) under that or any other Act may be

prohibited, if the government determines that the contractor is not in compliance with the provisions of this clause.

(e) The contractor shall include the substance of this clause, including this paragraph (f), in subcontracts under such contracts.

(f) The government may seek any available remedies in the event the contractor fails to comply with the provisions of this clause.

Other Task Order Requirements

C-1. ADDITIONAL INVOICING INSTRUCTIONS

(a) In accordance with FAR Part 32.905, all invoices submitted to USCIS for payment shall include the following:

(1) Name and address of the contractor.
(2) Invoice date and invoice number.
(3) Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number).
(4) Description, quantity, unit of measure, period of performance, unit price, and extended price of supplies delivered or services performed.
(5) Shipping and payment terms.
(6) Name and address of contractor official to whom payment is to be sent.
(7) Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.
(8) Taxpayer Identification Number (TIN).

(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 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
(802) 288-7600

C-2. 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 is encouraged to enroll at www.cpars.gov so it can participate in this process.

C-3. HSAR CLAUSES INCORPORATED

The following HSAR clauses of the parent EAGLE II Contract apply:

Clause	EAGLE II Section
HSAR clause 3052.204-71	I.4.2
Special Clause – Safeguarding of Sensitive Information (MAR 2015)	H.40
Special Clause – Information Technology Security and Privacy Training (MAR 2015)	H.41

C-4. POSTING OF ORDER IN FOIA READING ROOM

(a) The government intends to post the order resulting from this notice 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.

C-5. KEY PERSONNEL

For the purposes of the contract clause at HSAR 3052.215-70, Key Personnel or Facilities, the Key Personnel are listed in Section 5 in the Statement of Work (SOW). All personnel submitted by a contractor to fill a key person billet shall meet required standards per Section 5 of the SOW.

C-6. NOTICE TO PROCEED (NTP)

(a) Performance of the work requires unescorted access to government facilities or automated systems, and/or access to sensitive but unclassified information. The Attachment titled Security Requirements applies.

(b) The contractor is responsible for submitting packages from employees who will receive favorable entry-on-duty (EOD) decisions and suitability determinations, and for submitting them in a timely manner. A government decision not to grant a favorable EOD decision or suitability determination, or to later withdraw or terminate such decision or termination, shall not excuse the contractor from performance of obligations under this task order.

(c) The contractor may submit background investigation packages immediately following task order award.

(d) This task order does not provide for direct payment to the contractor for EOD efforts. Work for which direct payment is not provided is a subsidiary obligation of the contractor.

(e) The government intends for full performance to begin **60 days** after task order award (allowing 60 days for the EOD period). The contracting officer will issue an NTP at least one day before full performance is to begin.

C-7. CONSENT TO SUBCONTRACT

For the purposes of the contract clause at FAR 52.244-2, Subcontracts, the fill-in for paragraph (d) is "ALL."

C-8. EXPECTATION OF CONTRACTOR PERSONNEL

The government expects competent, productive, qualified IT professionals to be assigned to the Agile team. The Contracting Officer may, by written notice to the contractor, require the contractor to remove any employee that is not found to be competent, productive, or qualified IT professional.

C-9. 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 contract 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.