REQUEST FOR Quote (RFQ)
in support of:

Department of Homeland Security (DHS)
Customs and Border Protection (CBP)
Office of Information & Technology (OIT)
Targeting and Analysis Systems Program Directorate (TASPD)

(1)Information Technology (IT) Operations and Maintenance (O&M), Upgrades, Updates, Modifications and Enhancements Services (IT O&M) Solicitation# 70B04C20Q00000131

(2)Business Intelligence Support Services (BISS) Solicitation #70B04C20Q0000018~~1~~

Issued to:
All contractors under the General Services Administration (GSA) Alliant 2 Government Wide Acquisition Contract (GWAC)

Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
DHS/CBP /OIT/TASPD

A0021~~1~~

Date: August 15~~4~~~~3~~, 2020

B.1 GENERAL

The work shall be performed in accordance with all Sections of this solicitation and the contractor's Basic Contract, under which the resulting TO will be placed.

B.2 CONTRACT ACCESS FEE (CAF)

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a CAF. In accordance with the Alliant 2 base contract, the CAF shall be 0.75 percent of the total TO value with a cap of $1500,000 per year per order (when order is in excess of $13.3M per order year). This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO Award (TOA).

B.3 ORDER TYPES

The contractor shall perform the effort required by this RFQ on a Time-and-Materials basis with contractor-proposed CLIN structure. ~~However, Offerors may propose firm-fixed-price, fixed price level-of-effort, or labor hour for any CLIN(s) and provide an explanation for the type chosen.~~

B.4 SERVICES AND PRICES/COSTS

Long-distance travel is defined as travel over 50 miles from duty station as defined in Section F.2. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CAF	Contract Access Fee
CLIN	Contract Line Item Number
NTE	Not-to-Exceed
ODC	Other Direct Cost

B.4.1 Two (2) Task Orders (Transition and Requirements Execution) will be issued for each of the two (2) requirements (O&M and BISS)

TRANSITION TASK ORDER

~~)~~

CLIN	Description	T&M	LOE	NTE
0001 (Vendor to propose)	Transition	$	# hours	$

CAF

CLIN	Description	Total Ceiling Price
0002	CAF	$ 15~~0~~0,000.00

TOTAL CEILING TRANSITON TO CLINs: $_____

This page is intentionally left blank

REQUIREMENTS EXECUTION TASK ORDER

BASE PERIOD:

Proposed CLIN(s) should align with technical solution
LABOR CLIN(s)

CLIN	Description	T&M	LOE	~~Cost~~Price
0001 (Vendor to propose)	Labor	$	# hours	$

OPTIONAL SURGE CLIN

CLIN	Description	~~NTE~~Price
0002	Surge	~~NTE~~ 50% of CLIN 0001

ODC CLIN

CLIN	Description	Total Ceiling Price
0003	ODC	$ 100,000.00

CAF

CLIN	Description	Total Ceiling Price
0004	CAF	$ 1~~0~~50,000.00

TOTAL CEILING BASE PERIOD CLINs: $_____

B.4.2 FIRST OPTION PERIOD

LABOR CLIN(s)

CLIN	Description	T&M	LOE	~~Cost~~Price
1001 (Vendor to propose)	Labor	$	# hours	$

OPTIONAL SURGE CLIN

CLIN	Description	~~NTE~~Price
1002	Surge	~~NTE~~ 50% of proposed labor ceiling

ODC CLIN

CLIN	Description	Total Ceiling Price
1003	ODC	$ 100,000.00

CAF

CLIN	Description	Total Ceiling Price
1004	CAF	$ 150~~0~~,000.00

TOTAL CEILING FIRST OPTION PERIOD CLINs: $_____

B.4.3 SECOND OPTION PERIOD

LABOR CLIN(s)

CLIN	Description	T&M	LOE	~~Cost~~Price
2001 (Vendor to propose)	Labor	$	# hours	$

OPTIONAL SURGE CLIN

CLIN	Description	~~NTE~~Price
2002	Surge	~~NTE~~ 50% of proposed labor ceiling

ODC CLIN

CLIN	Description	Total Ceiling Price
2003	ODC	$ 100,000.00

CAF

CLIN	Description	Total Ceiling Price
2004	CAF	$ 150~~0~~,000.00

TOTAL CEILING SECOND OPTION PERIOD CLINs: $_____

B.4.4 THIRD OPTION PERIOD

LABOR CLIN(s)

CLIN	Description	T&M	LOE	~~Cost~~Price
3001 (Vendor to propose)	Labor	$	# hours	$

OPTIONAL SURGE CLIN

CLIN	Description	~~NTE~~Price
3002	Surge	~~NTE~~ 50% of proposed labor ceiling

ODC CLIN

CLIN	Description	Total Ceiling Price
3003	ODC	$ 100,000.00

CAF

CLIN	Description	Total Ceiling Price
3004	CAF	$ 150~~0~~,000.00

TOTAL CEILING THIRD OPTION PERIOD CLINs: $_____

B.4.5 FOURTH OPTION PERIOD

LABOR CLIN(s)

CLIN	Description	T&M	LOE	~~Cost~~Price
4001 (Vendor to propose)	Labor	$	# hours	$

OPTIONAL SURGE CLIN

CLIN	Description	~~NTE~~Price
4002	Surge	~~NTE~~ 50% of proposed labor ceiling

ODC CLIN

CLIN	Description	Total Ceiling Price
4003	ODC	$ 100,000.00

CAF

CLIN	Description	Total Ceiling Price
4004	CAF	$ 150~~0~~,000.00

TOTAL CEILING FOURTH OPTION PERIOD CLINs: $_____

GRAND TOTAL CEILING ALL CLINs: $_____

B.4.6 Option to Extend Services (OES) - 52.217-8

LABOR CLIN(s)

CLIN	Description	T&M	LOE	~~Cost~~Price
5001 (Vendor to propose)	Labor	$	# hours	$

OPTIONAL SURGE CLIN

CLIN	Description	~~NTE~~Price
5002	Surge	~~NTE~~ 50% of proposed labor ceiling

ODC CLIN

CLIN	Description	Total Ceiling Price
5003	ODC	$ 50,000.00

CAF

CLIN	Description	Total Ceiling Price
5004	CAF	$ 75~~0~~,000.00

TOTAL CEILING OES PERIOD CLINs: $_____

GRAND TOTAL CEILING ALL CLINs: $_____

B.5 SECTION B TABLES

B.5.1 INDIRECT/MATERIAL HANDLING RATE

Long-Distance Travel, Tools, and ODC costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices, provided that the basic contract does not prohibit the application of indirect rate(s) on these costs.

a. If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
b. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

B.5.2 DIRECT LABOR RATES

Labor categories proposed shall be mapped to existing Alliant 2 labor categories.

B.6 RESERVED

B.7 RESERVED

C.1 REQUIREMENTS

PERFORMANCE WORK STATEMENT (PWS)

Department of Homeland Security (DHS) - Customs and Border Protection (CBP) - Office of information and Technology (OIT) - Targeting and Analysis Systems Program Directorate (TASPD)

Information Technology (IT) Operations and Maintenance (O&M), Upgrades, Updates, Modifications and Enhancements Support Services (IT O&M Services)

1.0 BACKGROUND

Customs and Border Protection (CBP) is a component of the Department of Homeland Security (DHS). The priority mission of CBP is to prevent terrorists and terrorist weapons from entering the United States. This important mission calls for improved security at America's borders and ports of entry as well as for extending the zone of security beyond physical borders so that American borders are the last line of defense, not the first. CBP is also responsible for apprehending individuals attempting to enter the United States illegally, stemming the flow of illegal drugs and other contraband; protecting our agricultural and economic interests from harmful pests and diseases; protecting American businesses from theft of their intellectual property; and regulating and facilitating international trade, collecting import duties, and enforcing U.S. trade laws.

The Office of Information and Technology (OIT) is the information technology component of CBP. OIT's responsibilities are vast-ranging from designing, delivering and maintaining technology based capabilities to enterprise architecture and governance. OIT also provides solutions that support CBP inspection and enforcement activities to help CBP officers, agents, and analysts protect our borders and safeguard America. OIT is responsible for enhancing, administering, and maintaining intelligence and targeting systems and related systems that help secure the supply chain and support CBP's layered defense strategy for international cargo and passengers.

The Targeting and Analysis Systems Program Directorate (TASPD) is responsible for developing and maintaining analytical and targeting software systems. The main system housed within TASPD is the Automated Targeting System (ATS). The ATS is a web-based enforcement and decision support tool that is the cornerstone for all CBP's targeting efforts. The ATS incorporates intelligence information and technologies to target suspect inbound and outbound shipments for examinations and passengers for inspection. In this way, ATS allows CBP officers, agents, and analysts to focus their efforts on cargo shipments and passengers that most warrant further attention. The ATS standardizes names, phone numbers, addresses, ship names, and similar data so these data elements can easily be associated with other business data to form a complete picture of a passenger, import, or export in context with previous behavior of the parties involved.

Every person and shipment processed through ATS is subjected to a real-time evaluation utilizing rules and analytical models. The ATS receives much of its data in real time from various CBP systems, such as the Automated Commercial System (ACS), the Automated Export System (AES), TECS, hundreds of other input data feeds, and dozens of output data feeds. The ATS data consists of electronically filed bills, entries, and entry summaries for cargo imports; shippers' export declarations and transportation bookings and bills for cargo exports; manifests for arriving and departing passengers; airline reservation data; nonimmigrant entry records; and records from secondary referrals, incident logs, suspect and violator indices, and seizures.

The purpose of this Performance Work Statement (PWS) is to procure the full range of operations and maintenance support for the CBP TASPD suite of computer and software applications. Additionally, this PWS reflects migration to a cloud environment and a move to a DevOps strategy and includes upgrades, updates, modifications and enhancements of existing applications in response to evolving technologies,

threats, and mission requirements in direct support of the DHS and CBP in their mission critical initiatives to protect the borders (air, land, and sea) of the United States.

This work will be performed on a time and materials basis.

2.0 SCOPE

Operations & Maintenance.

The contractor shall provide any and all operations and maintenance (O&M) solutions, processes, and procedures necessary to sustain the suite of TASPD computer and software applications within the DHS enterprise at the highest levels of security, service and availability consistent with cost, schedule, and performance objectives. This full range of O&M solutions will ensure TASPD computer and software applications operate efficiently, effectively and securely, and are available to support CBP mission requirements.

This O&M support will emphasize performance monitoring to identify and resolve performance risks before they impact mission performance while responding to customer identified performance deficiencies and/or outages.

Upgrades, Updates, Modifications and Enhancements.

The contractor shall provide any and all TASPD computer and software application upgrades, updates, modifications or enhancements with a focus on moving towards a DevOps approach to enable development and operations teams to collaborate and deliver high quality software to end customers continuously, to generate code with fewer errors and do so faster, which speeds time to deployment, and increases reliability and stability on the production side of the house. This work includes but is not limited to ensuring application compatibility with and deploying new operating system versions, new application software versions, and new code library versions. Performance and documentation shall follow the Agile methodology according to the tailored DHS Systems Engineering Life Cycle Procedures (SELC).

Frequent updates and features to the existing suite of applications are necessary to keep up with evolving risks and threats. The contractor shall support ongoing collaboration with the Government lead on each project, as well as product owners and the user community, to ensure accurate prioritization of new requirements and timely implementation of those requirements. The contractor shall provide all services necessary to migrate to and operate the infrastructure, applications and services to the cloud.

2.1. APPLICABLE DOCUMENTS

- DHS Directive 102-01
- CBP Security Handbook
- DHS/CBP Program Lifecycle Process Guide
- DHS MD 8110 – Intelligence Integration and Management
- CBP Agile Framework
- CBP SELC process
- Office on Accessible Systems and Technology (OAST) Compliance
- DHS Information Security Policy, MD4300.1, Information Technology Systems Security
- DHS MD 4300A, DHS Sensitive Systems Policy and Handbook, CBP Information Systems
- Security Policies and Procedures Handbook HB-1400-05
- All applicable National Institute of Standards and Technology (NIST) Special Publications (800 Series)
- DHS Data Management Policy MD 103-01
- Addendum A - Security and IT Compliance Requirements
- Addendum B – General Environment and Key Technical Features

3.0 TECHNICAL ENVIRONMENT

Current Environment:

OIT performs system activities in a technical environment supported by a broad set of custom architectural components and/or commercial off-the-shelf (COTS) packages. Addendum B lists software and hardware components for general infrastructure and development and production environments. TASPD will ensure adequate computing capacity for our current and projected needs to include development, testing and production. This includes associated networking, storage and offsite infrastructure. The Contractor shall ensure that all solutions scale and shall provide guidance to the Government on additional infrastructure needs as the applications and user base continue to expand.

For informational purposes in regards to scope, size, and complexity, the largest transactional database described in the PWS is more than 400 TB and 30-40 billion transactions are performed against the database on a daily basis. The largest Hadoop file systems described in the PWS include over 4 PB of capacity. The Elastic index system includes a capacity over 800 TB, including over 40 billion documents indexed from over 40 data sources.

Future Environment:

Produced by the Office of Management & Budget (OMB), the February 2011 Federal Cloud Strategy outlines the impetus and benefits of migrating to cloud services, including acceleration of data center consolidation and better utilization of existing infrastructure assets. Based on the December 2010 25 Point Plan to reform Federal Information Technology Management, also from OMB, each Federal agency CIO has been directed to leverage this strategy to begin planning the migration of their IT services to cloud solutions. TASPD is in the process of readying workloads and applications to migrate to the cloud. The contractor must support the target operating model which is to migrate all hardware infrastructure and applications in this document to a cloud solution and operate in the cloud going forward.

The Government will provide the necessary software and licenses required for system maintenance, as well as all related and available documentation on TASPD computer software applications to the Contractor as required.

TASPD is in the final stages of refactoring and modernizing Legacy TASPD ATS applications, some of which use Microsoft. NET, into JAVA technologies, and migrating the functionality into more streamlined and unified applications which conform to the CBP Common Framework. Additionally, while the above and below technologies are currently being used, those technologies that are being moved away from are labeled as “Divest”.

3.1 TASPD Specific Systems

The Automated Targeting System (ATS) currently consists of four subsystems that provide selectivity and targeting capability to support CBP inspection and enforcement activities:

- ATS-Cargo (ATS-C)
- ATS-Passenger (ATS-P)
- Entitlement

The modules of the ATS span across and are supported by the various branches within TASPD; Cargo Targeting branch, Passenger Targeting branch, Architecture and Engineering branch, National Security Systems branch, and the Program Control branch.

TASPD developed and continues to maintain multiple systems and services, including but not limited to:

- Automated Targeting System (ATS) and ATS Subsystems
    - Automated Targeting System-Cargo (ATS-C)
        - National Initiative for Illicit Trade Enforcement (NIITE) is a Data Feed off ATS-C
        - ATS Import Cargo
        - ATS Outbound Cargo
        - ATS-International (ATS-I)
        - ATS-U.S. Postal Service (ATS-USPS)
        - Cargo Enforcement Reporting and Tracking System (CERTS)
            - Import Exam Mobile
        - Importer Security Filing (10+2)
        - Trend Analysis and Analytical Selectivity Program (TAP) 2000
        - Advanced Cargo Air Screening (ACAS)
        - Automatic Identification System (AIS)
        - Vessel Management System (VMS)
        - Cargo Integration Services (CIS)
        - Vessel Risk/Vessel Risk Tracker/Vessel Automation Forms
    - Automated Targeting System-Passenger (ATS-P)
        - Automated Targeting System-Land (ATS-L)
        - Automated Targeting System-Unified Passenger (UPAX) – Targeting Components
            - Traveler Hotlists, including General Aviation and Coast Guard
            - Visa and Visa Waiver Program Hotlists
            - Electronic Visa Update System (EVUS) Hotlist
            - Pre Adjudicated Thread Recognition and Intelligence Operations Team (PATRIOT)
            - Document Validation
            - Visa Overstay
            - Global Enrollment System (GES)
            - Refugee Applicants
            - Trusted Worker eBadge
            - Employee and Applicant Suitability and Eligibility
            - On Demand Batch Query Capabilities
            - System to System Interfaces to other CBP and DHS Systems in support of vetting
        - Automated Targeting System-Global (ATS-G)
        - User Defined Rules – Next Generation (UDR-NG)
        - Data Loaders
        - Advanced Search
        - Unified Person (Person Centric Model)
    - Entitlement
        - Convergence
        - Enhancements
    - Data sharing to dozens of OGAs
- Customs-Trade Partnership Against Terrorism (C-TPAT) Infrastructure

- Analytical Framework for Intelligence (AFI)
- Big Data Services (BDS)
- Enterprise Management Information System- Enterprise Data Warehouse (EMIS-EDW)
- Enterprise Reporting System (ERS)
- Port Radiation, Inspection, Detection and Evaluation (PRIDE)
    - Secure Freight Initiative (SFI)
    - Container Security Initiative-Remote Targeting (CSI-RT)
- New ACE (NACE)
    - ITDS
        - Document Image System (DIS)
        - Inter-operability Web Services (IWS)
        - Participating Government Agencies (PGA) Message Set (Data sharing to 47 PGAs)
    - Cargo Release
    - AES
- Traveler Verification System (TVS)
- Global Travel Assessment System (GTAS)
- Common Framework

New capability typically includes work such as: integration of data sources, refreshing the system based upon current threats and new risk factors including but not limited to database content updates, software code and configuration changes, at a minimum monthly to quarterly updates to the targeting systems and short turnaround updates to the system in response to a threat. Application changes include but are not limited to integration of major new workflows and features into existing applications, support for new user groups with tailored workflows, new targeting capabilities using new or expanded data sources, technology refresh/updates to conform to the CBP Common Framework, enhancements to existing functionality, changes to address Production defects, as well as critical changes to be applied as a result of a new threat or risk. Urgent changes need to be implemented in as little as a few hours to one day. Many teams which could be impacted by a high number of ongoing changes maintain an open Change Request on a weekly basis to account for both planned and urgent/unplanned changes.

3.1.1 ATS Cargo (ATS-C)

ATS-C is the outbound/inbound cargo targeting module of ATS that assists in identifying exports and imports which pose a high risk for examination.

ATS-C uses the Electronic Export information (EEI) data that exporters file electronically with CBP's Automated Export System (AES). The EEI data extracted from AES is sorted and compared to a set of rules and evaluated in a comprehensive fashion. This information assists CBP officers with targeting and/or identifying exports with potential aviation safety and security risks, such as hazardous materials and Federal Aviation Administration (FAA) violations. In addition, ATS-C identifies the risk of specific exported cargo for such export violations as smuggled currency, illegal narcotics, stolen vehicles or other contraband.

ATS-C provides CBP Officers and Advanced Targeting Units (ATUs) with a more efficient and consistent method for targeting high risk inbound cargo for examination. ATS-C helps to identify and select import cargo shipments that appear to have a higher likelihood of being associated with terrorism or possibly containing implements of terrorism, narcotics or other contraband in the sea, air (including express mail), rail and truck modes. ATS-C uses numerous rules, models and weight sets to analyze information from manifest, importer security filing, and entry data, to prioritize shipments for review and to generate recommended targets by scoring each shipment. In certain cases, ATS-C automatically places shipments on hold when they score above a specified risk threshold. Through the ATS-C web interface CBP personnel can create ad hoc queries on

cargo data, which allows for them to conduct further targeting using large sets of data. ATS-C is the foremost support tool for targeting inbound and outbound cargo at all major Ports of Entry (POE) in the United States. Vessel Risk is the primary application supporting CBP maritime domain awareness by integrating cargo and vessel crew targeting information with vessel inspection, documentation artifacts, and CBP management.

ATS-C inbound provides distributed data, distributed processing, and establishes and maintains historical reference data. ATS-C receives import bill of lading and entry data for all transportation modes, maintains trade entity data, and applies risk scoring algorithms to inbound shipments. Import Cargo provides cargo targeting capabilities using BDS to query, visualize, and analyze information to quickly identify import cargo threats and mitigate risks. ATS-C allows the end-user to capture examination, provides connectivity to TECS, and supports the Container Security Initiative (CSI) decision process. Cargo Integration Services (CIS) integrates components of Import Cargo and Exam Findings enabling cargo targeting services (Hold Manager, Exam Service, Importer Security Filing).

ATS-C provides the following features:

- Applies operationally developed business rules to identify import/export shipments that may have elevated risk
- Displays complex data and results in a modern web application interface
- Allows ad-hoc data queries for import cargo transactions
- Integrates with CBP cargo control systems and other transactional systems to ingest data and provide risk results
- Detailed permission mechanism for granular authorization and access control
- Automated bi-directional messaging to the trade leveraging Customs specific and trade data specifications
- Auditing and search capabilities
- Automated Reporting

3.1.2 ATS-Passenger (ATS-P) – Targeting Components

ATS-P is a web-based enforcement and decision support tool used to collect, analyze, and disseminate information for the identification of potential terrorists, transnational criminals and, in some cases, other persons who pose a higher risk of violating U.S. law. ATS-P capabilities are used at ports of entry to augment the CBP officer's decision-making about whether a passenger or crew member should receive additional screening.

ATS-P is also used within CBP by Ports of Entry, the National Targeting Center (NTC), Border Patrol agents, CBP headquarters intelligence analysts, and within DHS by DHS agents, analysts, and officers in the Office of Intelligence and Analysis (I&A), Immigration and Customs Enforcement (ICE), U.S. Coast Guard (USCG), and the Transportation Security Administration (TSA). ATS-P provides a hierarchical system that allows DHS personnel to focus efforts on potentially high-risk passengers, Visa Waiver Program / Visa holders and applicants, Electronic Visa Update System (EVUS) applicants, Trusted Traveler applicants, Trusted Worker eBadge applicants, or Admissibility Review Office (ARO) applicants by eliminating labor-intensive manual reviews of information or interviews with every traveler or applicant. Additionally, the ATS-P Targeting capabilities include CBP Employee and Applicant Suitability and Eligibility (EASE) checks. The assessment process is based on a set of uniform and user-defined rules based on specific operational, tactical, intelligence, or local enforcement efforts. ATS-P leverages a suite of COTS and custom developed algorithms to refine targeting and rule engine capabilities, which are evaluated and updated with the product owners and Subject Matter Experts on an ongoing basis to ensure a high level of accuracy and efficiency.

Additionally, ATS-P is used to vet arrival and departure information received from the Arrival and Departure Information System (ADIS) to identify potential visa overstay candidates based on supporting data available in ATS, i.e., border crossing information, I-94, and the Student and Exchange Visitor Information System (SEVIS). In addition to identifying the list of potential overstay candidates, ATS also develops priorities based

on associated risk patterns or possible matches to derogatory records. This prioritized list of overstay candidates is then passed on to LeadTRAC, case management system for ICE to generate case leads.

ATS-P's targeting algorithm is also integrated with other CBP and DHS systems to enhance the ability to identify high risk individuals and support other targeting and vetting programs across DHS.

In addition to the above, ATS-P permits specifically authorized DHS users to access Passenger Name Records (PNR) obtained from airlines or their travel reservation systems through the Airline Reservation Monitoring System (ResMon). ResMon interfaces with the airline reservation systems, allowing the airline reservation system to push PNR to CBP or, for certain carriers, allowing CBP to pull PNR based on a set schedule. ResMon also allows authorized CBP personnel to pull data in certain circumstances on an ad hoc basis, with supervisory approval, to ensure CBP has received the latest available information on specific high-risk travelers or flights.

The Automated Targeting System - Global (ATS-G) is a turnkey travel screening and analysis system for enhancing global security. It was developed by CBP to provide foreign partner government entities with a state-of-the-art targeting, analysis, and case management suite. ATS-G allows users to assess the risk of air and maritime travelers through real-time processing of user-defined rules and watch lists. Additional risk assessment tools include a robust set of querying capabilities, case management system, reporting functionality, data visualization, auditing capabilities, and system checks. It also includes an advanced set of administration tools for provisioning access to sensitive information to a targeting center.

3.1.3 Entitlement

The Entitlement subsystem of ATS is a group of CBP web applications and services responsible for authenticating, authorizing and maintaining data on users of ATS web applications, including the ATS family of subsystems.

Entitlement is scheduled to be replaced by the Oracle Identity Management Suite of products. There are two main parts to the Entitlement System:

Administration Interface

The Administration User Interface (UI) provides a system of web pages to add application users, remove application users, edit existing users, grant and revoke application entitlements, and view user audit information. The UI uses transport layer security (TLS) to secure communication to and from the end user. The Administration Interface ensures users have the appropriate application authorizations by sending messages directly to client application user data stores. Once the user has been granted the appropriate authority, the user is entitled to login to their respective system by means of the Entitlement authentication and authorization gateway services.

Entitlement Authentication and Authorization Gateway Services

The Entitlement Gateways are a system of intranet web services, secured using TLS, and used by client applications to validate user credentials, audit user activity, and to provide pertinent user information. The Entitlement Authentication Gateways provide a shared and universal means to authenticate users and track both valid and invalid logon attempts to client systems.

ATS users must have current security clearances (i.e., successfully adjudicated full field background investigations or BIs), be authenticated (i.e., have a validated business need), and have passed the TECS training to logon to

ATS. Once a BI is in place, a new user can obtain access to ATS only by receiving their supervisor's authorization, filling out and submitting appropriate CBP/ATS forms; then a user will receive only the lowest level privilege or privileges necessary to do his or her job.

Entitlement includes the ATS Access Processing System (APS) which serves as the automated system to track access requests and supervisor approvals within Entitlement supported roles. Entitlement enforces

role based access (RBAC) on the ATS systems and other CBP systems. Production enhancements to Entitlement includes improved navigation in the Administrator UI supporting individual and batch processing of entitlement requests.

Entitlement pulls a user's information from CBP Active Directory and CBP WebTele to populate user information fields such as USER ID (Hash ID), First Name, Last Name, Port Name, Port Country, Manager User ID, Background Investigation Status and TECS Status. In some cases, a user's Background Investigation Status and TECS Status must be verified by the supervisor/manager contacting the CBP Help Desk directly.

Entitlement also provides RBAC for the following CBP systems external to the ATS security authorization boundary:

- Port Radiation Inspection, Detection & Evaluation (PRIDE) & Secure Freight Initiative (SFI)
- Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW)
- New Automated Commercial Environment (NACE)
- Export System (formerly AES)
- Border Enforcement & Management Systems Division (Air & Marine Enterprise Reporting (AMO))
- System User Management & Monitoring for IT (SUMMIT) is an identity and system monitoring solution for UNIX and Lightweight Directory Access Protocol (LDAP) platforms. It uses a combination of LDAP, Postgres, and Apache to provide real time monitoring, alerting, user management, and privilege escalation (via Super User Do (SUDO)). A web interface allows users to request system accounts, privilege escalation, and to monitor systems in real time.

3.1.4 Customs-Trade Partnership Against Terrorism (C-TPAT) Infrastructure

The Customs Trade Partnership Against Terrorism (C-TPAT) program assists CBP in measuring risk by identifying import transactions where the risk is low, allowing CBP to focus on high risk transactions based on the data. The C-TPAT portal is a place for secure transactions and communications with C-TPAT applicants, partners and supply chain security specialist (SCSS) staff. The thousands of enrolled companies are critical players in the global supply chain, including U.S. importers, customs brokers, consolidators, port and terminal operators, carriers, and foreign manufacturers.

The goals of the C-TPAT program include: furthering CBP efforts to secure entry of goods into the U.S. and all countries by preventing terrorist access to transportation modalities, and to subsequently eliminate the potential for trafficking of implements of terror within the global supply-chain.

Under this contract, CBP requires C-TPAT infrastructure support.

C-TPAT is a joint government-business initiative to build cooperative relationships that strengthen overall supply chain and border security. Businesses apply to the program and commit to the following actions:

- Conduct a thorough self-assessment of supply-chain security using the C-TPAT security guidelines.
- Complete and submit a supply-chain security profile questionnaire to Customs.
- Develop a program to enhance security throughout the supply chain according to C-TPAT guidelines.
- Communicate C-TPAT guidelines to other companies in the supply chain and start building the guidelines into relationships with these companies.
-

3.1.5 Analytical Framework for Intelligence (AFI)

The Analytical Framework for Intelligence (AFI) system provides additional capabilities to DHS in the gathering, analysis, information sharing, and reporting of critical intelligence information within DHS and other

law enforcement partners. AFI directly supports CBP's strategic goals to secure the nation's borders from the entry of dangerous people and goods, while enabling the flow of legitimate trade and travel. Specifically, AFI provides the technology and tools that allow for the production of timely and actionable intelligence for CBP personnel protecting our borders, enhanced collaboration across CBP intelligence analysts, and more effectively share threat information and intelligence to its Federal partners charged with securing our nation.

AFI's purpose is to support the continued evolution of CBP as an intelligence-driven organization and improve the efficiency and effectiveness of intelligence lifecycle processes. AFI has evolved into a data analysis and intelligence product creation and dissemination platform that supports multiple DHS components, specifically CBP and Immigration and Customs Enforcement (ICE). AFI benefits include shorter time and expense in disseminating intelligence products to intelligence analysts in the field because reports are posted in a main repository and distributed to pre-identified communities. AFI serves as the one-stop shop for CBP and ICE-produced intelligence products with access available to intelligence organizations throughout DHS. AFI leverages existing legacy systems and provides an enhanced query, analysis, production, collaboration, and dissemination tool. AFI provides query, visualization, and analytic capabilities built on Big Data Services (BDS) Cloudera Hadoop and ElasticSearch. AFI provides an automated function that integrates information from multiple systems into a single platform that reduces manual effort and saves users valuable time.

AFI supports multiple CBP and DHS missions and goals. Specifically Preventing Terrorism and Enhancing Security. The AFI program:

- Creates efficiencies in collating and disseminating intelligence products, allowing for increased effectiveness and efficiency for CBP officers, OBP and Air and Marine agents in utilizing strategic and practical intelligence at and between ports of entry.
- Provides technology and tools that produce timely and actionable intelligence to DHS personnel charged with protecting our nation from threats posed by the illegal cross-border movement of goods and people, to include threat of terrorist activity.
- Provides data analysis and intelligence product creation and dissemination platform that supports multiple DHS components.

3.1.6 Enterprise Management Information System - Enterprise Data Warehouse (EMIS-EDW)

Enterprise Management Information System (EMIS) Enterprise Data Warehouse (EDW) consolidates CBP reporting capabilities to provide a common integrated view of the operational and business information and data for use within the CBP enterprise. EMIS EDW currently comprises reporting and analysis dashboards: BorderStat, Airport Wait Time, Managers, Western Hemisphere Travel Initiative (WHTI), and Workload Staffing Model Dashboards. Each reporting and analysis dashboard provides a specific and targeted view of the data from the EMIS EDW. Automated operations move data from source systems to the EMIS EDW on a regularly scheduled basis, to ensure that current data is available for reporting purposes.

EMIS EDW provides a one-stop access point for data in the areas of anti-terrorism, narcotics; passenger travel comprising of primary and secondary processing, apprehension and inadmissible, cargo processing and airport wait times. This data is stored in an optimized manner for cross-functional reports and analytical processing for management, analysts and field operatives within the Offices of Field Operations (OFO), Office of Border Patrol (OBP), Office of International Trade (OT) and Office of Intelligence (OI).

EMIS EDW continues to contribute to, and enhance, the Department of Homeland Security's (DHS) operational and intelligence management capabilities aimed at securing our nation's borders by providing accurate, timely and pertinent data that is updated from source systems on a regularly scheduled basis.

3.1.7 Enterprise Reporting System (ERS)

The Enterprise Reporting System provides the framework to implement agency-wide reporting and performance measurement capability across CBP. Support for under ERS includes support for all TASPD infrastructure. Hardware and platforms on which the TASPD system application operates is under the control of other programs and other contract vehicles, however application teams must support monthly server maintenance, as well as perform administration on both physical servers and virtual machines. Software changes are required to continue to properly interface with host platforms and existing physical and software interfaces.

3.1.8 Port Radiation, Inspection, Detection, and Evaluation (PRIDE)

The Port Radiation, Inspection, Detection, and Evaluation (PRIDE) System was developed as part of and in support of the Non-Intrusive Inspection (NII) program. The NII program deploys equipment at all ports of entry (POEs) that can screen conveyances, containers, and people for the presence of radiological weapons-grade material. PRIDE supports the NII program by connecting Radiation Portal Monitors (RPM), radioisotope identifier devices (RIID), visual identification systems (VIS), Optical Character Recognition (OCR) systems, and License Plate Readers (LPR) to the CBP network to provide data monitoring and retrieval capabilities that gives DHS and CBP the ability to immediately and accurately assess and respond to radiological threats.

PRIDE supports a rapid response to radiological threats by sending alerts and related data to scientists within seconds of an alert. In this way, PRIDE provides a valuable mechanism for scientists and officers to assess the threat and plan a course of action from a remote location.

PRIDE provides a standardized alarm resolution workflow via a web-based interface, and facilitates near real-time messaging and information sharing between remote port-based systems and centralized systems to facilitate collaboration with experts at centralized locations.

PRIDE provides the following features:

- Consolidation of data in a central database.
- Standardized alarm resolution/reporting workflow via a web-based interface
- Centralized data reporting via a web-based interface

3.1.9 New Automated Commercial Environment (NACE)

The New Automated Commercial Environment (NACE) is the commercial trade processing system that connects CBP, the international trade community, and Partner Government Agencies (PGA). It facilitates legitimate trade while strengthening border security by providing government officials with better automated tools and information to help them decide, before a shipment reaches U.S. borders, what cargo to target for further investigative action because it poses a potential risk and what cargo to expedite because it complies with U.S. laws. NACE provides the Single Window, the primary system through which the international trade community submits data and documentation required by all federal agencies for imports and exports, and through which the Federal Government will determine their admissibility.

The International Trade Data System (ITDS) provides the single system for Single Window, allowing for the multiple paper processes to be eliminated and importers and exporters to file information once to one system for the clearance of cargo. ITDS is made up of the Document Image System (DIS), Interoperability Web Services (IWS), and the Partner Government Agency (PGA) capabilities. CBP developed technical capabilities in NACE to automate and enhance interaction between participants by facilitating electronic collection, processing, sharing, and review of trade data and documents required by federal agencies as part of the cargo import and export process.

DIS allows the Trade to electronically supply documentation needed during the cargo release process by CBP and PGAs. This automated approach significantly improves the efficiency and cost effectiveness of the document submission and review process compared with the manual process in place. Messages are transmitted

in XML format using secure web services, FTP or MQ. The documents are securely stored and made available for review by CBP and PGAs. Documents submitted via DIS are in lieu of paper documents and provides basic document image submission and management capabilities:

- Allow Trade Partners to submit document images and associated descriptive meta data to CBP and PGAs in an automated manner using EDI communication
- Store all submitted documents in a secure centralized CBP data store and maintain associations with related data such as Entry and Bill numbers
- Allow authorized users to retrieve, view, and annotate documents via a web based user interface
- Provide basic security, authorization and auditing
- Offer back-end services that facilitate search and reporting capabilities to trade partners to verify the receipt of documents
- Provide capabilities for CBP Client Representatives to view raw received messages

IWS identifies and then builds the interfaces and protocols through which the PGAs and CBP will communicate and share information related to cargo imports. Interoperability plans are jointly developed and maintained by CBP and various PGAs.

The PGA Message Set is a single, harmonized set of information that is collected electronically from international traders by CBP on behalf of the PGAs, thereby allowing CBP and the PGAs to make decisions about what cargo can come into the U.S. without the myriad of paper forms currently required. This data set is used as the single record layout for all input from the trade for PGA data. This set is intended to be submitted as part of the NACE Entry Summary Certified for Release (or a Simplified Entry).

NACE Cargo Release (previously known as Simplified Entry) streamlines how filers transmit entry data to CBP to facilitate trade, while maintaining a strict adherence to U.S. laws. Filers are able to transmit entry information earlier allowing CBP personnel more time and resources to apply a risk-segmented approach to their inspections that allows them to focus resources on high-risk shipments while reducing transaction costs for importers. When CBP receives NACE Cargo Release data, CBP facilitates a decision to release the cargo and transmits a message to the filer. The merchandise will then be considered entered upon its arrival in the port with the intent to distribute the cargo into the U.S. commerce.

NACE Cargo Release is a web-based application provides an efficient way to process and view cargo information and forms the trade processing backbone and risk assessment within ATS.

The Automated Export System (AES) is a joint venture between CBP, the Foreign Trade Division of the Bureau of the Census (Commerce), the Bureau of Industry and Security (Commerce), the Directorate of Defense Trade Controls (State), other federal agencies, and the export trade community. It is the central point through which export shipment data required by multiple agencies is filed electronically to CBP, using the efficiencies of Electronic Data Interchange (EDI). AES provides an alternative to filing paper Electronic Export Information (EEI). Export information is collected electronically and edited immediately, and errors are detected and corrected at the time of filing. AES is a nationwide system operational at all CBP ports and for all methods of transportation. It was designed to assure compliance with and enforcement of laws relating to exporting, improve trade statistics, reduce duplicate reporting to multiple agencies, and improve customer service.

The export process begins when the exporter decides to export merchandise. The exporter or the authorized agent makes shipping arrangements (booking) with the carrier. The exporter or the authorized agent transmits the commodity (EEI) information using AES. This information can come directly from the exporter or the authorized agent or through a service center or port authority. AES validates the data against editing tables and U.S. Government agency requirement files and generates a confirmation message or error messages back to the filer. If the carrier is participating in the Vessel Transportation Module the carrier transmits the Receipt of Booking message when the booked cargo is received and the departure message following the actual departure of the vessel. Within ten calendar days after departure, the carrier will transmit the entire export manifest electronically using AES. AES also validates the transportation data then generates either a confirmation

message or an error message. Any errors messages generated by AES must be corrected and the corrections transmitted to AES. AES is a conduit through which required export shipment information reaches the appropriate agency. The Bureau of the Census extracts AES data to compile and publish export trade statistics. The goal is to eliminate manual processing and paper review of the EEI by providing accurate data, electronically, to be used for analytical and statistical reporting. AES checks dual-use shipments against licenses approved by the Bureau of Industry and Security and forwards the data to that agency.

3.1.10 Biometric Entry-Exit – Traveler Verification System (TVS)

In addition to the systems above, TASPD is also working in partnership with the air travel industry to transform air travel using biometrics as the key to enhancing security and unlocking benefits that dramatically improve the entire traveler experience. CBP will re-architect data flows and data systems to pre-stage biometrics data. The goal is to verify the traveler's identity upon departure from the United States and match the departing traveler's information with their corresponding entry information.

The CBP "Biometric Pathway" will utilize biometrics to streamline passenger processes throughout the air travel continuum, and provide the opportunity to validate identities against DHS information systems using the data available. CBP will partner with airlines, airports, OBIM, and TSA to build a device agnostic backend system that

interoperates with private sector investment in front-end infrastructure, such as self-service baggage drop off kiosks, facial recognition self-boarding gates, and other equipment; the CBP biometric-based entry-exit system will ultimately provide significant benefits to air travel partners, in addition to establishing a biometric air exit system.

For the purpose of this PWS, the offeror will support TASPD and other stakeholders by performing operations and maintenance of the system to support Biometric Air Entry-Exit. The contractor will also provide support in expanding Biometric Entry/Exit to other environments/modalities such as land and sea including, but not limited to cruise ships, Privately Owned Vehicles (POVs), commercial buses, and pedestrians. Each mode of travel requires unique capabilities to address operational and environmental conditions to perform biometric confirmations while not impacting trade and travel.

Land

Since land travel is often unscheduled, CBP does not have the benefit of receiving passenger manifest information prior to travel as it does with air and sea, therefore a person's identity and citizenship cannot be validated until they arrive at the primary inspection point. Proper inspection processing without advanced traveler information can take a considerable amount of time and result in severe congestion during peak crossing times at busy ports.

Contractor support will include incorporation of various data elements into a biometric matching capability at POV lanes. CBP is the owner of primary vehicle lanes (unlike the air environment, where a departure gate is owned by an airport authority or airline). Contract support will include the following:

- Implement a biometric solution to match inbound and outbound travelers to potential hotlists.
- Implement a system to record crossing data information

CBP will focus primarily on holding travelers accountable for self-reporting departure with a biometric verification component. If a traveler does not self-report their departure, CBP will assume the traveler is still in the United States (meaning the traveler would violate the terms of admission and not be eligible for re-admission).

Sea

The CBP mission in the sea environment is to facilitate the lawful entry and clearance of vessels, collect proper duties, prevent crew desertions, and prevent unlawful persons or prohibited items from making entry into the U.S. To achieve this mission without augmenting staff, CBP must find ways to improve the entry process by

leveraging mobile and biometric technologies. Because of the similarities between U.S. seaports and aviation ports, CBP plans to leverage solutions developed for the air environment to implement biometric exit at sea ports. Contractor support will include:

- Updates to mobile technology for matching to travelers in a cruise line environment, pleasure boats and boats for hire, which like general aviation present an extremely dynamic environment that will need innovative solutions.
- Interoperability and data integration with cruise lines for image capture of facial comparison to valid travel documentation (i.e. passport).
- Transmission of encrypted referral codes to cruise lines for traveler interception.
- Implementation of system threshold requirements and indicator to CBP and cruise lines (match/non-match).

3.1.11 Global Travel Assessment System (GTAS)

The Global Travel Assessment System (GTAS) is an air travel passenger screening and analysis system for enhancing global security. It was developed by CBP in the open source environment, so that foreign partner government entities could deploy it quickly with minimal startup costs. Ideally, these foreign partners would be engaged in the application's improvement, and those improvements would be shared back with the development community. GTAS allows users to assess the risk of travelers through real-time processing of user-defined rules and watch lists. Additional risk assessment tools include a robust set of querying capabilities, case management system, auditing capabilities, and system checks.

GTAS was built on a multi-tiered, modular system leveraging the most globally-accepted technology components. It currently supports 31 languages, and is available for download and use on github.com.

3.1.12 Common Framework

The Common Framework project is the enterprise effort responsible for the "common look + feel" across web and mobile applications. This includes responsive user interfaces, user experience design, reusable code and share services, developer experience, and application development best practices and education. The Common Framework project takes an open source, open data approach in promoting design, development, and operations best practices across the enterprise. The Common Framework directly aligns to the U.S. Digital Services Playbook.

The theme for U.S. Customs and Border Protection web applications can be found at https://us-cbp.github.io/cbp-theme. This is the common UI theme for CBP. It is used for internal and external web applications.

The CBP Style Guide compliments the CBP Theme and can be found at https://us-cbp.github.io/cbp-style-guide. The style guide describes CBP theme components and patterns and how to use them.

4.0 OPERATING CONSTRAINTS

4.1 The Contractor shall use DHS/CBP approved products, standards, services, and profiles as reflected by the hardware software, application, and infrastructure components of the DHS/CBP TRM/standards profile. If new hardware, software and infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal Technology Insertion (TI) process. The DHS/CBP TRM/standards profile will be updated as technology insertions are accomplished.

4.2 The contractor shall follow existing TASPD design standards unless deviation from those standards is approved by TASPD and the Contracting Officer's Representative (COR). The contractor is responsible for

understanding the OIT Common Framework code libraries, tools, style guide, services, and best practices and shall build and maintain CBP applications using the OIT Common Framework before using open source, custom, or third party solutions. This documentation will be made available to the contractor upon request.

4.3 All Application O&M and maintenance, updates, enhancements, upgrades, or modifications solutions within the scope of this PWS are inherent to the software applications and the corresponding application infrastructure. The hardware and platforms on which the TASPD system application operates is under the control of other programs and other contract vehicles, however application teams must support monthly server maintenance, as well as perform administration on both physical servers and virtual machines. Software changes are required to continue to properly interface with host platforms and existing physical and software interfaces. As infrastructure and applications are migrated to and operated in the cloud, the contractor must continue to meet or exceed current system performance. Security must also meet or exceed current levels while operating in the cloud.

4.4 All proposed enhancements, improvements, modernizations and new capabilities added to TASPD systems are subject to review and approval by the Government in accordance with the TASPD Configuration Management/Control Plan.

4.5 The AFI and ATS systems have a Section 508 waiver. Currently, all other systems are subject to 508 compliance.

4.6 TASPD strives to maintain full availability with an average acceptable quality level of 99.82%, which accounts for planned outages. The contractor will meet with this AQL. TASPD must regularly monitor system performance and tune system parameters to ensure a high level of system processing and responsiveness is available for thousands of end users. As such, operations and maintenance support includes Tier II and Tier III support related to TASPD applications, 24 hours a day, 7 days a week (24x7) for on call support, monitoring and administering the physical and virtual machines and 24x7 Database Administrator (DBA) support.

Most TASPD Tier III support is assigned from Tier I support (CBP Help Desk) directly to Tier II support (TASPD ATS Help Desk). If Tier II support cannot resolve the ticket, it is assigned to the application team (Tier III). Tier II will typically reach out directly to the application team for support. TASPD does not currently have dedicated Tier III staff, but each application team has to manage Production support and troubleshooting of issues that cannot be handled by Tier II.

In order to maintain availability 24 hours a day x 7 days a week x 365 days a year (24x7x365), all TASPD project teams are required to have a duty officer phone which are rotated among team members. These devices will be furnished by the Government and must be staffed at all times. If Production issues come up either during work hours or outside work hours, which need to be resolved right away, the application team (Tier III) will be contacted either by the CBP Duty Officer, CBP Technology Operations Center, TASPD Duty Officer, or TASPD Government Manager to troubleshoot and resolve the issue. Other team members may need to be engaged as necessary if the person carrying the duty phone needs support. Additionally, some users will reach out to the application teams directly (designated leads and POCs), including the TASPD Government Manager, with issues that need to be investigated. These issues may include diagnosing and addressing the questions raised by the users, corrections in Production that need to be applied right away, or code changes that need to be scheduled into a release.

4.7 Lifecycle support is required for all applications to include: requirements definition, tailored SELC and project documentation updates and training. Refreshes to the system happen at least on a monthly to quarterly basis, with the exception of urgent changes which can occur as quickly as within one day.

Production and troubleshooting support is expected on an ongoing basis, as well as support for priority data calls to support the user community.

4.8 All personnel supporting TASPD must have proper DHS/CBP security clearances per the CBP Security Handbook.

4.9 All contractor personnel supporting work on this PWS are required to use GFE computers and software hosting facilities. Exceptions must be approved on a case-by-case basis by the COR.

4.10 All software applications and the TASPD work in an environment that requires collaboration and cooperation with other government agencies and other contractors supporting TASPD and other related programs with common or shared missions and objectives.

5.0 OBJECTIVES

The overall objective of this task order is to obtain the full range of operations and maintenance support for the U.S. Customs and Border Protection (CBP), Targeting and Analysis Systems Program Directorate (TASPD) suite of computer and automated software applications. Additionally, the contractor will ensure all computer and automated software applications are updated and enhanced as necessary to respond to evolving technologies, threats, and mission critical requirements of CBP.

5.1 Objective 1- Task Order Project Management

Work efforts performed in support of this objective require management expertise, oversight, control, and direction in team building, communications, time management, quality assurance and quality control, procedure development, risk management, configuration management, cost management, and software integration. These areas and controls shall be continuously applied in the performance of the task areas shown below.

Provide overall project management support, including a transition plan, project planning, scheduling, tracking, and overall financial management. Specific duties shall include the preparation of plans and schedules based on technical and management data; scheduling and conducting technical and planning meetings; conducting reviews; and preparing status reports.

Weekly status meetings shall occur to discuss status of projects, issues, and problem areas related to the projects. The Contractor shall document the results of each meeting and submit this document weekly to the COR. In addition to reporting the status of each project, the Contractor shall provide the Government with fund status reports. Refer to section 7.5 for more information on the submission of each report.

The Contractor shall have the ability to recruit, hire, and retain CBP-cleared resources immediately following contract award, ensure proper staffing and skill set coverage at all times, and effectively address changes in work priorities and staffing. Demonstrate innovative ways to recruit and retain personnel.

Provide oral presentations and/or executive briefings on the project and application statuses when necessary.

Follow an iterative or Agile-based program and project management and deployment methodology which will allow for effective scope control and risk management. Agile methodology must follow the tailored SELC and comply with CBP and DHS policy, including DHS Directive 102-01. The Contractor shall also provide support to Integrated Product Teams (IPTs) as directed by the Government in support of the development/deployment of future functionality. The Contractor shall work with the IPTs to ensure alignment and compliance between deliverables, schedule, scope and agile methodologies. The Contractor shall also support the Government IPT project manager with Agile support and provide regular status reporting and scheduling that complements the Agile development methodology.

An Agile-based approach to management is critical to CBP's mission as it provides enhanced visibility throughout the lifecycle of a project, enabling OIT the necessary insight into achievement, progress, challenges, goals and next steps. It also enables TASPD to accommodate high priority changes and changes in direction as dictated by the product owners and the user community, in response to new and evolving threats and risks. TASPD is a very agile, nimble organization and new features which comply with the user requirements are often implemented in a very short amount of time. In an Agile organization, project teams deploy functionality incrementally, minimizing the potential for risk impacts, and provide streamlined documentation throughout the phases of a project. The contractor is expected to do sprint and release planning (with user stories in Jira), execution, review and demonstration and retrospectives. The contractor shall determine, prioritize, and document the product backlog for the project, develop definitions of done, conduct daily scrums, and utilize the Atlassian suite of tools to document the agile process.

5.2 Objective 2 – Operations and Maintenance of TASPD Computers, Server and Software Applications

The contractor shall provide all operations and maintenance (O&M) solutions, processes, and procedures necessary to sustain the suite of TASPD computer and software applications within the DHS enterprise at the highest levels of security, service and availability consistent with cost, schedule, and performance objectives. Application availability is exclusive of planned outages and deployment windows, but inclusive of computers, operating systems, network, work stations and software applications where TASPD has authority to operate as required to support the CBP mission objectives. Planned outages and deployments are scheduled with the product owners, with the goal of keeping down time to a minimum. The acceptable average quality level of application availability is 99.82% (See Section 5.6). Refer to the clauses in Addendum A for minimum security requirements. A full range of O&M solutions is necessary to ensure TASPD computer and software applications operate efficiently, effectively and securely, and are available to support CBP mission requirements. This O&M support will emphasize performance monitoring to identify and resolve performance risks before they impact mission performance while responding to customer identified performance deficiencies and/or outages (i.e., break/fix).

Performance shall be evaluated on a continual basis to ensure there is no degradation to current performance levels. The contractor shall maintain or improve the performance as system capabilities and usage continue to grow.

The contractor shall provide a full range of O&M to include, but not limited to, monitoring the health of production applications, troubleshooting software and system related issues, fixing software defects, as well as designing, creating, testing and implementing software production baseline updates. The contractor shall maintain strong collaboration with the Government lead, product owners and the designated POCs for the user community on an ongoing basis, to ensure that priority objectives and requirements are clearly understood by the contractor and implemented successfully based on established priorities. The contractor shall support all data modeling for new changes, new data feeds and data transfer mechanisms, data dictionary updates, ETL and cleansing, data analysis, and all database maintenance/administration tasks related to this.

5.3 Objective 3 – TASPD Computer and Software Application Performance Upgrades, Improvements and Enhancements

This effort encompasses system upgrades, improvements and enhancements, which are generally updates/changes to existing systems and the corresponding infrastructure installation, patching, and management. The Contractor shall provide all phases of software requirements, design, development, testing and implementation, to ensure TASPD software applications continue enabling their users to meet their mission goals and objectives. These efforts include the full range of software requirements, including, but not limited to, planning, requirements definition and analysis, systems design and development, coding and testing, integration, implementation and production support, and legacy system retirement. The contractor shall follow all CBP and DHS SELC procedures as applicable for the level of the enhancement. Consistent with the DHS/CBP SELC process and with the approval of the COR, the contractor shall take all necessary actions to

identify and incorporate software solutions to optimize the performance and operational cost efficiency of the TASPD suite of computer and software applications in support of the CBP mission. The offeror shall increase and enhance collaboration, responsiveness, transparency, and accountability with business owners and stakeholders, to ensure end users / stakeholders receive a high level of customer service to address high priority requests timely and to deliver new and enhanced solutions quickly, according to priorities set by the stakeholders.

5.4 Objective 4 – Cloud Migration

This objective encompasses migration of applications and services to the cloud, including legacy and new applications and all infrastructure, in a cost-effective, secure, and agile way. The strategy for migrating to cloud based services and infrastructure should align to the strategy of the Federal Data Center Consolidation Initiative (FDCCI), the objectives of the enterprise service delivery model, the CBP OIT target/cloud architecture, and support the agency's ability to deliver future sustainable services. This effort will enable TASPD to innovate and modernize the way software is built, deployed and managed. This approach will need to successfully enable TASPD to quickly, reliably and consistently deliver modernized digital solutions. These solutions include building digital solutions based on micro services, implementing API based modern web frameworks, building solutions that are extensible to mobile and forward-looking industry paradigms, building consistent, standard, reliable and portable environments in the cloud, defining container strategies and operational models. Support includes conducting an inventory (including users, applications, infrastructure, security and privacy, and service management), application mapping, conducting suitability analyses, providing recommendations to the government for the industry/service model, migration planning, including developing the migration roadmap, maintaining cloud infrastructure servers and virtual servers, operating systems, databases, applications containers and associated software, patching, DNS, network, storage and message transport).

The contractor will provide cloud migration support services that accommodate considerations from an enterprise perspective including impacts on other directorates, contract, management and technical components including application, infrastructure and security. The contractor shall tie cloud migration recommendations to the purpose of the applications or services being migrated and should include users, stakeholders, operating hours, and related input and output processes based on the role and business function of the affected systems. Specific objectives include:

5.4.1 Technical Objectives

- Provide all technical advisory services necessary to fully develop and deliver services for the appropriate phases.
- Provide services that account for the systems lifecycle, ranging from development, testing, and production and include considerations for maintaining cloud services post-deployment. Provide recommendations for commercial cloud environments for production, integration, development and sandbox purposes to support the complete systems lifecycle.
- Provide recommendations for open-standards based technologies whenever possible to provide interoperability. Recommend specific standards that should be utilized including:
    - Open Virtualization Format (OVF) – applicable only to IaaS virtual machines
    - Cloud Data Management Interface(CDMI)
    - Open Cloud Computing Interface (OCCI)
    - Other standards as required
- Provide capacity planning for additional resources for bandwidth, storage, and software licenses as required supporting the migration and on-going operations beyond the initial amount planned for operations.
- Provide migration status including milestones and support or implement specified migration testing plans and related rollback capabilities.
- Provide recommendations, standards, and associated SLAs to maintain sufficient and cost effective continuity of operations. Develop and contribute relative details to business continuity plans (BCP)

that satisfy the cloud service layers and components.

- Provide cloud solution requirements that maintain static, replicated, or live data at a site geographically disparate from the production site, when appropriate, such that the loss of one data center does not prohibit recovery of data within the prescribed recovery time objective.
- Provide approaches for efficient usage of cloud elements such as processor, RAM and data storage tiers, network capability and availability as needed within the target applications and services.

5.4.2 Security Objectives

- Provide support and cloud services in compliance and alignment with Federal statutory requirements (e.g. 38
  U.S.C. 5725) governing the protection of Personally Identifiable Information (PII) and Patient Medical Information (PMI), Federal Risk and Authorization Management Program (FedRAMP) standardized security assessment, authorization, and continuous monitoring policies as required by the scope of the project. Assessment and Authorization (A&A) activities will be included as part of the migration recommendations.
- Provide cloud migration security and privacy that are consistent with the NIST Special Publication 800-144 –
  "Guidelines on Security and Privacy in Public Cloud Computing" or other applicable standards and guidelines.
- Provide recommendations for and implement security for non-standard data transfers both in transit and at rest resulting from the migration of the infrastructure, applications and services to the cloud.
- Provide specified auditable events related to the infrastructure, applications and services
- Identify any additional Security and Privacy standards to which cloud service providers should conform their services/solutions. For example: Properly securing connections between formerly co-located systems, including systems not migrated for business or other reasons.
- Create effective compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for cloud service.
- Provide recommendations for administration support services to TASPD project system administrators to make sure that security controls not implemented by the Cloud Service Provider are available to the project administrators. Each Cloud Service Provider should publish a worksheet in their security documentation package that details security control responsibility for the particular type of cloud service offering (IaaS, PaaS, or Saas).
- Properly securing the connections between formerly collocated systems, including systems not migrated for business or other reasons.

5.4.3 Cloud Management Objectives

- Maintain clear government visibility into program cost, schedule, technical performance, and risk. This includes provide meaningful reporting and analytics weekly that provide TASPD with up-to-date and comprehensive information regarding technical and management performance.
- Provide recommended transition plans detailing milestones, activities, and timelines for the migration of infrastructure, applications and services to the cloud.
- Provide operational expertise and support for the business implementation as well as the user support required to ensure a successful implementation and rollout of the new cloud solutions. This includes but is not limited to communications to the workforce and external stakeholders, organizational change management, training, and documentation.
- Develop, maintain and support a change management strategy focused on optimizing user acceptance and technology adoption. The organizational change strategy shall address preparation for the change(s), and any impacts and steps for execution associated with changes needed to implement

cloud services.

5.5 Objective 5 – TASPD Performance Innovation

In addition to Objectives 1-3, the Government is interested in identifying new, innovative ways of enabling more effective and efficient performance. This task is to be used as a means for improvement and possible replacement of existing software applications and processes within TASPD. The Government is looking for innovation in, but not limited to, the following areas: surge capacity, increased consistency and value of applications, improved user experience, reduced project risks, and reduced implementation and O&M costs. CBP's vision is to continue to streamline operations and integrate with other systems to the extent possible.

The contractor shall innovate beyond simple modification of existing processes by recommending the utilization of new tools and methodologies. Tools not currently on the DHS approved list must be submitted to the Technical Reference Model (TRM), which has an estimated approval time of 14 days. The contractor shall use a variety of statistical metrics to generate quantified performance reports of project innovation, effectiveness and efficiency. Produce narrative descriptions, tabular data, graphical representations, and presentation materials that cover the entire process from methodology through results to include analysis of performance change.

The contractor shall provide the COR with a report detailing the recommendations for innovation and specific action plans to improve performance within 150 days of contract award, and every 6 months thereafter. The Government will review these reports and approve or deny the innovation as they see fit.

This task will run simultaneously to sections 6.1, 6.2, 6.3, and 6.4 throughout the life of the contract.

6.0 DELIVERABLES AND DELIVERY SCHEDULE

Deliverable ID	Description of Deliverable	Deliverable Date/Time Frame
0001	Security Plan, in accordance with 7.1	No later than 5 days after transition start date
0002	Draft Incoming Transition Plan	Due with Phase II response
0003	Performance Work Statement (PWS)	Due with Phase II response
0004	Submission of all CBP BI Packages	No later than 5 days following contract award
0005	Post-Award Kick-off Meeting	No later than 5 days following contract award
0006	Quality Control Plan	Due with Phase II response
0007	Final Revised Incoming Transition Plan	No later than 5 days after transition start date.
0008	Weekly Status Reports and Meetings	Weekly
0009	Contract Staff Training Requirements	As Required; To be reported by the 1st and 15th day of each month
0010	Ad-hoc reports	As Required

0011	Project Management and SELC Documentation	As Required for new projects
0012	Innovation Reports	No later than 150 days after contract award, every 6 months
0013	Cloud Migration Reports in accordance with Objective 4	Weekly
0014	Outgoing Transition Plan	365 days prior to the end of the final period of performance

6.1 Security Plan

The contractor will be responsible for ensuring that the contractor team complies with contract security requirements and sensitive information protection policies, including ensuring that all personnel have the appropriate level of clearances. The contractor will deliver an IT Security plan to the Government outlining their plan to comply with the Government's administrative, physical and technical security controls.

6.2 Incoming Transition Plan

The Contractor shall submit a draft Incoming Transition Plan for the transition from the incumbent to the Contractor with their Phase II response. The Contractor shall coordinate with the Government in planning and implementing a complete transition to the Contractor's proposed support model. The plan should include staffing approach including the processing of paperwork for the background investigation process, knowledge transfer and strategy for taking over the work including when responsibility for each project shifts to the newly awarded contractor.

The Government has designated a transition period for the incoming Contractor to coordinate and work with the incumbent Contractor. The Contractor shall assume support responsibilities in accordance with its Incoming Transition Plan, processes, procedures, and schedule. The Contractor shall implement the ramp-up process without disruption to TASPD operations or interruption/delay to the application systems and to the enhancement work in progress at the time of the transition. The Contractor shall make all necessary preparations to begin performance in order to ensure no impact to scheduled critical activities.

The Incoming Transition Plan shall include, at a minimum:

- Overview of the transition effort;
- A work plan that identifies milestones, measurable tasks, and resources required to assume responsibility for all in- progress and pending activities;
- A detailed summary of all transition events and estimated milestone dates. The transition timeline shall be presented as a schedule in graphic format showing the timing, sequence and interdependencies of tasks. The transition schedule shall be supplemented by narrative, as needed to provide a clear understanding of the transition plan.
- Define interfaces with CBP and the offeror's proposed coordination with the current contractors;
- If transfer of existing CBP databases to other hardware/software formats is proposed, the offeror shall explain how and when the proposed formats/systems and their capabilities will be demonstrated prior to effecting any transfer;
- Identify the risks to the transition effort and include mitigation and contingency plans in the event the transition cannot be executed on schedule;
- Specific measures and metrics to be used to monitor and evaluate the transition activities;
- How the offeror will recruit, hire and onboard the staff needed to ensure mission success to include incumbent capture;

- Government-furnished property inventory management assistance;
- Specific measures and metrics to be used to ensure that system performance and response times are not degraded during the transition period;
- Plan for submission of all available CBP BI packages
- Identification of the Incoming Transition team members by name, position, and responsibilities; and
- A plan for executing redundant performance with the outgoing contractor upon successful completion of knowledge transfer.

A Final Revised Incoming Transition Plan is due five (5) business days after the Contractor-Government kick-off meeting. The Final Incoming Transition Plan will be executed without disruption to operations. The Contractor is fully responsible for all aspects of the work throughout the Incoming Transition period in accordance with the Contractor's Incoming Transition Plan. The Contractor shall make all necessary preparations to begin Task Order performance in accordance with its Incoming Transition Plan in order to ensure no impact to daily operations or scheduled critical activities.

6.3 Clearance Process

The following information is provided to prospective organizations who have never worked with CBP before, or for those who do not have knowledge of the background investigation process. Information provided is based upon averages, and is meant to provide a basis for estimating the time it may take to clear resources.

The background investigation (BI) process within the Department of Homeland Security (DHS), Customs and Border Protection (CBP) begins when the contractor submits the Contract Employee Initial Background Investigation Form (Form 77), Background Investigations Requirements Determinations (BIRD) form, Fair Credit Reporting Act release form and the new contractor information sheet to the Government. The Government approved paperwork is then submitted to the Office of Professional Responsibility (OPR) for a determination regarding whether the applicant is eligible for 1) reciprocity, or 2) needs to be invited into e-QIP. CBP OPR will review the BIRD request, along with attachments, to conduct the appropriate systems check to render the appropriate determination, i.e., initiation required, reciprocity eligible, reactive, reciprocity revoked. This determination process takes approximately 1 week.

1) If candidate is eligible for reciprocity, the process to a full background investigation averages about 1 month.
2) If the determination rendered was "Initiation Required" or "Reciprocity Revoked," the Government will be responsible for taking the appropriate action to allow the applicant access to e-QIP. The applicant will need to complete e-QIP, financial disclosure forms and finger print cards. This process takes approximately one week, however the applicant has up to 30 days. All forms are to be submitted to the Government for review. If all forms and e-QIP are completed, the BI package is submitted to OPR. If not, e-QIP is rejected and must be corrected. After submitting the BI package to OPR, the BI is conducted. An Interim BI is the next step in the process and averages approximately 40-50 days. A full BI averages approximately 130-140 days after the Interim BI is granted. Please note that this is the best case scenario, applicants may drop into Delay, which means that more documentation is required for the BI to be completed. Delayed applicants can remain in delay for many months and may be found unsuitable and therefore unable to be hired onto the contract. From submission of documentation to a delay determination usually averages one to two months.

Overall, the average time to receive a Full BI, from submission of the required BI documents, is 175 days. This time estimate is furnished for the purposes of indicating the time required to obtain CBP BI cleared personnel. This is the Government's estimate and is not intended to be binding on either party or to be the only possible scenario.

All members of the project team must obtain CBP Suitability to begin work. Reference 5 CFR Part 731, "Suitability." Some of personnel under certain tasks will need to possess a Top Secret Security Clearance with access to SCI in order to research and review (Classified) threat information. When a security clearance of secret or higher is required in performance of the order, a completed DD Form 254 is required. Many of the contractors who support TASPD have Secret, Top Secret or TS/SCI clearances. Although no requirements are set forth for the number of contractors with clearances required, TASPD is moving in a direction where candidates with Secret and Top Secret clearances are preferred.

6.4 Quality Control Plan

The Contractor shall have an established, maintained, and effective Quality Management System (QMS) that ensures quality products and services are delivered to the Government. The Quality Control Plan shall describe the QMS in sufficient detail to permit an assessment of the contractor's QMS by the Government. The Quality Control Plan shall describe the Contractor's approach to meeting the quality, timeliness, responsiveness, customer satisfaction, and other product and service delivery requirements.

6.5 Weekly Status Reports

The contractor will provide regular communication of project status through weekly status reports and weekly face-to-face status meetings between the team, the COR, the CBP government leads and any other stakeholders as identified by the Government. The contractor is responsible for monitoring the contract by tracking expended funds.

The Contractor shall provide the COR with a weekly report, for each task in section 6.0 with an overview of work accomplished the previous period and work scheduled for the upcoming week. This report shall contain the following information at a minimum:

- Planned activities and desired results for the next reporting period with milestones and deliverables;
- Issues and risks affecting technical, schedule, or cost elements of the contract, including background, impact and recommendations for resolution;
- Results related to previously identified problem areas with conclusions and recommendations;
- Team organizational chart;
- Funds Status Report that supplies funding data about the task order.
    - Updating and forecasting contract funds requirements based on burn rates;
    - Developing funds requirements and estimates in support of approved investments;
    - Determining funds in excess of contract needs and available for de-obligation.

6.6 Contractor Staff Training

All contract personnel are required to complete the DHS/CBP mandatory PALMS training courses by the mandatory due date(s). The Contractor is responsible for maintaining records of contracting employees that have completed the mandatory training and provide semimonthly updates to the COR on the 1st and 15th day of each month or the next business day if the 1st or 15th is a Holiday or on the weekend. The Contractor is also responsible for providing copies of the training certificates to the COR when requested.

6.7 Contractor Outgoing Transition Plan

At the completion of performance of this task order, the Contractor shall fully support the transition of the Contractor's work that is turned over to another entity, either Government or a successor offeror(s). The Contractor shall assist with transition planning and shall comply with transition milestones and schedules of events.

The Contractor shall be responsible for the implementation of the transition and application cutover activities. The transition shall cause no disruption of services. To ensure the necessary continuity of services and to

maintain the current level of support, the Government may retain services of the incumbent Contractor for some, or all of, the transition period, as may be required.

The Contractor shall be responsible for the transition of all technical activities identified in this task order. 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, and Government Furnished Information (GFI) to include
- Transfer of documentation currently in process into repositories
- Transfer of all software code in process into repositories
- Certification that all non-public DHS information has been purged from any Contractor-owned system
- Exchange of accounts to access software and hosted infrastructure components
- Participate in knowledge transfer activities in accordance with the transition plan
- Provide members to and participate in transition management
- Identify transition risks and risk mitigation

The Contractor shall submit an Outgoing Transition Plan. The Outgoing Transition Plan shall include support activities for all transition efforts for follow-on requirements to minimize disruption of services. The Outgoing Transition Plan shall:

- Review, evaluation and transition of current support services
- Provide report on status of all deliverables;
- Provide report on problems encountered during period of performance;
- Provide report on current issues, problems, or activities in process that require immediate action;
- Applicable debriefing and personnel out-processing procedures; and
- Identify and provide a schedule of routine events for continuity of program
- Identify equipment, hardware, software, documents and other artifacts that are included in the transition
- Establish roadmap and backlog
- Identify transition risks and risk mitigation
- Define roles and responsibilities
- Define transition approval authorities and lines of communication
- Define a knowledge transfer approach
- Define a property inventory and transition approach
- Provide checklists

A Transition Plan shall be delivered 365 calendar days prior to the task order expiration date unless otherwise directed by the CO. The Contractor shall account for a 10 business day Government review process prior to executing the transition. Upon award of a follow-on contract, the incumbent Contractor will work with the new Contractor to provide knowledge transfer and transition support, as required by the COR.

7.0 GOVERNMENT FURNISHED EQUIPMENT AND INFORMATION

(a) The Government will furnish only that equipment necessary for the Contractor to carry out its work efforts under this PWS at the Government facility. This includes normal workspace accommodations such as desk, chair, desk phone, and computer. While performing work under this PWS in Government facilities, the Contractor may have the use of other normal office EIT devices, such as fax machines (not classified), copiers, projectors, etc. It is required that the contractor obtain CBP Personal Identity Verification (PIV) cards as they are necessary to log into all computers and laptops.

(b) The Government will provide to the Contractor cell phone, laptop or other portable devices, such as mobile devices or other PDAs upon the written consent of the COR justifying the need for such equipment.

(c) The Government will furnish all necessary related documentation in its possession that may be required for the Contractor to perform this contract.

8.0 PLACE OF PERFORMANCE AND HOURS OF OPERATION

8.1 Place of Performance

U.S. Customs and Border Protection (CBP) will provide space in multiple facilities for the on-site contractor staff to perform the required tasks in the Washington DC Metro area, however most work is performed at site (a) below. Other locations for this work are below, although other Washington DC area offices may be occasionally used. All work required under this contract shall be performed by the Contractor at Government sites unless otherwise directed by the Government. Travel to other Washington DC area Government locations may be necessary.

a. OIT, Kingstowne Facility, Alexandria, VA 22315
b. OIT, Herndon Facility, Herndon, VA 20170
c. Ronald Reagan Building, 1300 Pennsylvania Ave, NW, Washington, DC 20229
d. OIT, Ashburn Facility, Ashburn, VA 20147
e. Data Center, Newington VA
f. National Targeting Center, Sterling, VA 20164
g. Walker Lane Facility, Alexandria, VA 22310
h. Beauregard Facility, Alexandria, VA 22311

8.2 Hours of Operation

For those contractor personnel working in direct support of TASPD, the normal business hours are 7:00 am to 6:00 pm (EST), Monday through Friday with core business hours between 8:00 am and 5:30 pm each business day. The contractor shall ensure coverage of these core hours for those in direct support of the TASPD. TASPD and those directly supporting TASPD will recognize all official federal holidays. However, all TASPD computer and software applications support a 24/7/365 mission requirement and the contractor shall ensure system application performance standards are maintained over the full range of mission operations. Due to the nature of the work, overtime is authorized under this PWS, however all overtime must be requested in advance and approved by the COR and Contracting Officer. The Contractor must provide a central point of contact to reach the necessary staff in the event of system problems or emergencies. If required by the COR or Government Team Lead, the contractor's staff shall report on-site after normal hours to address system problems.

9.0 PERSONALLY IDENTIFIABLE INFORMATION (PII)

When a contractor, on the behalf of CBP, handles Sensitive PII data, stores and transmits, the contractor will Accredit (ATO) this information system to the High, High, Moderate (HHM) FIPS level.

PERFORMANCE WORK STATEMENT (PWS)

Department of Homeland Security (DHS) - Customs and Border Protection (CBP) - Office of information and Technology (OIT) - Targeting and Analysis Systems Program Directorate (TASPD)

Business Intelligence Support Services (BISS)

1 BACKGROUND

The U.S. Customs and Border Protection (CBP) is a component of the Department of Homeland Security (DHS), and the priority mission of CBP is to prevent terrorists and terrorist weapons from entering the United States. This important mission calls for improved security at America's borders and ports of entry as well as for extending the zone of security beyond physical borders so that American borders are the last line of defense, not the first. CBP also is responsible for apprehending individuals attempting to enter the United States illegally, stemming the flow of illegal drugs and other contraband; protecting our agricultural and economic interests from harmful pests and diseases; protecting American businesses from theft of their intellectual property; and regulating and facilitating international trade, collecting import duties, and enforcing U.S. trade laws.

The Office of information and Technology (OIT) is the information technology component of CBP. OIT's responsibilities are vast-ranging from designing, delivering and maintaining technology based capabilities to enterprise architecture and governance. OIT also provides solutions that support CBP inspection and enforcement activities to help CBP Officers and analysts protect our borders and safeguard America. OIT is responsible for enhancing, administering, and maintaining intelligence and targeting systems and related systems that help secure the supply chain and support CBP's layered defense strategy for international cargo and passengers.

The Targeting and Analysis Systems Program Directorate (TASPD), one of OIT's program directorate, is responsible for developing and maintaining analytical and targeting software systems. The purpose of this Performance Work Statement (PWS) is to procure services that will support TASPD with respect to business intelligence support services. As volumes of data increase in people, cargo and conveyances, officers require more efficient access to relevant real-time information on which to base critical admission decisions. Risk assessment strategies are multi-tiered in approach and founded on complex statistical studies, data analysis and rules based on knowledge engineering.

2 SCOPE

Business intelligence support services are needed to assist CBP officers and border enforcement personnel in effectively and efficiently identifying cargo, individuals and conveyances that may

present additional risk to the United States; conduct terrorism analysis and global assessments that convey changes in terrorism threats and identify emerging threats; develop and evaluate CBP-wide intelligence based targeting rules and intelligence driven special operations; and coordinate and enhance analysis and targeting efforts. Support includes:

- **Project Management:** Provide oversight to effectively and efficiently manage this task order including maintaining adequate levels of technical resources, reporting, quality assurance and financial controls.
- **Intelligence Analysis - Counterterrorism - Social Networking:** Provide research, analytical and targeting support by providing data extraction and data management support, network analysis, complex query design and visualization capabilities
- **Predictive Modeling**: Provide data-driven modeling to further modeling efforts incorporating state-of-the-art analytical tools, harnessing the power of machine learning, and focusing on analytical work. Work to discern anomalies that would escape the human eye as well as subtle common features that are highly predictive of future behavior.
- **Proxy Positives/National Security Inbound (NSI)**: Facilitate the standard definition of a Proxy Positive by reporting the Proxies (rail) that meet the criteria set out in National Security Proxy Positives Reporting Process and evaluating the results and providing feedback on which seizures to include, and reporting the refined set of Proxies. That NSI reporting process facilitates objective assessment of model efficiency and effectiveness for all other applicable modes of transportation and threat domains.
- **Entity Resolution**: Improve passenger vetting through improved true positive identification of imminent travelers, additional name variants and augmented data and advance matching probability that will improve matching precision to reduce labor, speed processing, and increase targeting accuracy.
- **Threat Research Support:** Research specific threat behavior using all reasonably available data (classified, open source, CBP historical and transactional data, etc.) and then analyze and model that behavior) for the purpose of developing threat assessment techniques to target that behavior.
- **Visualization:** Provide visual representation of threat indicators which allows analysts to visualize and comprehend vast amounts of interrelated information in graphical and spatial representation.
- **Query Support:** Provide query support on big data platforms to support a growing demand in the number of users, quantity of requests, and complexity of queries for intelligence analysis. Includes searching and analyzing data stores, querying and extracting information and running impact assessments.

3 APPLICABLE DOCUMENTS

DHS Directive 102-01

CBP Security Handbook

DHS/CBP Program Lifecycle Process Guide

DHS MD 8110 – Intelligence Integration and Management

CBP Agile Framework

CBP SELC process

Office on Accessible Systems and Technology (OAST) Compliance

DHS Information Security Policy, MD4300.1, Information Technology Systems Security

DHS MD 4300A, DHS Sensitive Systems Policy and Handbook, CBP Information Systems Security Policies and Procedures Handbook HB-1400-05

All applicable National Institute of Standards and Technology (NIST) Special Publications (800 Series)

DHS Data Management Policy MD 103-01

Addendum A – DHS Clauses

Addendum B - National Security Proxy Positives Reporting Process – The performance by the contactor of Task 4.4 of this Performance Work Statement must adhere to this established process.

Addendum C – Technical Environment

4 TECHNICAL ENVIRONMENT

OIT performs system activities in a technical environment supported by a broad set of architectural components and/or Commercial-Off-the-Shelf (COTS) packages. Addendum B lists hardware and software components of the general infrastructure and development / production environment in terms of both hardware and software. We have adequate computing capacity for our current and projected needs to include development, testing and production. This includes associated networking, storage and offsite infrastructure.

5 SPECIFIC TASKS

5.1 PROJECT MANAGEMENT

The Contractor shall maintain adequate levels of project management, technical resources, quality assurance and financial controls. These areas and controls shall be continuously applied in the performance of the task areas shown below.

This task is defined by the following activities:

1) Provide overall project management assistance, including project planning, scheduling, tracking, and overall financial management. Specific duties shall include the preparation of plans and schedules based on technical and management data; tracking budget and expended funds; scheduling and conducting technical and planning meetings; conducting reviews; and preparing status reports.
2) Weekly status meetings to discuss status of projects, issues, and problem areas related to the projects. The Contractor shall document the results of this meeting and submit this documentation weekly.
3) The Contractor shall provide oral presentations and/or executive briefings as needed.
4) The Contractor shall have a validated Earned Value Management System (EVMS) to accommodate any new development tasks or specific projects as identified by the Government that may arise during the course of this contract. An EVMS is only required for new large development projects that may begin during the course of this contract.
5) An iterative or Agile based program and project management and deployment methodology shall be used, as agreed upon with the Government, which~~that~~ will allow for effective scope control and risk management. Agile methodology must follow the tailored SELC and comply with CBP and DHS policy, including DHS Directive 102-01. The Contractor shall also provide support to Integrated Product Teams (IPTs) as directed by the Government in support of the development/deployment of future functionality. The Contractor shall work with the IPTs to ensure alignment and compliance between deliverables, schedule, scope and agile methodologies. The Contractor shall also support the Government IPT project manager with Agile support and provide regular status reporting and scheduling that complements the Agile development methodology.

5.2 INTELLIGENCE ANALYSIS - COUNTERTERRORISM - SOCIAL NETWORKING

The Contractor shall provide research, analytical and targeting support by providing data extraction and data management support, network analysis, complex query design, and data visualization capabilities to National Targeting Center (NTC) officers. This support includes integration of analytic services and support of existing application and new applications.

This task is defined by the following activities:

1. Perform **research to include identification and visualization of networks** using internal and external data sources. Create or augment networks that enhance understanding of transnational criminal organizations (TCOs). Research the entities, roles, and relationships within such networks to identify illicit activity. Entities include but are not limited to persons, conveyances, shipments, and documents. Analyze trade, travel, criminal activity, and money movement to isolate those actors, activities, and networks that represent threats to the US security or legal trade and travel.

2. Coordinate with **intelligence community**. Working within Sensitive Compartmented Information Facilities (SCIFs), gather analyst requirements, review classified information, and use analytic tools to support analysis of threats. Support the transfer of unclassified information to high side analysts. Support the deployment of tools used in

the unclassified environment for use in the classified environment. This includes but is not limited to all aspects of Extraction, Transaction, and Loading (ETL), Relational Database Management Systems (RDBMS) and non-SQL data stores, storage configuration, search, query, extraction, data preparation, data modeling, machine learning, predictive modeling, testing, optimization, metrics, deployment, and maintenance.

3. Perform **network analysis**. Conduct research to identify or advance understanding of specific actors, activities, or networks associated with directed or approved threat categories. Using open source, COT, Government-Off-the-Shelf (GOT), or other custom tools, create, navigate, edit, augment, save, share, and integrate into presentations and work products those networks required to best support NTC Officers and other analysts' ongoing efforts to support both emergent and ongoing mission demands.

4. Perform **data extraction**. Gather analyst requirements, identify required data, sources, and relationships, and perform SQL, non-SQL or User Interface (UI)-based application data extraction to produce data sets that meet analyst's requirements.

5. Perform **data management**. Gather analyst requirements, create, organize, and use data stores, create and use indexes, create and use data documents, and optimize the ability to query and retrieve required data. Save, store, organize and retrieve in an efficient manner analytical products to support analyst's requirements. Support hardware and software installation, configuration, optimization, customization, security, and maintenance. Tasks include but are not be limited to database administration, Virtual Machine (VM) administration, network administration, routing, capacity planning, logging, diagnostics, alerting, and reporting. Support a big data environment that consists of several dozen Hadoop clustered servers and several dedicated indexing servers. Support will range from ingest and ETL of external data to application of search and analytics tools. Apply predictive analytics to massive data sets (billions of rows, several hundred terabytes of data). Anticipated data growth is greater than 10% per year. Optimize processes for speed and accuracy. Balance resources against multiple, high priority, near real-time requests from thousands of concurrent users. Support entity resolution, search, ontology development, network visualization, and ad-hoc querying in the big data environment.

6. Perform **complex queries**. Gather analyst requirements, create, run, optimize, save, edit, and reuse SQL code and aggregated SQL or other scripts to meet complex information requests beyond mere data extraction. Perform data schema analysis, performance optimization, data profiling, data quality, data validation, testing, and integration to improve query results. Produce narrative explanation of results, spreadsheets, graphs, and other presentations.

7. Perform **data visualization**. Gather analyst requirements, and use a variety of tools – including desktop productivity application suites, network analysis visualization tools, and other COT, GOT, or custom environments – to present data in various graphic forms to include but not limited to graphs, charts, networks, and non-traditional presentations such as heat maps, clusters, 3-D, spatial, temporal, and other relational dimensions.

Work under this task includes daily production of reports on entities and networks, data management, data extractions, query request logs, and demonstrating visualization tools with production data to navigate, view, traverse, amplify, or better understand networks, entities, relationships. It includes coordination with the intelligence community and providing surge capacity for 24x7 operations should the need for rapid response to exigent circumstances outside of normal working hour arise.

5.3 PREDICTIVE MODELING

The Contractor shall provide data-driven modeling to further modeling efforts incorporating state-of-the-art analytical tools, harnessing the power of machine learning, and focusing on analytical work. Work to discern anomalies that would escape the human eye as well as subtle common features that are highly predictive of future behavior.

This task is defined by the following activities:

1. Conduct **data analysis**. Perform data profiling and associated statistical analysis in preparation for presenting data to machine modeling tools. Identify non-obvious data anomalies.

2. Perform **machine learning**. Use a variety of machine learning tools and algorithms to identify data correlations as potential components of aggregate predictive models. Explain in non-technical language the nature of found correlations, confidence in the results, and applicability to support mission objectives.

3. Generate **predictive models**. Use the results of machine learning to produce predictive models that use archived, calculated, and/or real-time data to predict actors, activities, and outcomes for various threats. Narratively and mathematically describe the model factors, coefficients, equation, and meaning of the probability result(s).

4. Conduct **hypothesis testing**. Establish hypotheses as logical frameworks to test predictive models against objective metrics of success. Run models against reserved non-training data to validate model performance and to confirm/reject hypothesis.

5. Perform **variance analysis**. Use a variety of statistical analysis tools to determine the expected variability surrounding predictions in multiple dimensions including but not limited to time, location, category of actor/activity/cargo, conveyance, volume/weight/quantity/quality of materials, mode of transportation, and workload capacity. Narratively and graphically describe predicted variance, confidence of the analysis, and observed variance on reserved training or actual new data. Recommend threshold values and time periods that delineate boundaries of acceptable variability. Provide statistical verification for products.

6. Conduct **sensitivity and specificity analysis**. Use a variety of statistical analysis tools to determine the sensitivity and specificity of the model relative to its designed/intended

predictive capacity. Narratively and graphically support conclusions including but not limited to creation of population, sampling methodology, factor descriptions, and receiver operating characteristic (ROC) curves. Compare model performance against random and existing models' performance.

7. Support **model integration**. Work with application and user interface developers; assist in the integration of produced models with application code to support decision support analysis.

8. **Measure and report results**. Use a variety of statistical metrics to generate quantified performance reports of predictive model innovation, effectiveness and efficiency. Produce narrative descriptions, tabular data, graphical representations, and presentation materials that cover the entire modeling process from methodology through result to include comparative analysis of random and existing model performance. Report results both orally and in writing to include but not limited to executive summaries and detailed written reports.

Work under this task includes monthly model development and refreshes. Refreshes include models already in production as well as models developed under this Performance Work Statement. It includes monthly reporting describing data analysis, machine learning, model hypothesis testing, variance analysis, sensitivity and specificity analysis and model integration work done in support of predictive modeling.

5.4 PROXY POSITIVES/NATIONAL SECURITY INBOUND (NSI)

5.4.1 CURRENT PROXY POSITIVES - RAIL

The Contractor shall facilitate the standard definition of a Proxy Positive by reporting the Proxies that meet the criteria set out in National Security Proxy Positives Reporting Process and support Government Accountability Office (GAO) activities against National Security Weight Sets. This is the current process used by the Government. The Government is interested in identifying new, innovative ways of representing this information. Section 5.4.2 describes innovative work that could be used as an alternate or possible replacement to current processes.

Using the guidance from the government lead, documentation supplied by OIT and defined and documented by the Proxy Positive Working Group, the contractor will run the proxy positive report by mode each quarter. The Contractor shall refer to the definitions as stated in the Working Group documentation, add or remove proxies accordingly, and send to the OIT team lead for Office of Intelligence (OI) concurrence. Once OI concurrence is received, the contractor will put the data into the ROC curve and run ROC curves and/or other metrics, to be determined by the government lead, for each mode each quarter.

This task is defined by the following activities:

1) Quarterly data pull of possible proxies (both automated and manual, when necessary based on the following).
    - Test and verify the functionality of proxies automated scripts and software applications. Testing of the software applications may be automated, but testing of performance reports such as the ROC, likelihood ratios and alternative metrics may involve a manual process to statistically sample structured and unstructured data based on pre-defined criteria for a proxy. The government has the right to require third party testing.
    - Support OI analysis to establish pre-defined criteria for a proxy based on automated and manual data exploratory analysis. Identify alternative approaches and performance measurement scenarios to improve the proxy selection process. Provide continuous findings, recommendations and analysis for OI analysts to review and assess the performance results for the proxy criteria.
    - Work with OIT and OI's Project Managers (PMs) to design, code, test and perform data analysis for the proxy identification and selection process. Produce data extracts and provide technical support to the PMs for functional assistance to identify and implement criteria for a proxy.
2) The contractor will assess trends to determine the inclusion or exclusion of other criteria to define a proxy. The contractor will provide innovation and recommendations for improving the proxy process.
3) Internal working group support (including meetings with OI's four mode PMs).
4) External working group support (currently including OI cargo targeting, OI analysis division, Office of Field Operations (OFO), and Office of Trade (OT) to validate the performance measure process.
5) Unmatched proxy research (both automated and manual, when necessary) to locate and determine if the proxy meets the pre-defined criteria for a proxy.
6) Audit support (i.e., explaining the process from the first automated data pull of proxies through the final ROC curve during audits of the process) to include preparing for/being present at briefs, interviews, and actual audit presentation.
7) Administrative support for all proxy meetings and the ROC curve process in general to include:
    - Documentation of all processes and procedures
    - Maintenance of the documentation
    - Updates to the documentation as agreed to by the Working Group
    - Correlation analyses for all proxies considered whether accepted or rejected
8) Work with mode PMs in OIT and OI to identify and resolve issues with the process and/or identification of proxies.
9) Per GAO recommendation, continually identify, assess and document alternatives to the ROC curve performance measure.
10) Present methodology/approach to revamping the Proxy/ROC Curve process and run this process alongside the current Proxy/ROC process to prove the concept.

5.4.2 NATIONAL SECURITY INBOUND (NSI)

The Contractor shall provide the Contracting Officer Representative (COR) with Quarterly National Security Model Performance Reports for all applicable modes of transportation and threat domains. These reports will provide an objective assessment of model efficiency and effectiveness to aid CBP in meeting GAO and congressional reporting requirements.

Each report will cover several key operational metrics and targeting attributes, including:

- Overall model target volume over time and by mode of transportation
- Distribution of target volume by national security-related threat
- Enforcement actions associated with model targets
- Overall inspection rates associate with model targets
- Geographic distribution of model targets by country and Port of Entry
- Commodity distribution of model targets by description and Harmonized Tariff Schedule
- Appendix including source data in tabular format for validation
- Classified appendix containing pertinent classified research and analysis conducted during the quarter, including if and how the National Security model was updated to reflect newly identified intelligence

The Contractor shall coordinate with business stakeholders to determine whether a quarter's report warrants updating the National Security Model portfolio and, if so, formulate a plan to execute the requisite changes.

The Quarterly National Security Model Performance Reports process requires retrieving pertinent transactional and enforcement data from CBP's Automated Targeting System (ATS), transforming the data to prepare it for analytics, generating summary statistics across pertinent targeting attributes, and visualizing key attributes for stakeholder consumption. In addition, the process requires cleared resources to evaluate pertinent classified intelligence to determine whether the National Security Models are incorporating the most up-to-date targeting criteria, or require updates outside of the general model operation and maintenance (O&M) lifecycle.

5.5 ENTITY RESOLUTION

The Contractor shall improve vetting efficiency through entity resolution applied research and algorithm implementation. The objective is to increase true positives while reducing false positives, with agile and dynamic threshold adjustments to meet workload capacity. Example activities include automated name matching of imminent travelers, production of name variants, and aggregate fuzzy search mechanisms across multiple corroborative entity attributes. Work includes advanced and real time match probability calculations that improve vetting processes by reducing labor, speeding processing, and increasing accuracy.

This task is defined by the following activities:

1. Conduct **data analysis**. Perform data profiling and associated statistical analysis in preparation for presenting data to rule sets, name matching algorithms, and entity matching tools.

2. Conduct **data mining**. Subsequent to data analysis, build data sets appropriate for machine learning tools. This includes but is not limited to observation of threat actors, activities, and associations. Aggregate data to permit correlations analysis and creation of data objects useful in predictive analytics. Both structured and unstructured data mining are required. Unstructured data filtering, parsing, imputing, validation and cleaning in support of subsequent entity matching are included. For example, scan an unstructured document and identify all persons, corporate entities, and addresses.

3. **Evaluate entity resolution tools**. Determine those tools that best support real-time and predictive match decision support for entity resolution to include but not limited to name matching, biometrics, role-matching, corporate attributes, address matching, document matching, geo-temporal analysis, pattern-of-life characteristics, and fuzzy logic for any/all of these attributes. Work is not limited to matching person but also corporate entities, conveyances, containers, and shipping methodologies.

4. Use **new methodologies**. Given the specific population of historical data for persons and cargo to be vetted, recommend innovative use of tools and methodologies to improve the true positive match rate while decreasing the false positive match rate.

5. Establish **objective performance metrics and evaluate constantly**. Given open source, internal, and reference data, determine the efficiency and effectiveness of matching methodologies. Make recommendations for improvement with statistical justification. See also predictive modeling and associated analyses.

6. Incorporate **lessons learned** continuously. For each failure to identify a true positive match or person or shipment to pre-arrival data and events, conduct an analysis to determine what, if anything could be done to avoid missing similar true positives in the future. Identify the characteristics of data preceding the event, the matching processes used to identify true positives, the proximate and aggregate causes for missing the match, and recommend process changes to improve matching within workload limits.

7. Conduct **performance tuning to optimize speed** of entity resolution processing. Using a systems theory approach, analyze end to end the processes in place to perform entity resolution and make recommendations to speed processing without sacrificing quality to include assumptions used in the analysis. Narratively described and where applicable code the logic used to optimize speed to include but no limited to preparation of data,

creation of indexes, tuning of SQL queries, calculation of constructed columns, and revised processing methodology. Innovate beyond modification of existing processes.

8. Recommend **proactive measures** to avoid future misses or to avoid increases in future workload. Beyond the activity above, use valid statistical methodologies to predict performance of current processes. Identify weaknesses by type of error most likely to occur and recommend measures to prevent future failures to match or excessive referrals.

9. Support **entity resolution integration** into applications or services as required for decision support systems. This includes replication of existing systems to permit real-time in parallel performance comparisons. Evaluate performance of candidate entity resolution models and processes to determine if they are appropriately superior to existing models and processes to warrant implementation in production.

10. **Measure and report results**. Use a variety of statistical metrics to generate quantified performance reports of entity resolution effectiveness and efficiency. Produce narrative descriptions, tabular data, graphical representations, and presentation materials that cover the entire entity resolution process from methodology through result to include comparative analysis of random and existing processes performance. Report results both orally and in writing to include but not limited to executive summaries and detailed written reports.

Work under this task includes documentation of adjustments made to name matching tools and results that demonstrate statistical foundation for recommended changes to increase signal/noise ratio and functional code that optimizes processes by increasing overall processing speed, accuracy. In includes recommendations to aggregate the results of multiple name matching and entity resolution tools to produce more effective and efficient results and documented logic that objectively demonstrates the value of innovation with test results on training and validation data sets.

5.6 THREAT RESEARCH SUPPORT

OIT is responsible for designing and developing threat research solutions for CBP based on requirements generated by the OI and OFO. Both OI and OFO have established requirements to design and develop more threat-specific assessment techniques that incorporate sophisticated analyses of intelligence and CBP data and the use of various machine learning techniques. Projects generically use data about potential actors, materials, behaviors, and modalities that are directed toward specific objectives that may threaten U.S. interests. The security concerns and threat objectives are provided by the government. The Contractor is given access to data element that includes information about actors, materials, behaviors and modalities. The Contractor shall integrate domain, threat and operational expertise in extracting and structuring various CBP data as well as data clustering and classification, entity resolution, data visualization, machine

learning and modeling to deliver operationally relevant and practicable threat assessment updates (i.e. rule sets, machine learning models, list of suspicious entities).

5.6.1 NEW THREAT ASSESSMENT PROJECTS

The Contractor shall complete each independent project (threat) with the submission of all findings, rules, and machine learning methods and models, code base for model and details of environment in which it was developed, specify data inputs, algorithms to process data and outputs of models, along with a recommendation for or against implementation of these concepts into the operational environment (actual implementation is not part of this scope). The Contractor shall cooperate with and assist other vendors to implement rule sets and models into production.

Activities include:

1. Conduct **threat research**. Use open source, unclassified, and classified data sources to gain a thorough understanding of new threat assessment projects and determine if there is sufficient information with respect to these activities to create rules and/or models for threat assessment.

2. Conduct **data analysis**. Perform data profiling and associated statistical analysis in preparation for presenting data to machine modeling tools. Includes structuring various CBP data, data clustering and classification, entity resolution, and data visualization.

3. Perform **machine learning**. Use a variety of machine learning tools and algorithms to identify data correlations as potential components of aggregate models. Explain in non-technical language the nature of found correlations, confidence in the results, and applicability to support mission objectives.

4. Generate **rule sets, machine learning models, and lists of suspicious entities**. Use the results of machine learning to produce rule sets, machine learning models and lists of suspicious entities. All outputs will use archived, calculated, and/or real-time data to predict actors, activities, and outcomes for identified project threats. Narratively and mathematically describe the model factors, coefficients, equation, and meaning of the probability result(s).

5. Conduct **hypothesis testing**. Establish hypotheses as logical frameworks to test rule sets and machine learning models against objective metrics of success. Run rules and models against reserved non-training data to validate model performance and to confirm/reject hypothesis.

6. Perform **variance analysis**. Use a variety of statistical analysis tools to determine the expected variability surrounding predictions in multiple dimensions including but not limited to time, location, category of actor/activity/cargo, conveyance, volume/weight/quantity/quality of materials, mode of transportation, and workload capacity. Narratively and graphically describe predicted variance, confidence of the analysis, and observed variance on reserved training or actual new data. Recommend threshold values and time periods that delineate boundaries of acceptable variability. Provide statistical verification for products.

7. Conduct **sensitivity and specificity analysis**. Use a variety of statistical analysis tools to determine the sensitivity and specificity of the rule sets and models relative to their designed/intended predictive capacity. Narratively and graphically support conclusions including but not limited to creation of population, sampling methodology, factor descriptions, and receiver operating characteristic (ROC) curves. Compare rule sets and model performance against random and existing rule sets and models' performance.

8. Support **rule set and model integration**. Work with application and user interface developers; assist in the integration of produced rule sets and models with application code to support decision support analysis.

9. **Measure and report results**. Use a variety of statistical metrics to generate quantified performance reports of project innovation, effectiveness and efficiency. Produce narrative descriptions, tabular data, graphical representations, and presentation materials that cover the entire project development process from methodology through result to include comparative analysis of random and existing threat identification and prediction performance. Report results both orally and in writing to include but not limited to executive summaries and detailed written reports.

5.6.2 OPERATIONS AND MAINTENANCE OF CURRENT THREAT ASSESSMENT PROJECTS

O&M will involve most of the activities of traditional software O&M; however the Contractor shall also need to repeat most of the threat modeling and machine learning tasks required in the creation of the original models to refresh production models.

Once a threat assessment technique has been integrated into the production targeting environment, it must then be operated and maintained. This O&M includes:

(1) Maintaining and updating threat models through regular review of open-source and classified data
- Designing and recommending rule changes based on any substantial changes in threat behavior

(2) Maintaining the relevant training set with new actual positives and, as appropriate, proxy positives (used for both rules development and machine learning) by monitoring the following:
    - Updates to Office of Foreign Assets Control (OFAC) list of Specifically Designated Nationals (SDN), other sanctions programs, prosecutions, and other sources (e.g., classified reporting) that identify new entities associated with threat activities
        i. Using entity resolution and database search techniques to identify historical transactions involving those entities in Automated Export System data
        ii. Using threat understanding to identify proxy positives

(3) Update key features and data elements used in training set

(4) Update/re-run models (using updated training set) on a semi-annual basis or when there have been substantial changes to the training set

(5) Evaluating methodologies to ensure threats, models, and rule sets maintain effectiveness and design and using objective measures and metrics to identify degradation of performance

(6) Routinely monitor performance of rules and models, including:
    - Tracking shipments and travelers recommended for inspection and recording (and assessing the significance of) inspection findings
    - Developing ROCs for rules and models on a semi-annual basis
    - Working with OI to develop mechanism for getting qualitative feedback from the intelligence and analysis community on OI referrals
    - Routinely monitor workload generated by rules and model and change rules and model as necessary to stay within workload ranges acceptable to OFO and OI

Additionally, O&M may yield any of the following work products:

(1) Updated or new rule sets for suspect entities identified during the research and analysis phase;

(2) New rule sets to target a specific subset of threat behavior; and

(3) New machine learning models to target this specific subset of behavior.

The Contractor shall be available to make changes to rules and models as requested by OI and OFO personnel based on user experience or tactical intelligence.

1. Update **rule sets, machine learning models and lists of suspicious entities**. The contractor will need to repeat the tasks identified in the new threat assessments to realize changes in threat behavior and to ensure rule set and model effectiveness.

2. Gain **qualitative feedback**. Develop mechanism to receive qualitative feedback on rule set and model referrals from OFO, OI and IC community.

3. **Measure and report results**. Use a variety of statistical metrics to generate quantified performance reports of project maintenance innovation, effectiveness and efficiency. Produce narrative descriptions, tabular data, graphical representations, and presentation materials that cover the entire project maintenance process from methodology through results to include analysis of performance changes, whether degradation or improvements. Report results both orally and in writing to include but not limited to executive summaries and detailed written reports.

5.7 VISUALIZATION

The Contractor shall provide visual representation of key performance indicators which allows analysts to visualize and comprehend vast amounts of interrelated information in graphical and spatial representation. Visualization is currently offered as a service and not as an independent application. As such, Visualization as a Service supports many data sets, user interfaces and applications, including dynamic cross domain communication.

This task is defined by the following activities:

1. Conduct **data analysis**. Perform data profiling and associated statistical analysis in preparation for presenting data to visualization data schemas. Identify data anomalies and recommend strategies for maintaining data fidelity while presenting as accurate as possible a picture of unaltered data.

2. Design, create, and **implement data loaders and extract, transform, load (ETL) processes** to accept data from various sources into a common visualization ontology.

3. Design, create, and **implement indexes to speed retrieval** of an overview of massive data sets either statistically or visually, using representative sampling data where appropriate.

4. Coordinate **back end, middle tier, and user interface code** to permit visualization of any database subset through the processes of ETL, ontology mapping, grouping, filtering, and user-driven selection for presentation based upon entity types, entity attributes, location, and time intervals. Use a variety of open source, COTS and custom tools to accomplish this work.

5. Develop **reference data sets**. Many visualization tasks require prior knowledge of or attribute information about various locations such as air and sea ports, time zones, country boundaries, etc. Given standards for reference data, locate, aggregate, enter, and verify reference data in support of visualization needs across the globe.

6. Develop **generic visualization services** in support of the above. This includes but is not limited to design, creation, population, and maintenance of geo-coding, geo-mapping, and entity-relation ontologies. Work modularly to maximize ability to address new visualization needs as data, threats, and relationships change.

7. Address **big data challenges**. Large data sets are difficult to visualize comprehensively on a globe. Use a variety of data sampling, clustering, and visual representation techniques to accurately represent huge data sets over all time, globally, while allowing rapid filtering and selection to subsets of data users wish to see. Use state of the art techniques to move from all data to specific subsets that enable rapid decision-making or provide visual insight into specific threat-related data. This includes temporal, locative, and relational perspectives across all data holdings, globally, and any entity relations.

8. **Measure and report results**. Use a variety of metrics to generate quantified and qualified performance reports of visualization innovation, effectiveness, efficiency, aesthetics, and user satisfaction. Produce narrative descriptions, tabular data, graphical representations, and presentation materials that cover the entire visualization process from data capture through visual interface and navigation. Describe methodology to include comparative analysis of alternate and existing visualization capabilities by producing report results both orally and in writing; to include but not limited to executive summaries, detailed written reports, and interactive demonstrations of visualization capabilities, with emphasis on innovation that enables more effective workflow and mission accomplishment. Primary measures of visualization performance are usability, navigation speed to desired information or perspective, and visual presentation speed (refresh rates).

5.8 QUERY SUPPORT

The Contractor shall provide query support on big data platforms to support a growing demand in the number of users, quantity of requests, and complexity of queries for intelligence analysis. This includes searching and analyzing data stores, querying and extracting information and running impact assessments.

This task is defined by the following activities:

1. **Gather requirements**. Apply experience, critical thinking, and exceptional communication skills to capture data request requirements. Clarify ambiguities in advance whenever possible. Identify and use previous analogous requirements and query scripts to maximize efficiency and effectiveness.

2. **Analyze data**. Demonstrate expertise in understanding large, complex, and possibly undocumented or unrelated databases, data schema, reference data, joining conditions, relationships, and use of these data to respond to requests.

3. Analyze **business logic**. Demonstrate expertise in applying business logic to data structures and requests to ensure query results conform to business rules and the specifics of the request.

4. Write **query code**. Design, create, run, save, edit, organize, store, comment, retrieve, and document queries using SQL and other languages.

5. Optimize **query speed**. In coordination with database experts, modify queries and scripts to optimize speed on available computing resources and within constraints of other users' needs for those same resources. Demonstrate agility in rapidly changing the priority of operation for running queries to meet exigent circumstances. Design, create, and maintain indexes as appropriate. Provide hints for queries as needed to ensure consistent performance under tight time constraints.

6. Work on **big data platforms**. This may include but not be limited to Oracle Exadata, and large Hadoop cluster platforms.

7. **Document** query requests, business logic, data sources used, query logic, query scripts, key performance measures, and persons involved.

8. Conduct **impact assessments** for hypothetical scenarios such as implementation of rules, new data sources, increased data loads, or new data transaction types.

9. **Increase efficiency**. Through analysis of historical and ongoing requests and results, identify common requests and methods for increasing service efficiency and effectiveness. Consider alternative means of improving service support beyond query speed to include but not limited to standardization, definitions, training, self-service interfaces, and improving data quality and relational integrity.

10. **Measure and report results**. Use a variety of statistical metrics to generate performance reports of query requests received, in-process, and completed. Include quantitative measures to include but not limited to the original data request and all variants whether initiated by the requester or by the query expert during data discovery, query, and results validation. Include qualitative measures of query results in terms of user satisfaction and need to repeat queries to address quality issues. Track request processing using Kanban and other methods. Produce narrative descriptions, tabular data, graphical representations, and presentation materials that cover the entire query service process from receipt through results delivery and follow-up to include comparative analysis of

previous performance. Report results both orally and in writing to include but not limited to executive summaries, updating tracking boards, and detailed written reports.

6 DELIVERABLES AND DELIVERY SCHEDULE

The Contractor shall submit the deliverables that are indicated in the tables below to the COR and any other appropriate Government team leads.

6.1 DELIVERABLE SCHEDULE

Deliverable ID	Task	Description of Deliverable	Deliverable Date/Time Frame
0001	5.1	Security Plan	No later than 5 days following contract award
0002	5.4	Draft Incoming Transition Plan	Due with proposal
0003	5.1	Post-Award Kick-off Meeting	No later than 5 days following contract award
0004	5.1	Quality Control Plan	No later than 5 days following contract award
0005	5.1	Final Revised Incoming Transition Plan	No later than 5 days following Kick-off Meeting
0006	5.1	Submission of all CBP BI Packages	No later than 5 days following contract award
0007	5.1	Weekly Status Reports and Meetings	Weekly
0008	5.1	Contract Staff Training Requirements	As Required; To be reported by the 1st and 15th day of each month.
0009	5.1	Ad-hoc reports	As Required
0010	5.1	Outgoing Transition Plan	365 days prior to the end of the period of performance
0011	5.2	Research summary reports, social network diagrams, network analysis	As Required

		reports, query request logs, SQL scripts, data extracts.	
0012	5.2	Data visualization tool enhancements.	Sprint cycles of 2 weeks
0013	5.3	Reports on data analysis, machine learning, model integration	As Required
0014	5.3	Predictive models including hypothesis testing, variance analysis reports and sensitivity and specificity analysis reports	A minimum of one new and refreshed model per month
0015	5.3	Summary report	Quarterly
0016	5.4	Quarterly National Security Inbound (NSI) Model Performance Evaluation and Assessment for Air Cargo	NLT 30 business days following the end of the current quarter
0017	5.4	National Security Inbound (NSI) Model Performance Evaluation and Assessment for Maritime Cargo	NLT 30 business days following the end of the current quarter
0018	5.4	National Security Inbound (NSI) Model Performance Evaluation and Assessment for Truck Cargo	NLT 30 business days following the end of the current quarter
0019	5.4	National Security Inbound (NSI) Model Performance Evaluation and Assessment for Rail Cargo	NLT 30 business days following the end of the current quarter
0020	5.4	National Security Inbound (NSI) Model Performance Evaluation and Assessment for Air Cargo Advance Screening (ACAS) Cargo	NLT 30 business days following the end of the current quarter
0021	5.4	ENTITY RESOLUTION CODE DEVELOPMENT	As Required
0022	5.4	THREAT RESEARCH REPORTS	As needed, average monthly, surge to prioritize emergent threats
0023	5.6	Development and recommendations,	Quarterly for each model

		integration and maintenance reports	

6.1.1 SECURITY PLAN

The Contractor shall be responsible for ensuring that the contractor team complies with contract security requirements and sensitive information protection policies, including ensuring that all personnel have the appropriate level of clearances. The Contractor shall deliver an IT Security plan to the Government outlining their plan to comply with the Government's administrative, physical and technical security controls.

6.1.2 INCOMING TRANSITION PLAN

The Contractor's proposal shall include a draft Incoming Transition Plan for the transition from the incumbent to the Contractor. The Contractor shall coordinate with the Government in planning and implementing a complete transition to the Contractor's proposed support model. The Government has designated a transition period for the incoming Contractor to coordinate and work with the incumbent Contractor. The Contractor shall assume support responsibilities in accordance with its Incoming Transition Plan, processes, procedures, and schedule. The Incoming Transition Plan shall include, at a minimum:

- Overview of the transition effort;
- A detailed summary of all transition events and estimated milestone dates. The transition timeline shall be presented as a schedule in graphic format showing the timing, sequence and interdependencies of tasks. The transition schedule shall be supplemented by narrative, as needed to provide a clear understanding of the transition plan.
- Submission of all available CBP BI packages;
- Date by which the Contractor will have sufficient, properly trained personnel to meet all Government PWS requirements;
- Coordination with Government representatives;
- Risks associated with the transition and the Contractor's plan to mitigate such risks and contingency plans in the event the transition cannot be executed on schedule.
- Review, evaluation and transition of current support services;
- Transfer of all necessary business and/or technical documentation to the COR;
- Identification of the principal Incoming Transition team members by name, position, start date, and responsibilities;
- A work plan that identifies milestones, measurable tasks, and resources required; and
- A plan for executing redundant performance with the outgoing contractor upon successful completion of knowledge transfer.

A Final Revised Incoming Transition Plan is due five (5) business days after contract award.

6.1.3 QUALITY CONTROL PLAN

The Contractor shall have an established, maintained, and effective Quality Management System (QMS) that ensures quality products and services are delivered to the Government. The Quality Control Plan shall describe the QMS in sufficient detail to permit an assessment of the contractor's QMS by the Government. The Quality Control Plan shall describe the Contractor's approach to meeting the quality, timeliness, responsiveness, customer satisfaction, and other product and service delivery requirements.

6.1.4 WEEKLY STATUS REPORTS

The contractor will provide regular communication of project status through weekly status reports and weekly face-to-face status meetings between the team, the COR, the CBP government leads and any other stakeholders as identified by the Government.

The Contractor shall provide the COR with a weekly report, for each task in section 4.0 with an overview of work accomplished the previous period and work scheduled for the upcoming week. This report shall contain the following information at a minimum:

- Planned activities and desired results for the next reporting period with milestones and deliverables;
- Issues and risks affecting technical, schedule, or cost elements of the contract, including background, impact and recommendations for resolution;
- Results related to previously identified problem areas with conclusions and recommendations;
- Team organizational chart.

6.1.5 CONTRACTOR STAFF TRAINING

All contract personnel are required to complete the DHS/CBP mandatory Virtual Learning Center (VLC) training courses by the mandatory due date(s). The Contractor is responsible for maintaining records of contracting employees that have completed the mandatory training and provide semimonthly updates to the COR on the 1st and 15th day of each month or the next business day if the 1st or 15th is a Holiday or on the weekend. The Contractor is also responsible for providing copies of the training certificates to the COR when requested.

6.1.6 CONTRACTOR OUTGOING TRANSITION PLAN

At the completion of performance of this task order, the Contractor shall fully support the transition of the Contractor's work that is turned over to another entity, either Government or a

successor offeror(s). The Contractor shall assist with transition planning and shall comply with transition milestones and schedules of events.

The Contractor shall be responsible for the implementation of the transition and application cutover activities. The transition shall cause no disruption of services. To ensure the necessary continuity of services and to maintain the current level of support, the Government may retain services of the incumbent Contractor for some, or all of, the transition period, as may be required.

The Contractor shall be responsible for the transition of all technical activities identified in this task order. 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, and Government Furnished Information (GFI) to include
- Transfer of documentation currently in process
- Transfer of all software code in process
- Certification that all non-public DHS information has been purged from any Contractor-owned system
- Exchange of accounts to access software and hosted infrastructure components
- Participate in knowledge transfer activities in accordance with the transition plan
- Provide members to and participate in transition management
- Identify transition risks and risk mitigation

The Contractor shall submit a Transition Out Plan. The Transition Out Plan shall include support activities for all transition efforts for follow-on requirements to minimize disruption of services. The Transition Plan shall:

- Identify equipment, hardware, software, documents and other artifacts that are included in the transition
- Establish roadmap and backlog
- Identify transition risks and risk mitigation
- Define roles and responsibilities
- Define transition approval authorities and lines of communication
- Define a knowledge transfer approach
- Define a property inventory and transition approach
- Provide checklists

A Transition Plan shall be delivered 365 days prior to the task order expiration date. The Contractor shall account for a 10 business day Government review process prior to executing the transition. Upon award of a follow-on contract, the incumbent Contractor will work with the new Contractor to provide knowledge transfer and transition support, as required by the COR.

6.1.7 SUMMARY REPORT

The Contractor shall provide the COR with a summary report of all predictive modeling work quarterly. A single report will provide an executive summary of each model, regardless of development stage, from inception through maintenance. The report shall contain the following at a minimum:

- Name and brief description of each model
- Current development category / status
- Work accomplished since the last reporting period
- Work planned for the forthcoming reporting period
- Model performance since the last reporting period
- Model performance trend since deployment to include seasonality, improvement or degradation (for those models in testing/production only)
- Summary of feedback received from business owners
- Recommendations for development, refresh, replacement, or retirement of any model(s)
- Recommendations for prioritization of work

6.1.8 BASELINE PERFORMANCE REPORT

The Contractor shall provide the COR with a baseline performance report of all existing national security proxy positives quarterly, within 60 days of the end of each calendar quarter. A single report will provide an executive summary of each proxy as well as detailed information about specific performance. The report shall contain the following at a minimum:

- Name and brief description of each proxy
- Metric used to evaluate the proxy
- Statistical analysis of proxy performance, to include confidence
- Recommendations for innovation to improve performance

6.1.9 NSI MODEL PERFORMANCE EVALUATION FOR AIR CARGO REPORT

The Contractor shall provide the COR with a quarterly report of National Security Inbound (NSI) Model performance report for the Air Cargo mode of transportation as an objective assessment of NSI performance and effectiveness to aid CBP in meeting GAO and congressional reporting requirements. A single report will provide an executive summary of model target volume and distribution of targets across key operational targeting attributes. The report shall contain the following at a minimum:

- Name and description of each model
- Total volume in subject mode of transportation compared to operational baseline

- Distribution of model total target volume by model targeting threat category/area (e.g., Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE), Anomaly Detection)
- Total exams and holds associated with NSI target volume
- Breakdown/Visualization of countries of origin and geographic distribution of model targets
- Prior Quarter model performance/volume comparison

6.1.10 NSI MODEL PERFORMANCE EVALUATION FOR MARITIME CARGO REPORT

The Contractor shall provide the COR with a quarterly report of National Security Inbound (NSI) Model performance report for the Maritime Cargo mode of transportation as an objective assessment of NSI performance and effectiveness to aid CBP in meeting GAO and congressional reporting requirements. A single report will provide an executive summary of model target volume and distribution of targets across key operational targeting attributes. The report shall contain the following at a minimum:

- Names and description of each model
- Total volume in subject mode of transportation compared to operational baseline
- Distribution of model total target volume by model targeting threat category/area (e.g., Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE), Anomaly Detection)
- Total exams and holds associated with NSI target volume
- Breakdown/Visualization of countries of origin and geographic distribution of model targets
- Prior Quarter model performance/volume comparison

6.1.11 NSI MODEL PERFORMANCE EVALUATION FOR TRUCK CARGO REPORT

The Contractor shall provide the COR with a quarterly report of National Security Inbound (NSI) Model performance report for the Truck Cargo mode of transportation as an objective assessment of NSI performance and effectiveness to aid CBP in meeting Government Accountability Office (GAO) and congressional reporting requirements. A single report will provide an executive summary of model target volume and distribution of targets across key operational targeting attributes. The report shall contain the following at a minimum:

- Names and description of each model
- Total volume in subject mode of transportation compared to operational baseline

- Distribution of model total target volume by model targeting threat category/area (e.g., Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE), Anomaly Detection)
- Total exams and holds associated with NSI target volume
- Breakdown/Visualization of countries of origin and geographic distribution of model targets
- Prior Quarter model performance/volume comparison

6.1.12 NSI MODEL PERFORMANCE EVALUATION FOR RAIL CARGO REPORT

The Contractor shall provide the COR with a quarterly report of National Security Inbound (NSI) Model performance report for the Rail Cargo mode of transportation as an objective assessment of NSI performance and effectiveness to aid CBP in meeting GAO and congressional reporting requirements. A single report will provide an executive summary of model target volume and distribution of targets across key operational targeting attributes. The report shall contain the following at a minimum:

- Names and description of each model
- Total volume in subject mode of transportation compared to operational baseline
- Distribution of model total target volume by model targeting threat category/area (e.g., Chemical, Biological, Radiological, Nuclear, and Explosive [CBRNE], Anomaly Detection)
- Total exams and holds associated with NSI target volume
- Breakdown/Visualization of countries of origin and geographic distribution of model targets
- Prior Quarter model performance/volume comparison

6.1.13 NSI MODEL PERFORMANCE EVALUATION FOR AIR CARGO ADVANCE SCREENING (ACAS) CARGO REPORT

The Contractor shall provide the COR with a quarterly report of National Security Inbound (NSI) Model performance report for the Air Cargo Advance Screening (ACAS) Cargo mode of transportation as an objective assessment of NSI performance and effectiveness to aid CBP in meeting GAO and congressional reporting requirements. A single report will provide an executive summary of model target volume and distribution of targets across key operational targeting attributes. The report shall contain the following at a minimum:

- Names and description of each model
- Total volume in subject mode of transportation compared to operational baseline
- Distribution of model total target volume by model targeting threat category/area (e.g., Chemical, Biological, Radiological, Nuclear, and Explosive [CBRNE], Anomaly Detection)
- Total exams and holds associated with NSI target volume

- Breakdown/Visualization of countries of origin and geographic distribution of model targets
- Prior Quarter model performance/volume comparison

6.1.14 THREAT RESEARCH REPORT

The Contractor shall provide the COR with a quarterly threat research report. The report shall contain the following at a minimum:

- Threat being addressed
- Methodology used to identify factors
- Data source(s) used to identify relevant data, actors, activities, scenarios
- Value to work already in progress or proposed work
- Recommendations for prioritization of work to move from research to threat scenario development, data analysis, and hypothesis testing

6.1.15 DEVELOPMENT AND RECOMMENDATIONS, INTEGRATION, AND MAINTENANCE REPORTS

The Contractor shall provide the COR with a quarterly report for all models / rule sets not already in production. The report shall contain work done to date and status of model development to include as applicable:

  - Data analysis
  - Machine Learning
  - Rule Set Development
  - Hypothesis Testing
  - Data source(s) used to identify relevant data, actors, activities, scenarios
  - Statistic derived from Variance, Sensitivity, and Specificity Analysis
- Recommendations for prioritization of work to move to integration / deployment

This report shall also include integration status for all models or rule sets approved for integration but not yet in production. The report shall contain the following at a minimum:

- Model / Rule Set name
- Integration Task List / Schedule
- Work accomplished since last report
- Recommendation to proceed, reprioritize, or abandon work

The report shall also cover maintenance status for all models / rule sets already in production. The report shall contain the following at a minimum:

- Threat being addressed
- Model / Rule Set name
- Performance measurement used
- Trend analysis since deployment
- Recommendation to collect further data, conduct maintenance, replace, or retire the model/rule set.

7 PLACE OF PERFORMANCE AND HOURS OF OPERATION

7.1 PLACE OF PERFORMANCE

U.S. Customs and Border Protection (CBP) will provide space in multiple facilities for the on-site contractor staff to perform the required tasks in the Washington DC Metro area; however, most work is performed at site (a) below. Other locations for this work are below, although other Washington DC area offices may be occasionally used. All work required under this contract shall be performed by the Contractor at Government sites unless otherwise directed by the Government. Travel to other Washington DC area Government locations may be necessary.

(a) OIT, Kingstowne Facility, Alexandria, VA 22315
(b) OIT, Herndon Facility, Herndon, VA 20170
(c) Ronald Reagan Building, 1300 Pennsylvania Ave, NW, Washington, DC 20229
(d) OIT, Ashburn Facility, Ashburn, VA 20147
(e) Data Center, Newington, VA
(f) National Targeting Center, Sterling, VA 20164
(g) Walker Lane Facility, Alexandria, VA 22310
(h) Beauregard Facility, Alexandria, VA 22311

7.2 HOURS OF OPERATION

For those contractor personnel working in direct support of TASPD, the normal business hours are 7:00 am to 6:00 pm (EST), Monday through Friday with core business hours between 8:00 am and 5:30 pm each business day. The Contractor shall ensure coverage of these core hours for those in direct support of the TASPD. TASPD and those directly supporting TASPD will recognize all official federal holidays. However, all TASPD computer and software applications support a 24/7/365 mission requirement and the contractor shall ensure system application performance standards are maintained over the full range of mission operations. Due to the nature of the work, overtime is authorized under this PWS, however all overtime must be requested in advance and approved by the COR and Contracting Officer. The Contractor must provide a central point of contact to reach the necessary staff in the event of system problems or emergencies. If required by the COR or Government Team Lead, the contractor's staff shall report on-site after normal hours to address system problems.

8 GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION

(a) The Government will furnish only that equipment necessary for the Contractor to carry out its work efforts under this PWS at the Government facility. This includes normal workspace accommodations such as desk, chair, desk phone, and computer. While performing work under this PWS in Government facilities, the Contractor may have the use of other normal office EIT devices, such as fax machines (not classified), copiers, projectors, etc. It is required that the contractor obtain CBP Personal Identity Verification (PIV) cards as they are necessary to log into all computers and laptops.

(b) The Government will provide to the Contractor cell phone, laptop, or other portable devices upon the written consent of the COR justifying the need for such equipment.

(c) The Government will furnish all necessary related documentation in its possession that may be required for the Contractor to perform this contract.

9 PERSONNEL SECURITY AND CLEARANCES

All members of the project team must obtain CBP Suitability to begin work. Reference 5 CFR Part 731, "Suitability." Some of personnel under certain tasks will potentially need to possess a Top Secret Security Clearance with access to SCI in order to research and review (Classified) threat information. When a security clearance of secret or higher is required in performance of the order, a completed DD Form 254 is required. The following number of personnel under each task will need to either possess a TS or TS/SCI.

Task	Task Description	Minimum Quantity of TS Personnel Required	Minimum Quantity of TS/SCI Personnel Required
4.1	Project Management	1	0
4.2	Intelligence Analysis-Counterterrorism-Social Networking	0	5
4.3	Predictive Modeling	2	0
4.4	Proxy Positives	2	0

4.5	Entity Resolution	2	0
4.6	Threat Research Support	0	4
4.7	Visualization	2	0
4.8	Query Support	2	0

10 INSPECTION AND ACCEPTANCE

The Government reserves the right to reject any deliverable based on defects with respect to completeness, correctness, clarity and logical consistency. In the event of a rejection of any deliverable, the COR will notify the Contractor in writing within five (5) business days of the receipt of the deliverable of any deficiencies to be corrected. The Contractor shall have five (5) business days to correct the deficiencies.

- Accuracy – all deliverables shall be accurate in presentation, content, and shall adhere to the requirements set forth in this document. All documentation presented to the Government shall be complete, correct, clear, and consistent.

- Clarity – deliverables shall be clear and concise.

- Timeliness – deliverables shall be submitted on or before the due date specified in the Performance Work Statement or submitted in accordance with a later scheduled dated mutually agreed upon by the Government and contractor. A deliverable is considered timely if submitted on or before the date specified in the Performance Work Statement and, and if the Government provides any written notifications of deficiencies, the contractor corrects the deficiencies within five (5) business days.

11 PERSONALLY IDENTIFIABLE INFORMATION (PII)

When a Contractor, on the behalf of CBP, handles Sensitive PII data, stores and transmits, the Contractor shall Accredit (ATO) this information system to the High, High, Moderate (HHM) FIPS level.

D.1 RESERVED.

E.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed by the COR and TASPD TPOC at TASPD locations.

E.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the COR and TASPD TPOC. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE ~~1~~5 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

The final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the quality assurance requirements stated within this TO, the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the COR.

E.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within ~~1~~5 workdays (unless specified otherwise in Section F) from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have five~~ten~~ workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The CO or COR will provide written notification of acceptance or rejection of all final deliverables within ~~1~~5 workdays. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.6 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies shall be corrected, by the contractor, within five~~ten~~ workdays of the rejection notice. If the deficiencies cannot be corrected within five~~ten~~ workdays, the contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within five~~ten~~ workdays.

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the contractor performance assessment reporting system (CPARS).

F.1 PERIOD OF PERFORMANCE

Each Award will consist of two (2) task orders (TOs). The first TO will have a period of performance of one (1) year and be for transition in. The second TO will have the following period of performance and be for requirements execution:

TASK ORDER TRANSITION:

Base Period: Up to Twelve (12) months (note: flexible end date)

TASK ORDER REQUIREMENTS EXECUTION:

Base Period: Twelve (12) months from Effective Date

Option Period 1: Twelve (12) months

Option Period 2: Twelve (12) months

Option Period 3: Twelve (12) months

Option Period 4: Twelve (12) months

F.2 PLACE OF PERFORMANCE

The duty station is defined as the authorized place of performance for the work of this TO. The primary Places of Performance can be located in PWS. Occasional/ad-hoc telework is permissible through coordination with Government program leads.

In January 2021 - date subject to change - CBP OIT plans to relocate several National Capital Region operations to Ashburn, VA.

F.3 TASK ORDER SCHEDULE AND MILESTONE DATES

The following schedule of milestones will be used by the COR to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

DEL: Deliverable
IAW: In Accordance With
NLT: No Later Than
TOA: Task Order Award
All references to days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

Data Rights Clause - Abbreviations in the Gov't Rights column of the table below shall be interpreted as follows:

UR: Unlimited Rights, per FAR 27.404-1(a) and 52.227-14

RS: Restricted Software, per FAR 27.404-2 and 52.227-14

LD: Limited Rights Data, per FAR 27.404-2 and 52.227-14

SW: Special Works, per FAR 27.405-1 and 52.227-17

F.4 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a Portable Document Format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA (Section F, Deliverable 33). The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S. Code (U.S.C.) § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

CBP will carefully consider the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by electronic mail (email) and removable electronic media. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

a. Text	MS Word, Google Docs, PDF
b. Spreadsheets	MS Excel, Google Sheets
c. Briefings	MS PowerPoint, Google Slides
d. Drawings	MS Visio, Google Drawings
e. Schedules	MS Project, Smartsheet, or other Government-approved media

F.6 PLACE(S) OF DELIVERY

Copies of all deliverables shall be delivered to the COR at the following address:

[To be provided upon contract award]

Copies of all deliverables shall also be delivered to the TASPD TPOC. The DHS TASPD TPOC name, address, and contact information will be provided at award.

F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the COR via a Problem Notification Report (PNR) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

G.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The CO appointed a COR in writing through a COR Appointment Letter. The COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the Contract or the TO.

G.1.1 CONTRACT ADMINISTRATION

CO:

Provided at award.

COR:
Provided at award.

TASPD TPOC:
Provided at award.

G.2 INVOICE SUBMISSION

ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: https://www.ipp.gov.

Under this contract, the following documents are required to be submitted as an attachment to the IPP*:*

-__Invoices_____

-__Signed Time Cards_____

-_____

-_____

-_____

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

G.3 INVOICE REQUIREMENTS

The contractor shall submit a draft copy of an invoice backup in Excel to ~~the COR~~the COR and TASPD TPOC for review prior to its submission to IPP. The draft invoice shall not be construed as a proper invoice in accordance with FAR 32.9.

Each contract type shall be addressed separately in the invoice submission. Receipts shall be provided on an as requested basis.

The contractor shall submit invoices on a monthly basis for costs incurred. . The contractor shall notify the COR if circumstances require the delay of invoices beyond one month.

The final invoice is desired to be submitted within six months of project completion. Upon project completion, the contractor shall provide a final invoice status update monthly.

Regardless of contract type, the contractor shall report the following metadata:

a. GWAC Contract Number.
b. TOA Number (NOT the Solicitation Number).
c. Contractor Invoice Number.
d. Contractor Name.
e. POC Information.
f. Current period of performance.
g. Amount of invoice that was subcontracted.

The amount of invoice that was subcontracted to a small business shall be made available upon request.

G.3.1 TIME AND MATERIALS (T&M) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the T&M CLINs. The invoice shall include the period of performance covered by the invoice (all current charges shall be within the active period of performance) and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The

listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees).
b. Employee company.
c. Exempt or non-exempt designation.
d. Employee Alliant 2 labor category.
e. Current monthly and total cumulative hours worked.
f. Direct Labor Rate.
g. Effective hourly rate (e.g., cumulative costs/cumulative hours).
h. Current approved billing rate percentages in support of costs billed.
i. Itemization of cost centers applied to each individual invoiced.
j. Any cost incurred not billed by CLIN (e.g., lagging costs).
k. . The invoice detail shall be organized by CLIN.

G.3.2 OTHER DIRECT COSTS (ODCs)

The contractor may invoice monthly on the basis of cost incurred for the Tools and ODC CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

a. ODCs purchased.
b. Request to Initiate Purchase (RIP) or Consent to Purchase (CTP) number or identifier.
c. Date accepted by the Government.
d. Associated CLIN.
e. Project-to-date totals by CLIN.
f. Cost incurred not billed by CLIN.
g. Remaining balance of the CLIN.

G.3.3 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulation (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
b. Joint Travel Regulations (JTR) Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, “Maximum Travel Per Diem Allowances for Foreign Areas” - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR/FTR/DSSR. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN. The current invoice period's travel details shall include separate columns and totals and include the following:

a. Travel Authorization Request number or identifier, approver name, and approval date.
b. Current invoice period.
c. Names of persons traveling.
d. Number of travel days.
e. Dates of travel.
f. Number of days per diem charged.
g. Per ~~diem~~Diem rate used.
h. Total per diem charged.
i. Transportation costs.
j. Total charges.
k. Explanation of variances exceeding ten percent of the approved versus actual costs.
l. Indirect handling rate.

G.4 TASK ORDER (TO) CLOSEOUT

The Government will unilaterally close out the transition and requirements TOs NLT six years after the end of each TO period of performance if the contractor does not provide final invoice by that time.

H.1 RESERVED

H.2 GOVERNMENT-FURNISHED PROPERTY (GFP)

The contractor shall institute property control and accountability procedures to safeguard and maintain all GFP, including Contractor Acquired Property (CAP), in accordance with FAR 52.245-1 and DHS 4300 A. The contractor shall report any loss or damage of Government Property to the TASPD TPOC and the COR. The contractor shall submit a Full Incident Report for any loss and damages. All GFP shall be accounted for and signed for by a designated contractor employee at each performance site. These designated contractor personnel shall also be accountable for inventory requirements and loss of or damage to GFP in accordance with FAR 52.245-1, Government Property.

H.3 GOVERNMENT-FURNISHED INFORMATION (GFI)

The contractor shall use GFI, data, and documents only for the performance of work under this TO, and shall return all GFI, data, and documents to the Government at the end of the performance period. The contractor shall not release GFI, data, and documents to outside parties without the prior and explicit consent of the CO.

H.4 SECURITY

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

H.4.1 CONTRACTOR PRE-SCREENING

Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to IT resources shall verify minimal suitability requirements, as described below, for all persons/candidates designated for employment under any CBP contract by pre-screening the person/candidate prior to submitting the name for consideration to work.

Pre-screening the candidate ensures that minimum suitability requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Candidates shall also be submitted for a financial background check. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:

a. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).
b. Illegal drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self-certification, by public records check; or, if the contractor or subcontractor already has drug testing in place. There is no requirement

for contractors and/or subcontracts to initiate a drug testing program if they do not have one already in place.

c. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self-certification, by public records check, or other reference checks conducted in the normal course of business.
d. Financial irresponsibility related to tax liens and bankruptcy within the last seven to ten years. An acceptable means of obtaining information related to financial irresponsibility is through a financial background check.

Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources.

Failure to comply with the pre-screening requirement will result in the CO taking the appropriate remedy.

H.4.2 CBP BACKGROUND INVESTIGATION (BI)

A BI is required for performance under this effort. Contractor employees and sub-contractors shall not begin working until, at a minimum, an interim or partial BI is approved by CBP. The citizenship requirements for accessing CBP systems and granting CBP BIs are outlined in CBP OIT Handbook 1400-05D, Section 4.1.1. Exceptions to this requirement, such as granting access to certain systems with a “limited” or “partial” BI, or authorizing work of any kind without a limited or partial BI, will be handled on a case-by-case basis, and access to facilities, systems, and data will be limited until the individual is cleared. Should clearance requirements beyond a CBP BI (e.g., Secret or Top Secret) be needed, a modification will be issued to add this requirement to the Key Personnel, or any contractor personnel, identified as needing such requirement.

All personnel employed by or sub-contracted to the contractor or responsible to the contractor for work performed hereunder shall either currently possess or be able to favorably pass a full BI as required by CBP policies and procedures prior to beginning work with CBP. This policy applies to any personnel who will perform work on this TO. Executive Order 13467 allows for the acceptance of “suitability reciprocity” to contractor personnel who are component employees within DHS.

Within five (5) business days after the contract kick-off meeting, the TASPD BI Process Coordinator (BIPC) will send the blank BI forms to the TOPM. These forms, which comprise the “BI package”, include:

- CBP Form 77 (Contractor Employee Initial Background Investigation);
- CBP Form 0078 (Background Investigation Requirements Document, or BIRD);
- Fair Credit Reporting Act (FCRA) form; and
- CBP Non-Disclosure Agreement (NDA) form.

The contractor TOPM (or designated contractor representative) is responsible for completing (pre-filling) sections on these forms that pertain to the contract, such as contract number, duty address, work phone numbers, and TASPD TPOC name. The contractor is responsible for providing these forms to any new employees and sub-contractors proposed for this TO at any

time throughout the period of performance of this TO for those individuals to complete the remainder of the information on the forms. After completion of the forms by the proposed contractor or sub-contractor, the TOPM shall review the package for completeness and forward the BI package to the TASPD BIPC.

The TASPD BIPC will review the submitted BI package for completeness and accuracy and will obtain the TASPD TPOC's signature on the Form 77. Once signed, the TASPD BIPC will submit the BI package to the CBP eQIP coordinator. The TASPD BIPC will retain a copy of the package in an electronic filing system.

The eQIP coordinator will review the BI package for completeness. If there are errors or missing information, the application will be rejected and returned to the contractor employee BI candidate for revisions, with notifications going to the TASPD TPOC, TASPD BIPC, and TOPM (or their designated contractor representative). The BI candidate shall make the necessary revisions and resubmit the BI package to the TASPD BIPC to route back to the eQIP coordinator.

Once the eQIP coordinator determines that the BI package is error-free, and if the BI candidate holds a current clearance, the eQIP coordinator will work with CBP's Office of Professional Responsibility (OPR) to determine if the contractor BI candidate is reciprocity-eligible. If the candidate is eligible for reciprocity, the candidate and the TOPM will be notified, and no eQIP or fingerprint cards will be needed. The reciprocity eligibility process can take 30 days or more.

If no reciprocity exists, or the candidate is otherwise not eligible for consideration for reciprocity, the eQIP coordinator will send the contractor BI candidate an email requesting them to complete the eQIP application. At the same time, the eQIP coordinator will send the BI candidate a set of fingerprint cards (form FD-258) to be completed. The BI candidate can complete the fingerprint cards at a local police department or CBP badging office. The BI candidate is responsible for sending the fingerprint cards to the eQIP coordinator via tracked mail if they are not completed at a CBP badging office.

After receipt of the fingerprint cards, the eQIP coordinator will review the eQIP application. The application must be submitted no later than 30 days after the initial eQIP invite, or else it will be rejected. If the eQIP coordinator finds incomplete sections or errors, the eQIP application will be rejected back to the BI candidate to address (with notifications to the TASPD TPOC, TASPD BIPC, and TOPM). The BI candidate shall correct any errors or incomplete sections and resubmit the eQIP directly back to the eQIP coordinator in the eQIP system.

Once the eQIP coordinator has determined that the eQIP application is complete and error-free, the eQIP application and fingerprint cards will be sent to OPR for the BI process to begin. It can take up to three (3) months to obtain a limited or partial BI. The full BI clearance has historically averaged six (6) months; however, the full BI clearance can take up to 9-12 months depending on the candidate and the volume of BIs being processed. Failure of any contractor personnel to successfully pass a full BI shall be cause for the candidate's immediate dismissal from the project and replacement by a similar and equally qualified candidate. This policy also applies to any personnel hired as replacements during the term of the TO.

H.4.3 CLEARANCES

Contractor personnel under this TO require a CBP BI. Some personnel may require Secret and

Top Secret clearances.

H.4.4 IDENTIFICATION BADGES

All contractor employees shall be required to wear CBP identification badges at all times when working in Government facilities.

H.4.5 PHYSICAL AND IT SECURITY REQUIREMENTS

The contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel shall be responsible for physical security of work areas and CBP furnished equipment issued under this contract.

The CO/COR may require the contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by ~~the CO~~the CO.

The contractor shall ensure that its employees, who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.

Upon completion of this contract, the contractor shall return all sensitive information used in the performance of the contract to the TASPD TPOC. The contractor shall certify, in writing, that all sensitive and non-public information has been purged from any contractor-owned system.

H.4.6 INFORMATION ASSURANCE

The contractor may have access to sensitive (including privileged and confidential) data, information, and materials of the U.S. Government. These printed and electronic documents are for internal use only and remain the sole property of the U.S. Government. Some of these materials are protected by the Privacy Act of 1974 (AMENDED) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

H.4.7 REMOTE ACCESS

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

H.4.8 HANDLING PERSONALLY IDENTIFIABLE INFORMATION (PII)

The contractor shall comply with the Privacy Act, CBP, and DHS privacy policies and procedures when handling PII. This includes reporting loss, theft, or unauthorized access to

sensitive PII within one hour of discovery and reviewing contractor applicable policies at least annually.

H.4.9 SECURITY CLEARANCES

In general, all necessary facility and employee security clearances shall be at the expense of the contractor. The contractor shall comply with all security requirements.

H.4.10 SECURITY CONTROLS

a. The contractor shall comply with the U.S. CBP administrative, physical, and technical security controls to ensure that the Government's security requirements are met.
b. All GFE/GFI shall be protected to the degree and extent required by local rules, regulations, and procedures. The contractor shall comply with all security policies contained in CBP Handbook 1400-05D, Information Systems Security Policies and Procedures Handbook.
c. All services provided under this contract shall be compliant with the DHS information security policy identified in DHS Management Directive (MD) 4300.1, IT Systems Security Program and DHS 4300A, Sensitive Systems Handbook.
b. All contractor employees under this contract shall wear identification (ID) access badges when working in CBP facilities. Prior to contractor employees' departure/separation, all badges, building passes, parking permits, keys, and pass cards shall be given to the TASPD TPOC.
c. All contractor employees shall be registered in the Contractor Tracking System (CTS) database. The contractor shall provide timely start information to the Government to initiate the CTS registration. Other relevant information will also be needed for registration in the CTS database such as, but not limited to, the contractor's legal name, address, brief job description, labor rate, Hash ID, schedule, and contract-specific information. Government personnel shall provide the contractor with instructions for receipt of CTS registration information.
d. The contractor shall provide employee departure/separation dates to the TASPD TPOC in accordance with CBP Directive 51715-006, Separation Procedures for Contractor Employees. Failure by the contractor to provide timely notification of employee departure/separation in accordance with the contract requirements shall be documented and considered when Government personnel complete a contractor performance review or other performance-related measures

H.4.11 DHS SPECIAL CLAUSE - SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(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, SSN, 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-PII can become PII 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, 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, U.S.C. (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 DHS (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 DHS (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: SSN, driver's license or state ID 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 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 CO including, but not limited to, the following:

(1) DHS MD 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 SPII

(6) DHS Instruction Handbook 121-01-007 DHS 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) 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) DHS policies and procedures on contractor personnel security requirements are set forth in various 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 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 DHS 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, DHS 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 COR NLT two 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 ATO signed by the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three 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 RTM and Government security documentation templates. SA documentation consists of the following: SP, Contingency Plan, Contingency Plan Test Results, CMP, Security Assessment Plan, SAR, and ATO 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 TASPD TPOC for acceptance by the Headquarters or Component CIO, or designee, at least 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 CO 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 the 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 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 PMPs 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 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 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 IA 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 TASPD TPOC 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 CO and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to 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 CO 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 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 CO, 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 CO’s email address is not immediately available, the contractor shall contact the CO 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 email. 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

Commercial and Government Entity (CAGE) code if the location of the event is different than the prime contractor location. (iv) POC if different than the POC recorded in the System for Award Management (address, position, telephone, email). (v) CO 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 estimated or actual number of records exposed and/or contained within the system. (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 CO 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 five business days after being directed to notify individuals, unless otherwise approved by the CO. The method and content of any notification by the contractor shall be coordinated with, and subject to prior written approval by the CO, 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 CO, 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. (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 CO: (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. (iv) Assistance to the individual with enrollment in the services and the use of fraud alerts.

(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 CO in coordination with the Headquarters or Component Chief Privacy Officer. (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 CO following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

H.4.12 DHS SPECIAL CLAUSE - IT SECURITY AND PRIVACY TRAINING (MAR 2015)

(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 DHS requires that contractor employees take an annual IT Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the 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. 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-trainingrequirements-

contractors. The contractor shall maintain copies of training certificates for all contractor and subcontractor employees as a record of compliance. The contractor shall notify ~~the COR~~the COR when the training has been completed. Subsequent training certificates to satisfy the annual training requirement shall be submitted to ~~the COR~~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 IT 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-andtraining-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within 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. The contractor shall notify ~~the COR~~the COR that the DHS Rules of Behavior have been signed by each employee not later than 30 days after contract award. The DHS Rules of Behavior will be reviewed annually and ~~the COR~~the COR will provide notification when a review is required.

(c) Privacy Training Requirements. All contractor and subcontractor employees that will have access to PII and/or 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-securityand-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. 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. The contractor shall notify ~~the COR~~the COR that the training has been completed by all applicable employees not later than 30 days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to ~~the COR~~the COR via e-mail notification not later than October 31st of each year. The email notification shall state the required training has been completed for all contractor and subcontractor employees.

H.5 UNIQUE STANDARDS

H.5.1 ENTERPRISE ARCHITECTURE (EA) COMPLIANCE

The Offeror shall ensure that the design conforms to the Department of Homeland Security (DHS) and Customs and Border Protection (CBP) Enterprise Architecture (EA), the DHS and CBP Technical Reference Models (TRM), and all DHS and CBP policies and guidelines (such as the CBP Information Technology Enterprise Principles and the DHS Service Oriented Architecture - Technical Framework), as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA).

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

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

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

All IT hardware and software shall be compliant with the HLS EA.

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

Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01. All data-related artifacts will be developed and validated according to DHS Data Management Architectural Guidelines.

Applicability of Internet Protocol version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005), regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant, as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance, defined in the USGv6 Test Program.

Compliance with DHS Security Policy Terms and Conditions

All hardware, software, and services provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.

Encryption Compliance

If encryption is required, the following methods are acceptable for encrypting sensitive information:

1. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
2. National Security Agency (NSA) Type 2 or Type 1 encryption.
3. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

Required Protections for DHS Systems Hosted in Non-DHS Data Centers

Security Authorization

A Security Authorization of any infrastructure directly in support of the DHS information system shall be performed as a general support system (GSS) prior to DHS occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization shall be performed in accordance with the DHS Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of the DHS information system.

At the beginning of the contract, and annually thereafter, the contractor shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS applies in the Security Authorization Process of its information systems. Any deficiencies noted during this assessment shall be provided to the COR for entry into the DHS' Plan of Action and Milestone (POA&M) Management Process. The contractor shall use the DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by the DHS POA&M Management Process. Contractor procedures shall be subject to periodic, unannounced assessments by DHS officials. The physical aspects associated with contractor activities shall also be subject to such assessments.

On a periodic basis, the DHS and its Components, including the DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these clauses. Evaluation could include, but it not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the contractor shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS

information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS in the event of a security incident.

Enterprise Security Architecture

The contractor shall utilize and adhere to the DHS Enterprise Security Architecture to the best of its ability and to the satisfaction of the DHS COR. Areas of consideration could include:

1) Use of multi-tier design (separating web, application and data base) with policy enforcement between tiers
2) Compliance to DHS Identity Credential Access Management (ICAM)
3) Security reporting to DHS central control points (i.e. the DHS Security Operations Center (SOC) and integration into DHS Security Incident Response
4) Integration into DHS Change Management (for example, the Infrastructure Change Control Board (ICCB) process)
5) Performance of activities per continuous monitoring requirements

Continuous Monitoring

The contractor shall participate in DHS' Continuous Monitoring Strategy and methods or shall provide a Continuous Monitoring capability that the DHS determines acceptable. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the contractor shall implement the following processes:

1. Asset Management
2. Vulnerability Management
3. Configuration Management
4. Malware Management
5. Log Integration
6. Security Information Event Management (SIEM) Integration
7. Patch Management
8. Providing near-real-time security status information to the DHS SOC

Specific Protections

Specific protections that shall be provided by the contractor include, but are not limited to the following:

Security Operations

The contractor shall operate a SOC to provide the security services described below. The contractor shall support regular reviews with the DHS Information Security Office to coordinate and synchronize the security posture of the contractor hosting facility with that of the DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The contractor staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the contractor staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the contractor facility SOC shall adhere to the incident response plan.

Computer Incident Response Services

The contractor shall provide Computer Incident Response Team (CIRT) services. The contractor shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS-specific incident response plan that adheres to DHS policy and procedure for reporting incidents. The contractor shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The contractor shall notify the DHS SOC of any incident in accordance with the Incident Response Plan and work with DHS throughout the incident duration.

Firewall Management and Monitoring

The contractor shall provide firewall management services that include the design, configuration, implementation, maintenance, and operation of all firewalls within the hosted DHS infrastructure in accordance with DHS architecture and security policy. The contractor shall provide all maintenance to include configuration, patching, rule maintenance (add, modify, delete), and comply with DHS' configuration management / release management requirements when changes are required. Firewalls shall operate 24x7x365. Analysis of the firewall logs shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Intrusion Detection Systems and Monitoring

The contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The contractor is responsible for creating and maintaining the NIDS rule sets. The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Physical and Information Security and Monitoring

The contractor shall provide a facility using appropriate protective measures to provide for physical security. The facility will be located within the United States and its territories. The contractor shall maintain a process to control physical access to DHS IT assets. DHS IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS security office.

Vulnerability Assessments

The contractor shall provide all information from any managed device to DHS, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

Anti-malware (e.g., virus, spam)

The contractor shall design, implement, monitor and manage to provide comprehensive anti-malware service. The contractor shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, and comply with DHS' configuration management / release management requirements when changes are required. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Patch Management

The contractor shall perform provide patch management services. The contractor shall push patches that are required by vendors and the DHS system owner. This is to ensure that the infrastructure and applications that directly support the DHS information system are current in their release and that all security patches are applied. The contractor shall be informed by DHS which patches that are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the contractor shall be responsible for deploying patches as directed by DHS. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the contractor prior to deployment in a test environment.

Log Retention

Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

Supply Chain Risk Management Terms and Conditions:

The Contractors supplying the Government hardware and software shall provide the manufacture's name, address, state and/or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state and/or domain of registration and DUNs number of those suppliers must also be provided.

Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.

The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.

Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software.

The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.

The Supply Chain Risk Management Plan shall address the following elements:

1. How risks from the supply chain will be identified,

2. What processes and security measures will be adopted to manage these risks to the system or system components, and

3. How the risks and associated security measures will be updated and monitored.

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Technical Representative (COTR) 30 days post award.

The Contractor acknowledges the Government's requirement to assess the Contractors Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents an unacceptable risk to national security.

The Contractor shall disclose, and the Government will consider, relevant industry standards certifications, recognitions and awards, and acknowledgments.

The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the Contracting Officer (CO). Contractors shall only provide Original Equipment Manufacturers (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

The Contractor shall be excused from using new OEM (i.e. “grey market,” previously used) components only with formal Government approval. Such components shall be procured from their original genuine source and have the components shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e. until the “end of life.”). Software updates and patches must be made available to the government for all products procured under this contract.

Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.

All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.

These records must be readily available for inspection by any agent designated by the US Government as having the authority to examine them.

This transit process shall minimize the number of times en route components undergo a change of custody and make use tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government’s request, shall be able to provide shipping status at any time during transit.

The Contractor is fully liable for all damage, deterioration, or losses incurred during shipment and handling, unless the damage, deterioration, or loss is due to the Government. The Contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software

being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

Personal Identification Verification (PIV) Credential Compliance

Authorities:

HSPD-12 ―Policies for a Common Identification Standard for Federal Employees and contractors‖

OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and contractors"

OMB M-06-16 ―Acquisition of Products and Services for Implementation of HSPD-12‖

NIST FIPS 201 ―Personal Identity Verification (PIV) of Federal Employees and contractors‖

NIST SP 800-63 ―Electronic Authentication Guideline‖

OMB M-10-15 ―FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management‖

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

Procurements for software products or software developments shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

ISO (Information Security) COMPLIANCE

Information Security Clause

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

Interconnection Security Agreements

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnect service agreements.

System Security documentation appropriate for the SELC status.

Security Certification/Accreditation

CBP Program Offices shall provide personnel (System Owner and Information System Security Officers) with the appropriate clearance levels to support the security certification/accreditation processes under this Agreement in accordance with the current version of the DHS MD 4300A, DHS Sensitive Systems Policy and Handbook, CBP Information Systems Security Policies and Procedures Handbook HB-1400-05, and all applicable National Institute of Standards and Technology (NIST) Special Publications (800 Series). During all SELC phases of CBP systems, CBP personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools. An ISSO performs security actions for an information system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO. While the ISSO performs security functions, the System Owner is always responsible for information system security (4300A). System owners shall include information security requirements in their capital planning and investment control (CPIC) business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS information system. System owners or AOs shall ensure that information security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.

Disaster Recovery Planning & Testing – Hardware

If the system owner requires a robust DR solution (full redundancy and failover capabilities (for near zero downtime)) then the funded DR solution must match the production environment like-for-like. This solution would also include additional software licenses, hardware, firmware and storage for the DR environment.

The system owner or program office must also include travel, per diem and approximately 16 over the core hours for travel to recovery facilities twice per fiscal year for system administrators, DBA’s, end users or testers

If the system owner requires a moderate DR solution that would provide a working environment that is capable of handling their mission essential functions then they can fund a scaled down solution which should still take into consideration additional hardware, software licenses, and storage for the DR environment.

The system owner or program office is still responsible for the costs associated with testing their DR solution; however, for a scaled down solution, it may be possible to leverage or share staff already designated to participate in DR activities.

If the system owner only requires a low DR solution then the system owner or program office can use internal resources to perform a table-top exercise, which generally does not require travel, additional hardware or software licenses.

Monitoring/reviewing contractor security requirements clause

Security Review and Reporting

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

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

Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 *Information Technology Systems*

Security and the *DHS Sensitive Systems Handbook* prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

OMB-M-07-18 FDCC

In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.

Engineering Platforms

Common Enterprise Services (CES) – Deliver the systems, infrastructure, and operational capabilities to fully implement the three service levels defined as part of the DHS/CBP Common Enterprise Services and support DHS Component use of those services. This includes the build out and integration of all required services and infrastructure, which must include the Single Sign-on Portal and CBP Enterprise Services Bus (ESB), required for the CES. Capabilities shall be designed to the DHS standard operating architecture (SOA), transportable between DHS data centers (CBP National Data Center, Stennis, and DHS 2nd data center).

Single Sign-on Portal – Design, build, and operate a single sign-on Portal - consistent with DHS' enterprise portal solution (for which ICE is the steward) - to provide a common point of access, with a single sign-on capability to existing applications and to provide the infrastructure for integrating diverse internal and/or external information and transactional resources. This includes the migration of the current ACE Portal to the Single Sign-on Portal as rapidly as feasible.

ITP (Infrastructure Transformation Program) COMPLIANCE

Help Desk and Operations Support

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

Interfacing

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

TRANSITION PLAN

The DHS CIO has established portfolio targets for the IT infrastructure that include production system consolidation at a DHS data center, and transition to OneNet. The contractor must be prepared to support CBP government leads, within the purview of this task order, to provide any required transition planning or program execution, associated with meeting the agreed to transition timeline, as directed by Government personnel. This includes the following types of taskings:

- Coordination with Government representatives
- Review, evaluation and transition of current support services
- Transition of historic data to new contractor system
- Government-approved training and certification process
- Transfer of all necessary business and/or technical documentation
- Orientation phase and program to introduce Government personnel, programs, and users to the contractor's team, tools, methodologies, and business processes, equipment, furniture, phone lines, computer equipment, etc.
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable debriefing and personnel out-processing procedures

Portfolio Review

Screening/Watchlist/Credentialing

Includes all activities that support the tracking and monitoring of travelers, conveyances and cargo crossing U.S. borders, and traffic pattern analysis, database (Federal, State, and Local) linking and querying, and managing status verification and tracking systems. Different investments and systems may support distinct screening and watchlist activities for people, cargo, and tangible goods. Credentialing encompasses all activities that determine a person’s eligibility for a particular license, privilege, or status, from application for the credential through issuance, use, and potential revocation of the issued credential.

H.5.2 SECURITY POLICY REQUIREMENT

All hardware, software, and services provided under this TO must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.

H.5.3 ENCRYPTION COMPLIANCE REQUIREMENT

a. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
b. National Security Agency (NSA) Type 2 or Type 1 encryption.
c. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the DHS IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

H.5.4 PERSONAL IDENTIFICATION VERIFICATION (PIV) CREDENTIAL COMPLIANCE

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

H.6 APPLICABLE DOCUMENTS

The contractor shall adhere to the policies, standards, directives, processes, and procedures required by the applicable documents outlined in each requirements document.

H.7 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.7.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

a. If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.
b. The contractor is required to complete and sign an OCI Statement (Section J, Attachment A). The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this contract, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.

c. If the contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.
d. In addition to the mitigation plan, the CO may require further information from the contractor. The CO will use all information submitted by the contractor, and any other relevant information known to GSA, to determine whether an award to the contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.
e. If any such conflict of interest is found to exist, the CO may determine that the conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the contractor may be found ineligible for award. Alternatively, the CO may determine that it is otherwise in the best interest of the U.S. to contract with the contractor and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded.

H.7.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) Form (Section J, Attachment D provides a sample NDA) and ensure that all its personnel (including subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.
b. Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel shall also be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained from the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.8 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 U.S.C. 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

H.9 RESERVED

H.10 RESERVED

H.11 RESERVED

H.11.1 TRAVEL AUTHORIZATION REQUESTS (TAR)

Before undertaking travel to any Government site or any other site in performance of this TO, the contractor shall have this travel approved by, and coordinated with, the COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-distance travel, the contractor shall prepare a TAR for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR or JTR. All travel requests (TARs) and approvals shall be done via CBP TASPD's OT&T application within Salesforce.

Requests for travel approval shall:

a. Be prepared in a legible manner.
b. Include a description of the travel proposed including a statement as to purpose.
c. Be summarized by traveler.
d. Identify the TO number.
e. Identify the CLIN associated with the travel.
f. Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.12 ODCs

The Government may require the contractor to purchase related supplies critical and related to the services being acquired under the TO. Such requirements may be identified during the course of a TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO, the contractor shall submit to the COR a Request to Initiate Purchase (RIP) If the prime contractor is to lose an approved purchasing system, the contractor shall submit to the CO a Consent to Purchase (CTP). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the COR or an approved CTP from the CO.

H.13 RESERVED

H.14 PRESS/NEWS RELEASE

The contractor shall not make any press/news release pertaining to this procurement without prior Government approval and only in coordination with the CO.

H.15 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application, or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply.

H.16 INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

All contractor employees using DHS information systems or processing DHS data shall be required to receive Security Awareness Training. This training will be provided by the appropriate component agency of DHS.

Contractors, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of DHS, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. DHS contractors, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access DHS information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or ISSO.

The following trainings are mandatory for all contractor employees on this TO.

Training Name	Frequency	Method of Delivery
CBP Suicide Prevention	Annual	Performance and Learning Management System (PALMS)
DHS Insider Threat Training	Annual	PALMS
CBP Cyber Security Awareness and Rules of Behavior Training	Annual	PALMS
Preventing and Addressing Workplace Harassment	Annual	PALMS
CBP Annual Integrity Awareness Training	Annual	PALMS
Privacy at DHS: Protecting Personal Information	Annual	PALMS
Counterintelligence Awareness Web-Based Training	Bi-annual (every two years)	PALMS
Basic Records Management	One Time (within 30 days of entry on duty)	PALMS

Note: this is the current list, however mandatory training is added periodically and training will be required to be completed by all contractors by the prescribed date.

H.17 SECURITY PROCEDURES (APR 2019)

A. Controls

1. The Contractor Employee shall comply with the U.S. Customs and Border Protection's (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.

2. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor Employee shall comply with all security policies contained in CBP Handbook 1400-05D, v.7.0, Information Systems Security Policies and Procedures Handbook, or latest available version.

3. All services provided under this contract must be compliant with the Department of Homeland Security (DHS) information security policy identified in DHS Sensitive Systems Policy Directive 4300A, v.13.1 and DHS Sensitive Systems Handbook 4300A, v.12.0, or latest available version.

4. All Contractor Employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor employees' departure/separation, all badges, building passes, parking permits, keys and pass cards must be given to the Contracting Officer's Representative (COR). The COR will ensure that the cognizant Physical Security official is notified so that access to all buildings and facilities can be revoked. NOTE: For contracts within the National Capitol Region (NCR), the Office of Professional Responsibility, Security Management Division (OPR/SMD) shall be notified if building access is revoked.

5. All Contractor Employees must be entered in the Contractor Tracking System (CTS) database by the Contracting Officer (CO) or COR. The Contractor Project Manager (CPM) shall provide timely start information to the CO/COR or designated government personnel to initiate the CTS entry. Other relevant information will also be needed for record submission in the CTS database such as, but not limited to, the contractor's legal name, contracting company address, brief job description, labor rate, Hash ID, schedule and contract specific information. The CO/COR or designated government personnel shall provide the CPM with instructions for providing required information.

6. The CO/COR may designate responsibility for out-processing to the CPM. This requires that the CPM have an active CBP Background Investigation (BI) and Active Directory (AD) account. CPM shall provide Contactor Employee departure/separation date and reason for leaving to the CO/COR in accordance with CBP Directive 1210-007B, Tracking of Contractor Employees. Failure by the CPM to provide timely notification of Contractor Employee departure/separation in accordance with the contract requirements shall be documented and considered when government personnel completes a Contractor Performance Report (under Business Relations) or other performance related measures.

Additionally, the CO/COR shall immediately notify OPR/SMD of the contractor's departure/separation.

B. Security Background Investigation Requirements

1. In accordance with DHS Instruction Handbook 121-01-007-01, Rev. 01, the Department of Homeland Security Personnel Security, Suitability and Fitness Program, Chapter 2, Personnel Security Program Standards, § 13, Citizenship Requirements, Contractor Employees who require access to sensitive information must be U.S. citizens or have Lawful Permanent Resident (LPR) status, § 13E. A waiver may be granted, as outlined in Chapter 2, § 14 of DHS Instruction Handbook 121-01-007-01.

2. Contractor employees that require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with Chapter 2, Personnel Security Program Standards, § 13, and Citizenship Requirements, § 13F. (Lawful Permanent Resident status is not acceptable in this case). A waiver may be granted, as outlined in Chapter 2, § 14 of DHS Instruction Handbook 121-01-007-01.

3. Provided the requirements of DHS Instruction Handbook 121-01-007-01 are met as outlined in paragraph 1, above, Contractor Employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated background investigation (BI) or a single scope background investigation (SSBI) prior to commencing work on this contract. Exceptions shall be approved on a case-by-case basis with the Contractor Employee's access to facilities, systems, and information limited until the Contractor employee receives a favorably adjudicated BI or SSBI. A favorable adjudicated BI or SSBI shall include various aspects of a Contractor Employee's life, including employment, education, residences, police and court inquires, credit history, national agency checks, and a CBP Background Investigation Personal Interview (BIPI).

4. The Contractor Employee shall submit within ten (10) working days after award of this contract a list containing the full legal name, social security number, place of birth (city and state), and date of birth of employee candidates who possess favorably adjudicated BI or SSBI that meets federal investigation standards. For Contractor employee candidates needing a BI for this contract, the Contractor Employee shall require the applicable Contractor Employees to submit information and documentation requested by CBP to initiate the BI process.

5. Background Investigation information and documentation is usually submitted by proper completion of standard federal and agency forms such as Electronic Questionnaires for investigations Processing (e-QIP), Fingerprint Card, CBP Form 78-Background Investigation Requirements Determination (BIRD), Fair Credit Reporting Act (FCRA) Form, a Contractor Employee Initial Background Investigation (BI) Form (CBP Form 77) (Sections A and B). These forms must be submitted to the designated CBP official identified in this contract. The designated CBP security official will review the information for completeness.

6. The estimated completion of a BI or SSBI is approximately sixty (60) to ninety (90) days from the date of receipt of the properly completed forms by CBP security office. During the term of this contract, the Contractor is required to provide the names of its employees who successfully complete the CBP BI or SSBI process to the CO and COR. Failure of any Contractor Employee to obtain and maintain a favorably adjudicated BI or SSBI shall be cause for dismissal. For key personnel, the Contractor shall propose a qualified replacement employee candidate to the CO and COR within 30 days after being notified of an unsuccessful candidate or vacancy. For all non-key personnel Contractor Employees, the Contractor shall propose a qualified replacement employee candidate to the COR within 30 days after being notified of an unsuccessful candidate or vacancy. The CO/COR shall approve or disapprove replacement employees. Continuous failure to provide Contractor Employees who meet CBP BI or SSBI requirements may be cause for termination of the contract.

C. Security Responsibilities

1. The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel will be responsible for physical security of work areas and CBP furnished equipment issued under this contract.

2. The CO/COR may require the Contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to carelessness, insubordination, incompetence, or security concerns.

3. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The Contractor Employee shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.

4. The Contractor shall ensure that its employees who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.

5. Upon completion of this contract, the Contractor Employee shall return all sensitive information used in the performance of the contract to the CO/COR. The Contractor shall certify, in writing, that all sensitive and non-public information has been purged from any Contractor-owned system.

D. Notification of Contractor Employee Changes

1. The CPM shall notify the CO/COR via phone, facsimile, or electronic transmission, immediately after a personnel change becomes known or no later than five (5) business days prior to departure of the Contractor Employee. Telephone notifications must be immediately followed up in writing. CPM's notification shall include, but is not limited to name changes, resignations, terminations, and reassignments to another contract.

2. The CPM shall notify the CO/COR and program office (if applicable) in writing of any proposed change in access requirements for its employees at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed change. If a security clearance is required, the CO/COR will notify OPR/SMD.

E. Non-Disclosure Agreements

As part of the BI package, Contractor Employees are required to execute and submit a Non-Disclosure Agreement (DHS Form 11000-6) as a condition to perform on any CBP contract.

H.18 3052.204-71 CONTRACTOR EMPLOYEE ACCESS (JUN 2012)

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

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

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

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

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

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

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

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

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

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

(End of clause)

ALTERNATE I (JUN 2012)

When the contract will require contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

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

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

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

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

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

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

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

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

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

(End of clause)

ALTERNATE II (JUN 2006)

When the Department has determined contract employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to IT resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-55 1). Any exceptions must be approved by the Department's Chief Security Officer or designee.

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

I.1 TASK ORDER CLAUSES

All applicable and required clauses set forth in FAR 52.301 automatically flow down to all Alliant 2 TOs, based on their specific contract type (e.g., cost, fixed-price, etc.), statement of work, competition requirements, commercial or not commercial, and dollar value as of the date the TO solicitation is issued.

I.2 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. The full text of a clause may be accessed electronically at the FAR website:

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

FAR	TITLE	DATE
52.203-13	Contractor Code of Business Ethics and Conduct	OCT 2016
52.203-14	Display of Hotline Poster(s)(https://www.oig.dhs.gov/hotline)	OCT 2016
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	APR 2014
52.204-2	Security Requirements	AUG 1996
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	OCT 2016
52.204-13	System for Award Management Maintenance	OCT 2018
52.204-14	Service Contract Reporting Requirements	OCT 2016
52.204-21	Basic Safeguarding of Covered Contractor Information Systems	JUN 2016
52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities	JUL 2018
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Deviation 20-05)	AUG 2020
52.212-4	Contract Terms and Conditions-Commercial Items	OCT 2018
52.212-4, Alt.I	Contract Terms and Conditions-Commercial Items,Alternate I	JAN 2017
52.215-23	Limitations on Pass-Through Charges	OCT 2009
52.223-15	Energy Efficiency in Energy Consuming Products	DEC 2007
52.223-16	Acquisition of EPEAT®-Registered Personal Computer Products	OCT 2015
52.224-1	Privacy Act Notification	APR 1984
52.224-2	Privacy Act	APR 1984

FAR	TITLE	DATE
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008
52.225-25	Prohibition on Contracting With Entities Engaging in Certain Activities or Transactions Relating to Iran—Representations and Certifications	OCT 2015
52.227-14	Rights in Data – General	MAY 2014
52.227-14	Rights In Data –Alternate II	DEC 2007
52.227-14	Rights In Data –Alternate III	DEC 2007
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	DEC 2007
52.227-17	Rights In Data Special Works	DEC 2007
52.227-21	Technical Data Declaration Revision and Withholding of Payment – Major Systems	MAY 2014
52.232-18	Availability of Funds	APR 1984
52.232-22	Limitation of Funds	APR 1984
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.237-3	Continuity of Services	JAN 1991
52.239-1	Privacy or Security Safeguards	AUG 1996
52.244-6	Subcontracts for Commercial Items	JAN 2017
52.245-1	Government Property	JAN 2017
52.246-25	Limitation of Liability – Services	FEB 1997
52.251-1	Government Supply Sources	APR 2012

I.2.1 FAR CLAUSES INCORPORATED BY FULL TEXT

FAR 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILANCE SERVICES OR EQUIPMENT (AUG 2019)

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

"Covered foreign country" means The People's Republic of China.

"Covered telecommunications equipment or services" means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

"Critical technology" means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.* Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in Federal Acquisition Regulation 4.2104.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

FAR 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS-COMMERCIAL ITEMS (JUL 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, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(3) 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).

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015).

(5) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(6) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Public Laws 108-77 and 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:

[Contracting Officer check as appropriate.]

_X_ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (June 2020), with Alternate I (Oct 1995) (41U.S.C.4704 and 10 U.S.C. 2402).

_X_ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Jun 2020) (41 U.S.C. 3509)).

__ (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 (Jun 2020) (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).

_X_ (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. (Jun 2020) (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 (Mar 2020) (15 U.S.C. 657a).

__ (ii) Alternate I (Mar 2020) of 52.219-3.

__ (12) (i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Mar 2020) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

__ (ii) Alternate I (Mar 2020) of 52.219-4.

__ (13) [Reserved]

__ (14) (i) 52.219-6, Notice of Total Small Business Set-Aside (Mar 2020) of 52.219-6 (15 U.S.C. 644).

__ (ii) Alternate I (Mar 2020) of 52.219-6 .

__ (15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (Mar 2020) (15 U.S.C. 644).

__ (ii) Alternate I (Mar 2020) of 52.219-7.

__ (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 (Jun 2020) (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 (Jun 2020) of 52.219-9.
__ (v)Alternate IV (Jun 2020) of 52.219-9
__ (18) (i) 52.219-13, Notice of Set-Aside of Orders (Mar 2020) (15 U.S.C. 644(r)).
(ii) Alternate I (Mar 2020) of 52.219-13.
__ (19) 52.219-14, Limitations on Subcontracting (Mar 2020) (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 (Mar 2020) (15 U.S.C. 657f).
__ (22) (i) 52.219-28, Post Award Small Business Program Rerepresentation (May 2020) (15 U.S.C. 632(a)(2)).
(ii) Alternate I (MAR 2020) of 52.219-28.
__ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Mar 2020) (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 (Mar2020) (15 U.S.C. 637(m)).
__ (25) 52.219-32, Orders Issued Directly Under Small Business Reserves (Mar 2020) (15 U.S.C. 644(r)).
__ (26) 52.219-33, Nonmanufacturer Rule (Mar 2020) (15U.S.C. 637(a)(17)).
__ (27) 52.222-3, Convict Labor (Jun 2003) (E.O.11755).
_X_ (28) 52.222-19, Child Labor-Cooperation with Authorities and Remedies (Jan2020) (E.O.13126).
_X_ (29) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
_X_ (30) (i) 52.222-26, Equal Opportunity (Sep 2016) (E.O.11246).
__ (ii) Alternate I (Feb 1999) of 52.222-26.
_X_ (31) (i) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).
__ (ii) Alternate I (Jul 2014) of 52.222-35.
_X_ (32) (i) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).
__ (ii) Alternate I (Jul 2014) of 52.222-36.
_X_ (33) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).
_X_ (34) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
_X_ (35) (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_ (36) 52.222-54, Employment Eligibility Verification (Oct 2015). (Executive Order 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.)
__ (37) (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.)
__ (38) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O. 13693).
__ (39) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).
__ (40) (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.
__ (41) (i) 52.223-14, Acquisition of EPEAT®-Registered Televisions (Jun 2014) (E.O.s 13423 and 13514).
__ (ii) Alternate I (Jun2014) of 52.223-14.
__ (42) 52.223-15, Energy Efficiency in Energy-Consuming Products (May 2020) (42 U.S.C. 8259b).
__ (43) (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_ (44) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (Jun 2020) (E.O. 13513).
__ (45) 52.223-20, Aerosols (Jun 2016) (E.O. 13693).
__ (46) 52.223-21, Foams (Jun2016) (E.O. 13693).
__ (47) (i) 52.224-3 Privacy Training (Jan 2017) (5 U.S.C. 552 a).
__ (ii) Alternate I (Jan 2017) of 52.224-3.
__ (48) 52.225-1, Buy American-Supplies (May 2014) (41 U.S.C. chapter 83).
__ (49) (i) 52.225-3, Buy American-Free Trade Agreements-Israeli Trade Act (May 2014) (41 U.S.C.chapter83, 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.
__ (50) 52.225-5, Trade Agreements (Oct 2019) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).
__ (51) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
__ (52) 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. 2302Note).
__ (53) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov2007) (42 U.S.C. 5150).
__ (54) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov2007) (42 U.S.C. 5150).
__ (55) 52.229-12, Tax on Certain Foreign Procurements (Jun 2020).
__ (56) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).
__ (57) 52.232-30, Installment Payments for Commercial Items (Jan2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

_X_ (58) 52.232-33, Payment by Electronic Funds Transfer-System for Award Management (Oct2018) (31 U.S.C. 3332).
__ (59) 52.232-34, Payment by Electronic Funds Transfer-Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).
__ (60) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).
__ (61) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).
_X_ (62) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(13)).
__ (63)
(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:
__ (1) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter67).
__ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).
__ (3) 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).
__ (4) 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).
__ (5) 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).
__ (6) 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).
__ (7) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).
__ (8) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706).
__ (9) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) (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, as defined in FAR 2.101, on the date of award of this contract, 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 (Jun 2020) (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).

(v) 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 the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(vi) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(vii) 52.222-26, Equal Opportunity (Sep 2015) (E.O.11246).

(viii) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).

(ix) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).

(x) 52.222-37, Employment Reports on Veterans (Jun 2020) (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 (Aug2018) (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 (Mar2015) of 52.222-50 (22 U.S.C. chapter 78 and 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 (May2014) (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 (May2014) (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 (Jun 2020) (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)

FAR 52.217-7 OPTION FOR INCREASED QUANTITY – SEPARATELY PRICED LINE ITEM (MAR 1989)

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer may exercise the option by written notice to the Contractor 30 days. Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

(End of clause)

FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six months. The Contracting Officer may exercise the option by written notice to the Contractor within 7 days of the end of the period of performance.

(End of clause)

FAR 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 5 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 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 66 months.

(End of clause)

FAR 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013)

(a) Upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.

(b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of clause)

I.3 RESERVED

I.4 DHS ACQUISITION REGULATION SUPPLEMENTS (HSAR) CLAUSES INCORPORATED BY REFERENCE

The full text of a clause may be accessed electronically at HSAR website:

www.dhs.gov/publication/homeland-security-acquisition-regulation-deviations/

I.5 OPTION FOR ADDITIONAL AS-NEEDED SERVICES

The Government may require additional, as-needed support during the base or any option period, and these modifications will be in-scope to provide increased support for the defined task areas of Section C. Additional, as-needed support is OPTIONAL and is not a guarantee. If the Government determines that an increased quantity of support is required for the task areas defined in Section C, the Government reserves the right to exercise the additional, as-needed

support unilaterally. The CO will provide written notice to the Contractor at least 30 calendar days prior to any unilateral exercise of the additional, as-needed support services. In the event the Government does elect to exercise the additional, as-needed Option, support will be realigned under new or existing CLINs for the relevant task areas identified in Section C, and an equal amount will be deducted from the additional, as-needed support services CLIN amount. This support will be provided at the same labor rates that have been evaluated for price reasonableness at time of TO award for the applicable ordering period. Any unexpended capacity may be carried forward to be exercised in a future period of performance, and conversely, any future capacity can be purchased in the current period of performance, if needed.

I.6 TELEWORK (FEB 2015)

A. Definitions

"Telework" is an alternative work arrangement which allows a contractor employee to perform work at an alternate worksite (e.g. home, telework center, contractor's office). In accordance with 41 U.S.C. § 3306(f), employees of Federal Government contractors are permitted to telework in the performance of contracts entered into with executive agencies. The term "telecommuting" used in the Federal Acquisition Regulation (FAR) is synonymous with the term "telework" as used in this clause. A contractor employee can telework on a core or episodic basis. A core arrangement occurs on a routine and recurring basis, whereas an episodic arrangement occurs on an occasional and non-routine basis, such as during inclement weather.

"Telework-ready contractor employee" is a contractor employee who has been approved to telework, has an established alternate worksite, is prepared to telework by having enough work to cover the scheduled telework period, and has the appropriate secure technology equipment to meet the needs of the telework arrangement and a high-speed Internet connection.

B. Requirements

The Contractor shall provide adequate oversight of work products when telework is authorized to ensure continuity of contract performance and quality control. Equipment provided by U.S. Customs and Border Protection (CBP) for telework purposes will be treated as Government Furnished Equipment (GFE) and guidelines in CBP HB 1400-05D, CBP Information Systems Security Policies and Procedures Handbook shall be followed. All CBP training required for telework-ready contractor employees, such as the annual CBP IT Security Awareness and Rules of Behavior training, shall be completed prior to commencement of an individual's telework schedule. The Contracting Officer's Representative (COR) will notify the Contractor's program manager (PM) of the required training courses. Once the training is completed, contractor employees shall submit their certificates of completion to the COR. Contractor employees shall comply with the security requirements stated in HSAR 3004.470 and HSAM 3004.470, and

work according to the guidance set forth in DHS 4300A, Sensitive Systems Handbook, Rules of Behavior.

A contractor employee's telework schedule shall be approved by the Contractor's PM and coordinated with the COR. Once approved, requests to change a scheduled telework day shall be submitted in advance when possible to the Contractor's PM, who will coordinate with the COR. The Contractor's PM continues to be responsible for contractor employees' time and attendance and notifying the COR of any changes.

If a Federal Government closing affects the Government facility, contractor employees who are telework-ready shall begin to telework at their normal start time and are expected to work the entire day. If OPM announces the option for unscheduled telework, a contractor employee may request to telework by contacting the Contractor's PM, who will coordinate with the COR.

If a contractor employee has performance issues, does not follow the security procedures, or does not complete required training while in a telework status, the COR will contact the Contractor's PM and the contractor employee's telework privileges may be revoked.

C. Information Technology (IT) and Security

Contractor employees are required to use only GFE provided by CBP when teleworking. Should the GFE fail or require repair or replacing, the contractor employee shall be required to return to the traditional worksite to perform their duties. CBP shall provide maintenance and technical support for IT GFE used by teleworkers. CBP's inability to provide IT GFE shall not constitute an excusable delay. The Contractor or contractor employee is responsible for providing high speed internet connectivity for teleworking and will bear the cost of the internet connection. The contractor employee shall be accessible at all times, via telephone, e-mail, or video conferencing during his/her working hours. Contractor employees' use of GFE and Government information shall be for contractual performance only and shall be protected from unauthorized access, disclosure, sharing, transmission, or loss. The contractor employee shall keep Government property and information safe, secure, and separated from his/her personal property and information. Contractor employees who telework shall be the sole operators of the GFE they use and shall abide by CBP HB 5200-13C, Personal Property and Asset Management Handbook. Contractor employees who telework shall not work on, have access to, or keep in their possession classified information at an alternate worksite. Contractor employees shall comply with the guidance in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information. Contractor employees shall return all GFE provided by CBP to the COR upon separation from the contract.

D. Subcontracts

The Contractor shall include the substance of this clause in all subcontracts where telework is permitted. The Contractor shall be responsible for monitoring the subcontractor's adherence to this clause.

J.1 LIST OF ATTACHMENTS

The following attachments are attached, either in full text or electronically.

ATTACHMENT	TITLE
A	Organizational Conflict of Interest (OCI) Statement
B	Electronic Reading Room - instructions
C	Department of Defense (DD) 254 (O&M and BISS)
D	~~Corporate~~ Non-Disclosure Agreement (NDA) *provided as an example*
E	SF 1449s BISS
F	SF 1449s O&M

This page intentionally left blank.

L.1 FAR 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the CO will make the full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation of offer. Also, the full text of a solicitation provision may be accessed electronically at this address:

https://www.acquisition.gov/far

FAR	TITLE	DATE
52.204-24	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment	AUG 2020
52.204-26	Covered Telecommunications Equipment or Services-Representation	DEC 2019
52.212-1	Instructions to Offerors-Competitive Acquisition	JUN 2020
52.216-31	Time-and-Materials/Labor-Hour Proposal Requirements-Commercial Item Acquisition	FEB 2007
52.217-5	Evaluation of Options	JUL 1990
52.232-38	Submission of Electronic Funds Transfer Information with Offer	JUL 2013

L.1.1 SOLICITATION PROVISIONS PROVIDED IN FULL TEXT

L.2 GENERAL INSTRUCTIONS

a. The Offeror is expected to examine this entire solicitation document including the Master/Basic Contract. Failure to do so will be at the Offeror's own risk.

b. The Government may make award based on initial offers received, without discussion of such offers. Proposals shall set forth full, accurate, and complete information as required by this solicitation package (including Attachments listed in Section J). The penalty for making false statements in proposals is prescribed in 18 U.S.C. 1001.

c. Offerors that include in their proposals data that they do not want disclosed to the public for any purpose, or used by the Government except for evaluation purposes, shall –

(1) Mark the title page with the following legend:

This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed--in whole or in part--for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this Offeror as a result of--or in connection with--the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without

restriction. The data subject to this restriction are contained in sheets [insert numbers or other identification of sheets]; and

(2) Mark each sheet of data it wishes to restrict with the following legend:

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal."

d. The Government assumes no liability for disclosure or use of unmarked data and may use or disclose the data for any purpose. Unless restricted, information submitted in response to this request may become subject to disclosure to the public pursuant to the provisions of the Freedom of Information Act (5 U.S.C. 552).

e. This procurement is conducted under the procedures of FAR Subpart 16.5. The policies and procedures of FAR Subpart 15.3 do not apply.

L.3 GENERAL INFORMATION

The Government is utilizing this solicitation for two (2) distinct requirements, Information Technology (IT) Operations and Maintenance (O&M), Upgrades, Updates, Modifications and Enhancements Services (IT O&M) Solicitation# 70B04C20Q00000131 and Business Intelligence Support Services (BISS) Solicitation# 70B04C20Q0000018**1**. When responding, please label the proposal with the appropriate solicitation number.

This solicitation contains 2 distinct PWS, one for O&M and one for BISS. Alliant 2 IDIQ contract holders may propose for one or both requirements. If the Offeror intends to propose to both requirements, the Offeror is required to submit two (2) complete, distinct submissions, as well as indicate in each submission which requirement is being proposed. Any reference to information contained in another submission will not be considered.

Proposals shall be valid for a period of not less than 120 calendar days from the date of delivery. **For proposal purposes only**, Offerors shall use a Transition Task Order Start date of September 28, 2020.

L.4 SUBMISSION OF OFFERS

Each offer shall be provided to the Government in three separate parts and shall contain the following:

a. Part I – Phase I Video Submission (video submission will not exceed 15 minutes)

b. Part II – Written Technical Proposal (page limit: 30 pages) & Price Proposal (no page limit)

The Offeror shall submit each part on the due dates indicated on the Cover Letter.

Unless otherwise specified, one page is one side of a U.S. Letter size (8.5" x 11") piece of paper. All electronic files shall be in MS Word, PowerPoint, PDF, or Excel formats. Any documents provided in Section J, List of Attachments, shall be submitted using the same file format (e.g., Project Staffing Plan shall be submitted in Excel file format); this includes the same font size and margins as the document provided. When printed, pages (with the exception of Excel and PowerPoint) must maintain one inch margins. Excel files must maintain margins of no less than 0.7 inches, and PowerPoint files must maintain margins of no less than 0.5 inches. When printed,

pages must maintain 12 point Times New Roman font and be single spaced, with the exception of charts/graphics/tables. Charts/Graphics/Tables must maintain a minimum of ten point Times New Roman font. Charts/Graphics/Tables embedded in the proposal will count toward page limitations. Headers and footers may be of a font larger than 12 point, but shall not be smaller than ten point font. Ledger size (11" x 17") paper may be used in the Project Staffing Plan or when providing charts/graphics/tables. A single side of an 11" x 17" piece of paper will be counted as two pages where page limitations apply. Items such as a Title Page, Table of Contents, Cover Letter, List of Figures, and Acronym Lists are excluded from the page counts below, unless they are inclusive of a document (e.g., a Table of Contents within the Draft Transition-In Plan), in which case it would count toward the stated page limitations. PDF files will be allowed for executed documents such as, if applicable, Letters of Commitment.

Any pages submitted beyond the page limitations will be removed and not evaluated.

L.5 RFQ PHASES

L.5.1 PHASE I: WRITTEN INFORMATION AND VIDEO SUBMISSION (PART I, FACTOR 1)

This volume shall contain the following:

a. OCI Statement and Corporate NDAs (Tab A)
b. [Reserved] (Tab B)
c. Prior Specialized Experience (VIDEO)
d. FPDS & CPARS[1] (Tab C) - no page limit

L.5.1.1 OCI STATEMENT AND CORPORATE NDAs (TAB A)

The Offeror and each subcontractor, consultant, and teaming partner involved in proposal development shall complete and sign an OCI Statement and Corporate NDA. All information pertaining to OCI is outlined in Section H.7.1. All information pertaining to NDA is outlined in Section H.7.2.

L.5.1.2 CORPORATE EXPERIENCE (VIDEO)

Phase I, Video Response Instructions:

Phase I of the RFQ is being issued to GSA Alliant 2 IDIQ contract holders. Failure to follow these instructions may make the submission non-responsive to the RFQ requirements. All submissions shall adhere to all specified time limits and page limits.

(a) The Offeror shall elaborate on its Corporate Experience on projects that are similar in size, scope, and complexity to the requirements as described in Section C of the RFQ. The Offeror shall discuss the scope of work, applicability to PWS tasks, the client and project relationship to the RFQ, the specific responsibilities of the Offeror, major deliverables produced, approach to client support to include quality assurance, risk management, subcontractor management, maintaining effective lines of communication performance measures/service levels applied, and

[1] The Government will allow submission of base contract award documents and past performance questionnaires (PPQs) for projects supporting law enforcement sensitive and Intelligence Community clients.

any problems or issues that occurred and the corrective action taken. Offerors may use slides/charts/other background materials on the video screen to display information about the corporate experience references.

The submitted example(s) must have begun no earlier than five (5) years before the release date of this RFQ or remain currently performing/ongoing under a continuous period of performance. At least two of the corporate experiences shall be the Offeror's direct experience as a prime contractor of similar scope and complexity to the requirements identified in Section C. The offeror shall include additional prior experience from team members or subcontractors that is similar in scope and complexity to the requirements identified in Section C that the team member or subcontractor is proposed to perform.

(b) All projects examples shall be contracts or orders for the performance of actual technical requirements. A master contract vehicle (e.g., Blanket Purchase Agreement (BPA), Indefinite Delivery/Indefinite Quantity (IDIQ) contract) that has one or more TOs that were awarded and performed under that vehicle and supports a single customer or program, may be grouped and counted as one Prior Specialized Experience project example. Task Orders under government-wide, department-wide, or agency-wide contracts (e.g., Alliant, SEAPORT, EAGLE) may not be grouped unless they support the same program.

(c) General Video Submission Instructions:

Video submissions shall adhere to the proposal content maximum time limits utilizing Youtube.com for the Government to access. Videos may be marked public or private. By the date and time specified, Offeror's shall send a YouTube link to the cbptaspdrequirements@cbp.dhs.gov in order for CBP to access the video submission. Do not provide a shortened URL, such as youtu.be.

The Government does not intend to evaluate the quality of the video submissions. Unnecessarily elaborate videos beyond that which is sufficient to present a complete and effective response to this RFQ are not desired. Computer-generated graphics, background music, elegant sets, and so forth are neither necessary nor wanted. The Government strongly encourages not to invest significantly in the video submission. A low-cost video production is encouraged.

The DHS Procurement Innovation Lab (PIL) has produced the following video to provide helpful information about video submissions: DHS YouTube Skit and Mock Video: https://www.youtube.com/watch?v=8DJpJ2qECtM&feature=em-share_video_user. Offerors are not required to adhere to the DHS mock video format.

The Offeror will submit one YouTube.com link for each requirement, if proposing to more than one solicitation. If the Offeror submits one (1) video comprising of multiple requirements, the Government will not evaluate the Offeror's Phase 1 submission and the Offeror will not be allowed to continue to participate in Phase 2.

1. Offeror's video submission will not exceed 15 minutes in length/duration utilizing Youtube.com for the Government to access. Anything over 15 minutes will not be evaluated by the Government.

2. In addition to the YouTube.com submission, Offerors shall submit their FPDS & CPARS records for federal and all public sector project(s) or similar certified information for commercial project (or if performed as subcontractor) for all cited corporate experience example(s). The most current FPDS and CPARS record (current period or last issued modification) shall be provided. If no FPDS and/or CPARS is currently available for the example(s), the contractor may submit similar certified information for federal/public sector (e.g., a copy of the Base Contract Award and Modification(s), Balanced Scorecard(s), etc.). FPDS & CPARS records may be provided as one searchable document in lieu of individual records.

3. The Government desires no more than two (2) individuals be featured in the video. The video shall feature at least one (1) individual who will serve as the Principal/Program Manager and will responsible for managing any resultant contract. Offerors are encouraged to use visual aids within the video presentation. The video must display a letter of commitment for each (if any) proposed subcontractor ~~referenced in the responses to the experience questions provided below~~. The video must also display a letter of commitment from any video participant who is not an employee of the prime Offeror.

L.5.1.3 ADVISORY NOTIFICATION

After the Government completes evaluation Factor 1, Offerors will receive an advisory notification via e-mail from the Contracting Officer. This notification will advise the Offerors of the Government's evaluation of Phase I for the vendor's consideration in their voluntary decision on whether to proceed to Phase II. The intent of this notice is to minimize proposal development costs for those Offerors with little to no chance of receiving an award.

Failure to participate in Phase I of the procurement precludes further consideration of a Offeror's. Phase II submissions will not be accepted from Offerors who have not submitted Phase I proposals by the due date and time stated in this solicitation.

L.5.2 SUBMISSION OF THE WRITTEN COST/PRICE PROPOSAL (PART II)

The Offeror shall fully support all proposed costs/prices. An Offeror's proposal is presumed to represent the Offeror's best efforts in response to the solicitation. Any inconsistency, whether real or apparent, between promised performance and cost/price, shall be explained in the proposal.

Offerors shall clearly differentiate descriptive information for evaluation purposes from that which is promissory for inclusion in the resultant award. Offerors are encouraged to keep descriptive information to a minimum.

Written Cost/Price Proposals shall be submitted as one electronic copy. **The Cost/Price Excel Workbook shall only be provided as one electronic copy**; No thumb drives will be accepted. The Offeror shall submit all proposed costs/prices using MS Excel software utilizing the formats without cells locked and including all formulas. The Offeror shall include adequate information, which will allow the Government to perform a price analysis.

Important note regarding email attachments: CBP's email system limits incoming email attachments to 10MB per email. Offerors should NOT submit .zip files as these may be stripped by CBP's email system. All incoming files are scanned so there may be a delay between the

time the file is submitted and the time it is received. Therefore, Offerors must ensure they submit proposals with sufficient time to reach the required destination no later than the response due date identified above. Offerors are strongly encouraged to verify receipt of their response (via email) as noted above. Offerors may submit attachments in multiple emails due to size constraints; however, the complete proposal (including all required submissions) must be received by the due date and time identified above.

Proprietary information shall be clearly marked.

The Offeror shall not include any cost/price data in any technical narratives of the proposal.

L.5.2.1 SOLICITATION, OFFER AND AWARD (SF 1449) (TAB A)

When completed and signed by the Offeror, Standard Form (SF) 1449, "Solicitation, Offer and Award," constitutes the Offeror's acceptance of the terms and conditions of the proposed TO. Therefore, the form must be executed by representatives of the Offeror authorized to commit the Offeror to contractual obligations. The Offeror shall sign the SF 1449.

L.5.2.2 PRICE/COST (FACTOR 5)

Part II of Written Price/Cost Proposal and shall contain the following:

a. Solicitation, Offer and Award (SF1449) (Tab A)
b. Section B - Cost/Price Excels (Tab B). Offerors shall add additional CLINs, ~~subCLINs~~ sub CLINs, or any other structural modification to Section B in an Excel to illustrate their proposed costs as aligned to the proposed technical solution. Transition must be a separately addressed, including a separate excel.
c. Cost/Price Supporting Documentation (Tab C)
d. Subcontractor Supporting Documentation (Tab D)
e. Cost/Price Assumptions (Tab E)
f. Reserved (Tab F)

1. General Information:

It is anticipated that all pricing information submitted in response to these instructions will be treated as business confidential. Except for the total price, none of the price quote information will be disclosed outside of the Government. Pricing for the Transition TO must be a separated out. There is no page limitation for the price volume.

The price volume must be mathematically correct and all parts must be numerically consistent.

The price volume must correlate with the technical volume and staffing plan in a logical and consistent manner.

The required price volume format shall be submitted in Microsoft® Office Suite 2013 (or higher versions when available). All Excel spreadsheets shall maintain all formulas and links between

the spreadsheets and tables presented in the price proposal. Formulas in the electronic spreadsheets shall not be converted to hard coded values.

2. Price Proposal Content:

- Price volume format: Roll Up – Shall include company name (prime and subcontractor) for all proposed labor. All labor shall be defined by company name and labor categories for the Base Period plus all Options Periods.
- The Offeror shall also provide a comprehensive narrative that discusses in detail the assumptions, methods and business decisions that form the basis for the proposed price.
- The Offeror shall provide a brief statement and support for the basis of the Offeror's proposed productive labor year.
- The Offeror shall provide a brief statement and support for the basis of the Offeror's annual labor escalation factors.
- Offeror's shall include additional CLINs, sub-CLIN's which align to their technical solution to supplement the format provided.

L.5.2.2.1 SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS (TAB B)

The Offeror shall indicate the cost/price to be charged for each item in **Section B** rounded to the nearest whole dollar. The Offeror shall insert not-to-exceed indirect/material handling ceiling rates in accordance with Section B.5.1.

Note for the Transition TO: the flexible end date for the transition TO will be function of post-award readiness efforts, and not a function of competitive evaluation. For purposes of evaluation and pricing, all Offerors should use 12 month period for transition TO.

As a supplement to the summary information provided in Section B, the Offeror shall provide full back-up documentation for the CLINs for each period of performance, and include any additional CLINs or sub-CLINS to further delineate the proposed technical solution for each task area using an Excel Workbook. **The Offeror shall not lock any cells and the Offeror shall ensure all calculation formulas are included in order to effectively show the cost build up in the Cost/Price Excel Workbook.** The back-up documentation shall include a summary total for each ~~element~~proposed CLIN.

Note: Offerors shall provide a CLIN roll up consisting of labor categories, corresponding proposed hours, and labor rates. Discounts are encouraged and should be easily identified.

L.5.2.2.2 COST/PRICE SUPPORTING DOCUMENTATION (TAB C)

The cost/price supporting documentation is required to enable the Government to perform a price analysis. Supporting documentation for the Transition TO must be distinct from the Requirements TO.

The Offeror shall provide a detailed narrative, which explains the processes and methodologies used to develop its price proposal. This includes, but is not limited to, the estimating methodology used by the Offeror to estimate direct labor and subcontractor labor, planning assumptions used in the development of the cost estimate, etc. The Offeror shall provide the

labor rate (fully burdened) for all proposed labor categories and all projected rates (factoring in escalation) for all option years. The Offeror shall identify all direct labor escalation factors and basis for any escalation index being utilized for all option years.

The Government is also providing an estimated magnitude for each requirements as follows:

The Government estimates that the total value of the Operations and Maintenance Transition requirement is between $40,000,000.00 and $50,000,000.00. This range is for a twelve (12) months period of performance.

The Government estimates that the total value of the Operations and Maintenance requirement is between $950,000,000.00 and $975,000,000.00. This range is inclusive of all CLINs over the full ~~6~~5 year performance period and 6 month OES.

The Government estimates that the total value of the Business Intelligence Support Services Transition requirement is between $13,000,000.00 and $15,000,000.00. This range is for a twelve (12) months period of performance.

The Government estimates that the total value of the Business Intelligence Support Services requirement is between $300,000,000.00 and $325,000,000.00. This range is inclusive of all CLINs over the full 5~~6~~ year performance period and 6 month OES.

The total estimated value for all proposed optional surge CLINs (CLIN TBD) and requirements must be ~~no greater than~~ fifty percent of the mandatory CLINs (CLIN TBD) value; the mandatory CLINs do NOT include ODCs or Long-Distance Travel, or CAF. Additionally, the surge estimate does not include ODCs or Long-Distance Travel, or CAF. Any proposal that is not within this range shall include an explanation that specifically draws the Government's attention to any unique technical aspects of the proposal the Offeror would like the Government to consider as the justification for the deviation from the range. Optional surge CLINs are fluid in that they may carry forward to future periods of performance if ~~unactivated~~inactivated in the current period, and may be transferred forward from a future period if needed for current performance. Optional surge quantities do not expire with the contract's period of performance.

L.5.2.2.3 SUBCONTRACTOR SUPPORTING DOCUMENTATION (TAB D)

The Offeror shall also provide supporting cost/price documentation for all proposed subcontractors, including the total value of the proposed subcontract, the proposed type of subcontract, the rationale and/or justification for this type of subcontract type. Additionally, the Offeror shall provide a narrative detailing the processes used to evaluate the subcontracts it is proposing. Failure to provide complete supporting documentation may result in no further consideration of the Offeror's proposal. **Failure to propose at least 25% of the total contract value as subcontractor effort will result in no further consideration for award**.[2] For the final subcontracting percentage, which must be greater than 25%, it is the intent of CBP to negotiate

[2] Alliant 2, Section G.22 INDIVIDUAL SMALL BUSINESS SUBCONTRACTING PLAN, references the Master Subcontracting Plans each contract holder manages with goals that need to be met across all task orders. The total small business goal for Alliant is 50%.
As delineated in the ordering guide, in order to support Alliant's small business subcontracting plan and receive Socio-Economic Credit, the Ordering Contracting Officer's (OCO's) should negotiate specific individual subcontracting goals at the Task Order level without creating a separate subcontracting plan.
DHS's small business subcontracting goal is 41%.

an individual small business goal within the subcontracting effort **after award of the task orders**. Subcontractors may submit proprietary data directly to the CO via CBPTASPDRequirements@cbp.dhs.gov. The prime contractor shall specifically state whether the estimated costs of any proposed subcontractor will be in excess of $10M over the life of the TO for Government accomplished Equal Employment Opportunity (EEO) verification purposes.

L.5.2.2.4 COST/PRICE ASSUMPTIONS (TAB E)

The Offeror must submit all (if any) assumptions upon which the Cost/Price Proposal is based.

L.5.3 SUBMISSION OF THE WRITTEN TECHNICAL PROPOSAL (PART II)

Part II of Written Technical Proposal and shall contain the following:

a. DD254 (Offeror is required to complete Blocks 6a, 6b and 6c; and Subcontractors are required to complete blocks 7a, 7b and 7c.)

b. Written Technical Submission as below.

Each Offeror shall submit all information described in the following paragraphs. The Offeror shall provide one original electronic copy, containing all required sections of this Part. No thumb drives will be accepted. The written Technical Proposal is limited to 30 pages total.

L.5.3.1 TECHNICAL APPROACH (FACTOR 2)

The Offeror shall identify and describe the methodology and analytical techniques to be used in fulfilling the technical requirements identified in the RFQ. The Offeror should tailor the technical approach to achieve the requirements as identified in this solicitation. The Offeror's proposal shall be relevant to this RFQ and reflect an effective understanding of RFQ requirements. The Agile framework described in the PWS shall be applied in the performance of all tasks identified the PWS and throughout this requirement. Throughout the proposal, Offerors should discuss the benefits the Government should expect to realize as a result of implementing the solutions proposed.

These elements are not ~~subfactors~~sub factors and will not be individually rated, but will be evaluated as a whole to arrive at the factor-level rating:

a. Offerors shall discuss their technical approach to meeting the objectives, conditions, and task requirements identified in this solicitation.
b. Offeror's shall propose performance measures, metrics, and performance standards that align with their proposed technical solution in the form of a Quality Assurance Surveillance Plan (QASP). Discuss why they were selected, the performance levels, and to the expected benefit the Government should realize.
c. Innovation and Technology Transfer: The Offeror shall describe any innovative techniques or approaches in performing the requirements that would benefit the CBP mission by way of optimizing and improving performance as well as reducing performance risk. Offerors shall discuss their innovation and technology transfer methods and describe any partnerships with academia, commercial partners, think tanks, vendor

centers of excellence, and technology transfers from other Agencies as means to introduce cutting edge techniques to the Targeting mission. Offeror's shall discuss other corporate innovation and proven approaches of targeting models.

d. The Offeror shall describe its agile process and discuss the ideal frequency of Sprints. Offeror's shall describe an effective approach for coordination and collaboration within agile teams, across the TO, and outside of TASPD to ensure efficient service delivery, promote knowledge sharing, manage stakeholders, and support customer requirements.

L.5.3.2 MANAGEMENT APPROACH (FACTOR 3)

The Offeror shall describe the management approach for managing the work described in the PWS~~, the Scope, Specific Tasks, and Deliverables sections~~. These elements are not ~~subfactors~~sub factors and will not be individually rated, but will be evaluated as a whole to arrive at the factor-level rating:

a. Offerors shall discuss their managerial approach to meeting the objectives, conditions, and task requirements identified in this solicitation.

b. The Offeror shall describe how its management approach contributes to the efficient use of human resources, and its approach to recruiting and retaining a skilled workforce that has the diverse skill sets required to effectively service the full range of needs.

c. The Offeror's approach for providing program management for this TO, communication with the TASPD TPOC and COR, process management and control, project status and cost reporting, proactive risk management, subcontractor management and program metrics.

d. For each subcontractor and teaming partner, Offeror's shall explain how management control will be exercised directly related to satisfying mission critical performance requirements. This explanation shall demonstrate clearly how the Offeror will minimize CBP's involvement in managing the day-to-day operations for which the Offeror will be responsible.

e. Offerors shall submit teaming agreements with all proposed teaming partners, and state whether or not the agreement is exclusive. Please note exclusive teaming agreements are discouraged, but not prohibited. Teaming agreements are exempt from page counts.

f. The proposal must clearly demonstrate at least 25% of this effort is subcontracted.

g. The Offeror shall describe its plan for ensuring they have an established, maintained, and effective Quality Management System (QMS) that ensures quality products and services are delivered to the Government. This plan shall align with its proposed QASP.

h. Security Plan; The Offeror shall describe its plan for ensuring the contractor team complies with contract security requirements and sensitive information protection policies, including ensuring that all personnel have the appropriate level of clearances.

i. Assignments of Teaming Partners; the proposal shall describe the assignment of team partners to each PWS task and technical area, and describe the technical expertise and capability of the teaming partner proposed to perform each task.

j. Project Staffing Plan. The Offeror shall describe its rationale for the proposed labor mix, skill mix, use of subcontractors and level of effort to support each task indicated in PWS. The Offeror shall also describe:

   a. Rationale for choosing the personnel/team partner. Describe how personnel and team partners would be involved in each task/subtask and how their qualifications and experience uniquely qualify them for the work they are proposed to perform.
   b. The rationale for projected staffing and approach to how each task and subtask is staffed including estimated hours and labor mix of the proposed personnel.
   c. Rationale for proposed labor categories and level of effort for each task.
   d. Approach to hiring, retaining, replacing, and surging appropriately cleared and certified personnel with appropriate skillsets throughout the life of this TO.

L.5.3.3 TRANSITION APPROACH (FACTOR 4)

The Offeror shall provide a Transition-In Plan that aligns with the requirements stated in PWS as a phased approach that provides for a seamless transition from the incumbent to the new contractor (hereafter referred to as the Offeror). The proposal shall include:

a. Timelines for the transition and the identification of risks associated with the transition.
b. Roles and responsibilities of the Offeror including proposed schedule(s) and milestones to ensure no disruption of service. The Transition-In Plan shall also identify and discuss the roles and responsibilities of the incumbent contractor and information expected from the incumbent.
c. The Offeror shall also identify any actions the Offeror assumes are the responsibility of the Government.
d. The Offeror shall define interfaces with the CBP and the Offeror's proposed coordination with the current contractor(s). If transfer of existing CBP databases to other hardware/software formats is proposed, the Offeror shall explain how and when the proposed formats/systems and their capabilities will be demonstrated prior to effecting any transfer.
e. The Offeror shall identify the risks to the transition effort and include mitigation and contingency plans in the event the transition cannot be executed on schedule.
f. The transition plan shall include specific measures and metrics to be used to monitor and evaluate the transition activities and to ensure that system performance and response times are not degraded during the transition period.
g. The transition plan shall include a work plan which identifies milestones, measurable tasks, and resources required, to include the Offeror's staffing strategy and how they will

recruit and hire and onboard background investigation cleared personnel if needed to ensure mission success.

h. The transition plan shall include a plan for executing redundant performance with the outgoing contractor upon successful completion of knowledge transfer.

L.6 DELIVERY INSTRUCTIONS

The Offeror shall deliver written proposals to and receive acceptance from cbptaspdrequirements@cbp.dhs.gov by dates listed in the cover letter.

M.1 METHOD OF AWARD

(a) Four- (4) single award Time and Materials (T&M) Task Order (TO) awards are contemplated as a result of this solicitation. There will be two (2) TOs awarded for O&M – Transition Task Order and Requirements Execution TO; likewise, there will be two (2) TOs awarded for BISS-Transition Task Order and Requirements Execution TO. One Offeror will be selected for each requirement, who has been determined to represent the best value to the Government, all factors considered. The technical evaluation factors are of equal importance. There are no sub-factors. Award may be made to other than the lowest priced technically acceptable proposal.

(b) This procurement is being conducted using a two-phased voluntary down-select process. Offerors will receive an advisory notification from the Contracting Officer after Phase I evaluations are complete, and must inform the Government of their intent to participate in Phase II within three (3) days of receiving their notification.

(c) This acquisition is being conducted under FAR 16.5. Principles and procedures of Subpart 15.3 do not apply. Accordingly, the Government reserves the right to do any or all of the following:

a. Award on initial proposals, without discussion.
b. After an Offeror has been selected for award based upon a best value determination, the Government may negotiate a final reduced price. The Government may make award based on initial offers received or the Government may make award after clarifications of some aspects of the proposal or discussions relative to price only.
c. Have communications; ask clarifying questions, request corrections relative to minor errors in the cost/price proposal, or request cost/price substantiating documentation to facilitate the Government's final evaluation of cost proposals with one or some Offerors. These communications, clarifications, or requests for corrections or substantiating documentation will not materially change the Offeror's proposal in terms of conformance to requirements, constitute discussions, or materially change pricing.

The Government anticipates selecting the best-suited Offeror from initial responses, without engaging in exchanges with Offeror. Offeror are strongly encouraged to submit their best technical solutions and price in response to this solicitation.

Once the Government determines the Offeror that is the best-suited (i.e., the apparent successful Offeror), the Government reserves the right to communicate with only that Offeror to address any remaining issues, if necessary, and finalize a task order with that Offeror. These issues may include technical and price. If the parties cannot successfully address any remaining issues, as determined pertinent at the sole discretion of the Government, the Government reserves the right to communicate with the next best-suited Offeror based on the original analysis and address any remaining issues. Once the Government has begun communications with the next best-suited Offeror, no further communications with the previous Offeror will be entertained until after the task order has been awarded. This process shall continue until an agreement is successfully reached and a task order is awarded.

M.2 EVALUATION

FAR 52.212-2 EVALUATION—COMMERCIAL ITEMS (OCT 2014)

a. The Government will award a contract resulting from this solicitation to the responsible Offeror whose offer, conforming to the solicitation, will be the most advantageous to the Government, price and other factors considered. The following factors shall be used to evaluate Offerors:

Factor 1: Corporate Experience,

Factor 2: Technical Approach,

Factor 3: Management Approach,

Factor 4: Transition Approach, and

Factor 5: Price

b. Options. The Government will evaluate offers for award purposes by adding the total price for all option periods and optional quantities to the total price for the requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of the option(s) shall not obligate the Government to exercise the option(s).

c. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer) unless a written notice of withdrawal is received before award.

M.3 PASS/FAIL ELEMENTS

The Government will evaluate the following pass/fail elements. **A failure on any single Pass/Fail criteria will make the proposal ineligible for award, with no further evaluation of the technical and cost proposal conducted by the Government.**

Pass/Fail Elements:

The following will be evaluated on a Pass/Fail basis:

a. The Government will reject any proposal where the Offeror is not an awardee of the master contract.
b. The Government will reject any proposal where the Offeror does not meet the minimum level of subcontracting. Please refer to section L.5.2.2.3 for further information.

M.4 COST/PRICE PROPOSAL EVALUATION

The Offeror's cost/price proposal will be evaluated to assess for price reasonableness, accuracy, completeness, consistency, and traceability to the proposed technical approach. The importance of price may increase as the differences between Offeror's non-price factors decreases.

The CAF is not included in the price evaluation.

Costs that are excessively high or low (without sufficient justification) may be considered unrealistic and unreasonable and may receive no further consideration. Any proposal that is not within the total estimated value cited in Section L.5.2.2.2 shall include an explanation that specifically draws the Government's attention to any unique technical aspects of the proposal the Offeror would like the Government to consider as the justification for the deviation from the range. The Government may perform a price realism analysis.

The labor mix will be assessed in conjunction with task requirements to determine whether proposed labor categories and the skill level of proposed workers are appropriate for the work to be accomplished.

Options will be evaluated in accordance with FAR 52.217-5, Evaluation of Options.

Offerors shall provide an estimated overall price for the base period and all option periods, including option to extend services, based on the rates they provide and their unique technical solutions. The Government will not provide a Sample Price Format, however, pricing and Section B's CLIN Structure should correlate to the Offeror's proposed unique technical solution. The Government will review the Offeror's proposed labor categories and corresponding labor rates in accordance with the Offeror's GSA Alliant 2, Unrestricted Schedule Contract. Proposed rates must be at or below the Offeror's published GSA Alliant 2, Unrestricted schedule rates. The Government is requesting discounts, which should be clearly noted in the price proposal.

M.5 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

Tab A will be evaluated to assess whether or not an actual or potential OCI exists as defined by FAR Part 9.5. If an actual or potential OCI is identified that cannot be feasibly mitigated, avoided, or resolved in accordance with FAR Part 9.5, that Offeror may be ineligible for award.

M.6 COST ASSUMPTIONS

The Government reserves the right to reject any proposal that includes any cost assumptions that may adversely impact satisfying the Government's requirements.

M.7 OVERTIME AND EXTENDED BILLING HOUR PRACTICES

The Government reserves the right to reject any proposal that includes overtime or extended hours billing practices that adversely impact or affect the Government's requirements.

M.7 TECHNICAL EVALUATION FACTORS

M.7.1 FACTOR 1: CORPORATE EXPERIENCE (PHASE I)

The Prior Specialized Experience factor will be evaluated based on an overall (i.e., taken as a whole) consideration of the following (these elements are not ~~subfactors~~sub factors and will not be individually rated, but will be evaluated as a whole to arrive at the factor-level rating):

a. Corporate experience reflects/identifies experience on projects that are similar in size, scope, and complexity to the requirements contained in Section C of the RFQ.

b. Corporate experience reflects current experience and the Offeror's roles and responsibilities are similar in scope and complexity to the requirements contained in Section C of the RFQ.
c. Corporate experience reflects the Offeror's approach to client support including quality assurance, risk management, and maintaining effective lines of communication.

M.7.2 FACTOR 2: TECHNICAL APPROACH (PHASE II)

The Government will evaluate the Technical Approach factor based on the clarity and completeness of the approach and the degree to which the proposal meets the requirements of the solicitation and includes innovative and efficient methodologies. The following elements are not ~~subfactors~~sub factors and will not be individually rated, but will be evaluated as a whole to arrive at the factor-level rating:

a. A clear, comprehensive, and relevant approach to meeting the objectives conditions, and task requirements identified in the solicitation.
b. An effective approach for coordination and collaboration within agile teams, across the TO, and outside of TASPD to ensure efficient service delivery, promote knowledge sharing, manage stakeholders, and support customer requirements.
c. Practical and detailed performance measures, metrics, that quantify, measure, track, and report operational performance relating to both systems and management performance, as well as the degree to which they achieve the agency's objectives/requirements in the Offeror's proposed QASP.

M.7.3 FACTOR 3: MANAGEMENT APPROACH (PHASE II)

The Government will evaluate the approach for providing program management support, communication with TASPD TPOC and COR, process management and control, project status and cost reporting, proactive risk management, and program metrics. The following elements are not ~~subfactors~~sub factors and will not be individually rated, but will be evaluated as a whole to arrive at the factor-level rating:

a. The Project Staffing Plan will be evaluated to assess the degree to which it complies with the requirements outlined in Section L., including the estimated hours, labor mix, experience, skills, and qualifications of the personnel proposed.

b. Clear and comprehensive staffing and approach to how each task and subtask is staffed including estimated hours and labor mix of personnel, and functional knowledge.
   - Clear and detailed value that the personnel add to the project team, including their specific skills, experience, and qualifications.
   - Clear rationale for proposed labor categories and level of effort for each task.
   - A clear and effective approach to recruiting, hiring, retaining, replacing, and surging appropriately cleared and certified personnel with appropriate skill sets throughout the life of this TO.
   - Subcontractor task alignment

M.7.4 FACTOR 4: TRANSITION APPROACH (PHASE II)

The Transition-In Plan will be evaluated based on its comprehensiveness, detail, and effectiveness to assume full contractual responsibility for the entire proposed PWS without degradation of high quality services.

M.8 TECHNICAL ASSUMPTIONS

Offeror assumptions should be included with and will be reviewed in the context of the technical factor to which they apply. The Government reserves the right to reject any proposal that includes any assumption that may adversely impact satisfying the Government's requirements.